



Branch Circuit Monitor

User Guide
Release 3.1.0

Copyright © 2015 Raritan, Inc.

BCM-0D-v3.1.0-E

March 20, 2015

255-64-0002-00

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 2013 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.



CAUTION:

To reduce the risk of shock — Use indoors only in a dry location. No user serviceable parts inside. Refer servicing to qualified personnel. For use with IT equipment only. Disconnect power before servicing.



Safety Guidelines

WARNING! These instructions must be performed by a licensed electrician.

WARNING! Raritan products must not be serviced while energized. When power is present, do not open any panels or service the line cord. Always disconnect the far end of the line cord from power before servicing. Servicing the product while energized may result in electric shock, fire, personal injury and death.

WARNING! Read and understand all sections in this guide before installing or operating this product.

WARNING! Connect this product to a 3-phase AC power source whose voltage is within the range specified on the product's nameplate. Operating this product outside the nameplate voltage range may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to a 3-phase AC power source that is current limited by a suitably rated circuit breaker in accordance with national and local electrical codes. Operating this product without proper current limiting may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to a protective earth ground. Failure to connect to a protective earth ground may result in electric shock, fire, personal injury and death.

WARNING! This product contains no user serviceable parts. Do not open, alter or disassemble this product. All servicing must be performed by qualified personnel. Disconnect power before servicing this product. Failure to comply with this warning may result in electric shock, personal injury and death.

WARNING! Use this product in a dry location. Failure to use this product in a dry location may result in electric shock, personal injury and death.

WARNING! A current transformer (CT) must never be operated when it is not connected to the Branch Circuit Monitor. Operating a CT "open circuit" will cause permanent damage to the CT.

WARNING! Snap CTs only onto circuit conductors that are properly insulated per national and local electrical codes. Failure to snap CTs onto properly insulated conductors may result in electric shock, fire, personal injury and death.

WARNING! Do not rely on the power data displayed by this product to determine whether power is being supplied on a particular circuit/line. Disconnect the device from the branch circuit before performing repair, maintenance or service on the device. Failure to disconnect a device before servicing it may result in electric shock, fire, personal injury and death.

WARNING! Do not use this product to measure and monitor the power source that powers critical patient care equipment, fire or smoke alarm systems. Use of this product in such applications may result in personal injury and death.

WARNING! Installation of this product and CTs must be performed by a licensed electrician, and the power system monitored by this product must be suitably rated based on the product's nameplate ratings and national and local electrical codes. Installation by unlicensed electricians or failure to select a suitably rated power system may result in electric shock, fire, personal injury or death.

WARNING! This product contains a chemical known to the State of California to cause cancer, birth defects, or other reproductive harm.

Safety Instructions

1. Installation of this product and current transformers (CTs) should only be performed by a licensed electrician.
2. Make sure the line cord is disconnected from power before physically mounting or moving the location of this product.
3. Connect the line cord of this product only to a 3-phase AC power source that is current limited by a suitably rated branch circuit breaker in accordance with national and local electrical codes.
4. Examine the branch circuit that will supply electric power to this product. Make sure the branch circuit's power lines, neutral and protective earth ground terminals are wired correctly and are the correct voltage and phase. Make sure the branch circuit is protected by a suitably rated circuit breaker.
5. Before installing CTs, make sure there are no damages, cuts or wear on the insulation of CT leads.
6. Do NOT operate a CT when it is not connected to the Branch Circuit Monitor. Operating a CT "open circuit" causes permanent damage to the CT. Make sure the branch circuit breaker is turned OFF before snapping the CT onto a branch circuit conductor and do NOT turn the breaker on until the CT is properly connected to the Branch Circuit Monitor.
7. Make sure that the circuit conductors that CTs will monitor are properly insulated per national and local electrical codes, and the conductor's insulation is at least 0.4mm thick.

Contents

Safety Guidelines	iii
--------------------------	------------

Safety Instructions	iv
----------------------------	-----------

What's New in the Branch Circuit Monitor Release 3.1.0	xiii
---	-------------

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

Overview	2
Product Models	3
Connection Ports	3
Product Features	4
Package Contents.....	7

Chapter 2 Installation and Configuration	8
---	----------

Before You Begin	8
Unpacking the Product and Components.....	8
Observing the Safety Guidelines and Instructions	8
Checking the AC Electrical Panel	9
Printing the Circuit Monitoring Worksheet	9
Connecting an Electrical Conduit.....	10
Mounting the Branch Circuit Monitor	11
Channel Convention	12
Setting Up a Power Monitoring System	14
Raritan Current Transformers (Optional).....	16
Configuring the Branch Circuit Monitor	22
Connecting the Branch Circuit Monitor to a Computer.....	23
Installing the USB-to-Serial Driver (Optional)	24
Connecting the Branch Circuit Monitor to Your Network.....	25
Initial Network Configuration via CLI	26
Bulk Configuration.....	32
Saving a Branch Circuit Monitor Configuration	33
Copying the Branch Circuit Monitor Configuration	34

Mapping Channels with Branch Circuits	35
Cascading the Branch Circuit Monitor via USB	37

Chapter 3 Connecting External Equipment (Optional) 40

Connecting Environmental Sensor Packages	40
DPX Sensor Packages	41
DPX2 Sensor Packages	44
DX Sensor Packages	47
Connecting the Asset Management Sensor	51
Connecting a Logitech Webcam	61
Connecting a GSM Modem	62
Connecting an Analog Modem	62
Connecting an External Beeper	63
Connecting an RF Code PDU Sensor Tag	63

Chapter 4 Panel Components 64

Line Cord	64
Channels	65
Mains Channels	65
Branch Circuit Channels	66
CT Terminals and Buttons	66
Connection Ports	67
LCD Display Panel	68
LCD Display	68
Control Buttons	71
Operating the LCD Display	71
Reset Button	78

Chapter 5 Using the Web Interface 79

Supported Web Browsers	79
Logging in to the Web Interface	80
Login	80
Changing Your Password	82
Logout	82
Introduction to the Web Interface	83
Menus	84
Explorer Pane	84
Setup Button	87
Status Bar	88
Add Page Icon	89
Logout Button	90
Data Pane	90
More Information	90
Viewing the Dashboard	95
Alerted Sensors	95

Alarms List	96
Device Management	97
Displaying the Device Information	98
Naming the Branch Circuit Monitor	103
Modifying the Network Configuration	103
Modifying Network Service Settings	111
Setting the Date and Time	118
Setting Default Measurement Units	121
Configuring the Feature Port	121
Configuring the Serial Port	123
Specifying the Device Altitude	124
Setting Data Logging	125
Configuring SMTP Settings	126
Checking the Internal Beeper State	127
Rebooting the Branch Circuit Monitor Device	128
Channel or CT Configuration	128
Configuring the Mains Channels	129
Configuring the Branch Circuit Channels	130
Naming the Mains Channels	132
Naming Branch Circuit Channels	132
Monitoring the Mains Channels	133
Monitoring the Branch Circuit Channels	134
Setting Power Thresholds	136
Setting the Mains Thresholds	136
Setting the Branch Circuit Thresholds	137
Bulk Configuration for Branch Circuit Thresholds	138
What is Deassertion Hysteresis?	139
What is Assertion Timeout?	141
User Management	141
Creating a User Profile	142
Modifying a User Profile	145
Deleting a User Profile	146
Changing the User List View	146
Setting Up Your Preferred Measurement Units	146
Setting Up Roles	147
Creating a Role	147
Modifying a Role	148
Deleting a Role	149
Changing the Role List View	149
Access Security Control	150
Forcing HTTPS Encryption	150
Configuring the Firewall	150
Setting Up User Login Controls	157
Setting Up Role-Based Access Control Rules	161
Setting Up a TLS Certificate	165
Certificate Signing Request	166
Creating a Self-Signed Certificate	168
Installing Existing Key and Certificate Files	170
Downloading Key and Certificate Files	170
Setting Up External Authentication	171
Gathering the External Authentication Information	171
Adding Authentication Servers	173

Sorting the Access Order	177
Testing the Server Connection	177
Editing Authentication Server Settings	178
Deleting Authentication Server Settings	178
Disabling External Authentication	178
Enabling External and Local Authentication Services	179
Event Rules and Actions	180
Components of an Event Rule	180
Creating an Event Rule	181
Sample Event Rules	213
A Note about Infinite Loop	215
Modifying an Event Rule	216
Modifying an Action	217
Deleting an Event Rule or Action	218
A Note about Untriggered Rules	218
Viewing Connected Users	219
Monitoring Server Accessibility	220
Adding IT Devices for Ping Monitoring	220
Editing Ping Monitoring Settings	221
Deleting Ping Monitoring Settings	222
Checking Server Monitoring States	222
Managing Event Logging	223
Viewing the Local Event Log	223
Clearing Event Entries	224
Viewing the Wireless LAN Diagnostic Log	224
Environmental Sensors and Actuators	225
Identifying Environmental Sensors	226
Managing Environmental Sensors and Actuators	229
Configuring Environmental Sensors	231
Viewing Sensor Data and Actuator Data	237
Unmanaging Environmental Sensors	241
Disabling the Automatic Management Function	242
Controlling Actuators	242
Asset Management	243
Configuring the Asset Sensor	243
Setting Asset Sensor LED Colors	245
Changing a Specific Rack Unit's LED Color Settings	246
Expanding a Blade Extension Strip	247
Displaying the Asset Sensor Information	248
Webcam Management	249
Configuring Webcams	249
Adjusting Image Properties	250
Viewing Webcam Snapshots or Videos	251
Sending Snapshots or Videos in an Email or Instant Message	253
Snapshot Storage	255
Firmware Upgrade	258
Updating the Branch Circuit Monitor Firmware	258
Viewing Firmware Update History	259
Full Disaster Recovery	259
Viewing the Communication Log	260
Network Diagnostics	260
Pinging a Host	261

Tracing the Network Route	261
Listing TCP Connections	261
Downloading Diagnostic Information	262
Backup and Restore of Branch Circuit Monitor Device Settings	262
Accessing the Help	263
Retrieving Software Packages Information	263
Browsing through the Online Help	263

Chapter 6 Using SNMP 265

Enabling SNMP	266
Configuring Users for Encrypted SNMP v3	267
Configuring SNMP Notifications	268
SNMPv2c Notifications	269
SNMPv3 Notifications	271
SNMP Gets and Sets	273
The Branch Circuit Monitor MIB	273
A Note about Enabling Thresholds	275

Chapter 7 Using the Command Line Interface 276

About the Interface	277
Logging in to CLI	277
With HyperTerminal	277
With SSH or Telnet	278
With an Analog Modem	279
Different CLI Modes and Prompts	280
Closing a Local Connection	280
Help Command	281
Querying Available Parameters for a Command	282
Showing Information	282
Device Configuration	283
Network Configuration	283
Date and Time Settings	285
Default Measurement Units	286
Branch Circuit Information	286
Mains Information	287
Branch Circuit Threshold Information	288
Branch Circuit Pole Threshold Information	289
Mains Threshold Information	290
Mains Pole Threshold Information	291
Environmental Sensor Information	292
Environmental Sensor Package Information	294
Actuator Information	295
Environmental Sensor Threshold Information	296
Environmental Sensor Default Thresholds	297
USB-Cascading Configuration Information	298
Security Settings	298
Existing User Profiles	299

Existing Roles	300
Serial Port Settings	300
Asset Sensor Settings	301
Rack Unit Settings of an Asset Sensor.....	301
Blade Extension Strip Settings	302
Event Log.....	303
Wireless LAN Diagnostic Log	304
Server Reachability Information	304
Reliability Data.....	305
Reliability Error Log	306
Command History	306
History Buffer Length	306
Examples	306
Clearing Information.....	308
Clearing Event Log	308
Configuring the Branch Circuit Monitor Device and Network	308
Entering Configuration Mode.....	309
Quitting Configuration Mode	309
Device Configuration Commands.....	310
Network Configuration Commands.....	311
Configuring Environmental Sensors' Default Thresholds	381
Example - Default Upper Thresholds for Temperature	383
Environmental Sensor Configuration Commands	383
Changing the Sensor Name	384
Specifying the CC Sensor Type	384
Setting the X Coordinate	385
Setting the Y Coordinate	385
Setting the Z Coordinate.....	386
Changing the Sensor Description	386
Using Default Thresholds	387
Setting the Alarmed to Normal Delay for DX-PIR.....	387
Examples	387
Environmental Sensor Threshold Configuration Commands	388
Example 1 - Upper Critical Threshold for a Temperature Sensor	390
Actuator Configuration Commands.....	391
Example - Actuator Naming.....	392
USB-Cascading Configuration Commands	392
Configuring the Cascading Mode	392
Asset Management Commands	393
Asset Sensor Management	393
Rack Unit Configuration.....	396
Examples	399
Actuator Control Operations	399
Switching On an Actuator	400
Switching Off an Actuator	400
Example - Turning On a Specific Actuator	401
Unblocking a User.....	401
Resetting the Branch Circuit Monitor	401
Restarting the Device	402
Resetting to Factory Defaults	402
Network Troubleshooting	403
Entering Diagnostic Mode	403

Quitting Diagnostic Mode	403
Diagnostic Commands	403
Retrieving Previous Commands	406
Automatically Completing a Command.....	406
Logging out of CLI.....	407

Appendix A Specifications 408

Branch Circuit Monitor Specifications	408
Raritan CT Specifications	408
Mains CT Rated at 200A	408
Mains CT Rated at 250A	409
Branch Circuit CTs Rated at 60A	410
Branch Circuit CTs Rated at 60A	411
Power Measurement Accuracy.....	412
Mains Accuracy	412
Branch Circuit Accuracy	412
Maximum Ambient Operating Temperature.....	413
Appendix B RADIUS Configuration Illustration	414
Microsoft Network Policy Server.....	414
Non-Windows RADIUS Server	438
Serial RS-232 Port Pinouts	440
Sensor RJ-12 Port Pinouts	440
Feature RJ-45 Port Pinouts	440

Appendix C Circuit Monitoring Worksheet 442

Appendix D Resetting to Factory Defaults 443

Using the Reset Button	443
Using the CLI Command.....	444

Appendix E LDAP Configuration Illustration 445

Step A. Determine User Accounts and Groups	445
Step B. Configure User Groups on the AD Server	446
Step C. Configure LDAP Authentication on the Branch Circuit Monitor Device	447
Step D. Configure Roles on the Branch Circuit Monitor	450

Appendix F Integration 454

Power IQ	454
Adding PDUs to Power IQ Management.....	455

Contents

Dominion KX II	457
Connecting to KX II.....	457
Naming the Branch Circuit Monitor in the KX II.....	458
RF Code Energy Monitoring Solution	460
 Appendix G Additional Branch Circuit Monitor Information	461
<hr/>	
Altitude Correction Factors	461
Raritan Training Website	462
Truncated Data in the Web Interface.....	462
Reserving IP Addresses in Windows DHCP Servers	463
Ways to Probe Existing User Profiles	463
 Index	465
<hr/>	

What's New in the Branch Circuit Monitor Release 3.1.0

The following sections have changed or information has been added to the Branch Circuit Monitor help based on enhancements and changes to the equipment and/or user documentation.

- ***DPX Sensor Packages*** (on page 41)
- ***DPX2 Sensor Packages*** (on page 44)
- ***DX Sensor Packages*** (on page 47)
- ***Environmental Sensor Information*** (on page 75)
- ***Configuring Environmental Sensors' Default Thresholds*** (on page 381)
- ***Environmental Sensor Configuration Commands*** (on page 383)
- ***Environmental Sensor Threshold Configuration Commands*** (on page 388)
- ***Actuator Configuration Commands*** (on page 391)
- ***USB-Cascading Configuration Commands*** (on page 392)
- ***Actuator Control Operations*** (on page 399)
- ***Connecting a GSM Modem*** (on page 62)
- ***Connecting an Analog Modem*** (on page 62)
- ***Connecting an External Beeper*** (on page 63)
- ***Checking the Internal Beeper State*** (on page 127)s

Please see the Release Notes for a more detailed explanation of the changes applied to this version of the Branch Circuit Monitor.

Chapter 1

Introduction

This chapter briefly introduces the Raritan Branch Circuit Monitor (BCM) and current transformers (CTs), which provide a centralized power monitoring solution at the circuit level.

In This Chapter

Overview	2
Product Models.....	3
Connection Ports	3
Product Features	4
Package Contents	7

Overview

The Branch Circuit Monitor (BCM) is a product that is designed to measure and display the power and energy consumption of multiple branch circuits.

BCM provides power and energy data on branch circuits and mains in an electrical service entrance or a remote power panel. It provides an accurate view of electrical capacity, energy use, and monitoring for uptime and reliability. Anytime a circuit's current approaches a breaker's limit, BCM sends an alarm, helping you to prevent potential problems. Customizable alarms allow the operator to easily set sensitivity parameters.

Use of this product helps you do the following at the CIRCUIT level:

- Monitor the power and energy consumption
- Analyze and optimize the power efficiency
- Avoid potential overload risks

To establish such a centralized power monitoring system, the items below are required:

- A Branch Circuit Monitor: You can remotely monitor the power and energy consumption of each conductor in the electrical panel through the Branch Circuit Monitor.
- Raritan CTs: A CT can detect the current of the conductor where it is snapped, and transmit the data to the Branch Circuit Monitor where it is connected. There are two types of CTs: mains CTs for monitoring mains circuits and branch circuit CTs for monitoring branch circuits.

Currently, the Branch Circuit Monitor applies to a 3-phase Wye-connected electrical panel that is rated up to 250A (or higher with appropriately rated mains CTs, such as 400A/600A), and contains at least one 3-phase branch circuit breaker rated at 20A (North America) or 16A (Europe).

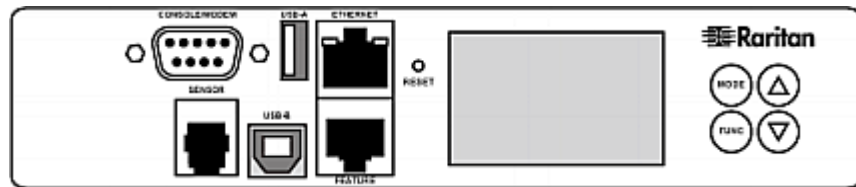
Note: Contact Raritan sales for more information on measuring electrical panels that are rated higher than 250A.

Product Models

The Branch Circuit Monitor comes in several models that are built to stock and can be obtained almost immediately. Raritan also offers custom models that are built to order and can only be obtained on request.

Download the Branch Circuit Monitor Data Sheet from Raritan's website, visit the **Product Selector page** (<http://www.findmypdu.com/>) on Raritan's website, or contact your local reseller for a list of available models.

Connection Ports



The table below explains the function of each port.

Port	Used for...
USB-B	Establishing a USB connection between a computer and the Branch Circuit Monitor device. This port can be used for disaster recovery of the Branch Circuit Monitor device. Contact Raritan Technical Support for instructions.
USB-A	Connecting a USB device, such as a Logitech® webcam. This is a "host" port, which is powered, per USB 2.0 specifications.
FEATURE	Connecting a power CIM, asset sensor, or external beeper using an Category 5e/6 cable. <i>Warning: This is not an RS-232 port so do NOT plug in an RS-232 device, or damages can be caused to the device.</i>
CONSOLE/ MODEM	Establishing a serial connection between a computer and the Branch Circuit Monitor device: This is a standard DTE RS-232 port. You can use a null-modem cable with two DB9 connectors on both ends to connect the Branch Circuit Monitor device to the computer.
SENSOR	Connection to Raritan's environmental sensor packages. A Raritan sensor hub may be required if you want to connect multiple environmental sensors. However, Raritan does sell multiple sensors connecting to the SENSOR port through a single RJ-12 connector. For example, a DPX-T3H1 (3 temperature and 1 humidity sensor) uses only

Port	Used for...
	one RJ-12 port connection.
ETHERNET	<p>Connecting the Branch Circuit Monitor device to your company's network:</p> <p>Connect a standard Cat5e/6 UTP cable to this port and connect the other end to your network. This connection is necessary to administer or access the Branch Circuit Monitor device remotely using the web interface.</p> <p>There are two small LEDs adjacent to the port:</p> <ul style="list-style-type: none"> ▪ Green indicates a physical link and activity. ▪ Yellow indicates communications at 10/100 BaseT speeds. <p>For a USB-cascading configuration in the bridging mode, the wired network connection is a must for the <i>master</i> Branch Circuit Monitor. See Cascading the Branch Circuit Monitor via USB (on page 37) for details.</p> <hr/> <p><i>Note: Connection to this port is not required if connection to a wireless network is preferred.</i></p>

Product Features

The Branch Circuit Monitor features include:

- The capability to monitor the following at the mains level:
 - RMS current per line (A)
 - RMS voltage per line pair (V)
 - Active power (W)
 - Apparent power (VA)
 - Power factor
 - Active energy (Wh)
 - Unbalanced load percentage (for 3-phase models)
- The capability to monitor the following at the branch circuit level:
 - RMS current (A)
 - RMS voltage (V)
 - Active power (W)
 - Apparent power (VA)
 - Power factor
 - Active energy (Wh)
 - Line frequency (Hz), if available on your model
 - Unbalanced load percentage (for a 3-phase branch circuit only)

Note: The Branch Circuit Monitor only supports measuring and monitoring single-phase and 3-phase branch circuits.

- The capability to monitor environmental factors such as external temperature and humidity
- User-specified location attributes for environmental sensors
- Configurable alarm thresholds and hysteresis
- Configurable assertion timeout for thresholds
- Support for SNMP v1, v2, and v3
- The capability to send traps and informs using the SNMP protocol
- The capability to retrieve branch circuit specific data using SNMP, including current, voltage, and power
- The capability to store a data log of all sensor measurements and retrieve it via SNMP

Note: Raritan's Power IQ or other external systems can retrieve the stored data (samples) from the Branch Circuit Monitor.

- The capability to configure and set values through SNMP, including power threshold levels
- The capability to save one Branch Circuit Monitor device's configuration settings and then deploy those settings to other Branch Circuit Monitor devices
- The capability to back up and restore a Branch Circuit Monitor device's configuration
- Support for SSH and Telnet services
- For SSH, both password and public key authentications are supported
- Support for both of IPv4 and IPv6 networking
- Support for Modbus/TCP protocol
- Support for Baytech BSNMP
- Zero configuration service advertisement support
- Wireless connection via a Raritan-provided USB WIFI adapter
- The capability to share one Ethernet connection by cascading multiple Branch Circuit Monitor devices via the USB interface
- The capability to visually monitor the data center environment through a connected Logitech® webcam
- Support for webcam images sent via email to designated recipients
- Support of Cinterion® MC52iT and MC55iT GSM modems, which allow you to send customized SMS messages to designated recipients for specific events
- Remote dial-in access to the Branch Circuit Monitor via an analog modem
- The capability to monitor a connected Schroff® LHX-20, SHX-30 or LHX-40 heat exchanger
- Support for using any external beeper as an audio notification tool
- Support for Cisco EnergyWise
- The capability to diagnose the network, such as pinging a host or listing TCP connections
- The capability to monitor sever accessibility
- Full disaster recovery option in case of a catastrophic failure during a firmware upgrade
- The capability to display temperatures in Celsius or Fahrenheit, height in meters or feet, and pressure in Pascal or psi according to user credentials
- The capability to visually monitor the data center environment through a connected Logitech® webcam.

Package Contents

The following describes the equipment shipped with a Branch Circuit Monitor device. If anything is missing or damaged, contact the local dealer or Raritan Technical Support for help.

- The Branch Circuit Monitor
- Ring terminals
- Split-core mains current transformers (Optional)
- Split-core branch circuit current transformers (Optional)
- A null-modem cable with DB9 connectors on both ends (Raritan number: 254-01-0006-00) (optional)
- Cable ties

Chapter 2 Installation and Configuration

This chapter explains how to install a Branch Circuit Monitor device and configure it for network connectivity.

In This Chapter

Before You Begin	8
Connecting an Electrical Conduit	10
Mounting the Branch Circuit Monitor	11
Channel Convention	12
Setting Up a Power Monitoring System.....	14
Configuring the Branch Circuit Monitor	22
Bulk Configuration	32
Mapping Channels with Branch Circuits.....	35
Cascading the Branch Circuit Monitor via USB.....	37

Before You Begin

Before beginning the installation, perform the following activities:

- Unpack the product and components
- Check the AC electrical panel
- Print the Circuit Monitoring Worksheet
- Review the safety guidelines and instructions

Unpacking the Product and Components

1. Remove the Branch Circuit Monitor device and other equipment from the box in which they were shipped. See **Package Contents** (on page 7) for a complete list of the contents of the box.
2. Compare the serial number of the equipment with the number on the packing slip located on the outside of the box and make sure they match.
3. Inspect the equipment carefully. If any of the equipment is damaged or missing, contact Raritan's Technical Support Department for assistance.

Observing the Safety Guidelines and Instructions

1. Review the **Safety Guidelines** (on page iii) listed in the beginning of this user guide.
2. Review the **Safety Instructions** (on page iv) listed in the beginning of this user guide.

Checking the AC Electrical Panel

Before installing the Branch Circuit Monitor, verify that the electrical panel that it will monitor satisfies the following requirements:

- A 3-phase Wye-connected AC power system.
- The current and voltage ratings meet the ratings specified on the Branch Circuit Monitor's nameplate or label.
- Contains at least one 3-phase branch circuit breaker rated at 20A or 16A, conforming to national and local codes, such as UL508A Sec.17.5 in North America or EN/IEC 60934 and VDE 0642 in Europe. The Branch Circuit Monitor is connected to such a 3-phase branch circuit for electricity reception.
- Free of extreme temperatures and humidity. See **Maximum Ambient Operating Temperature** (on page 413) in the User Guide.

For example, an electrical panel must meet the following for a BCM-2400 model:

Power system	3-phase Wye-connected
Rated current	Max. 250A, or higher -- depending on the mains CT used
Rated voltage	190 to 415VAC
Circuit breaker	Contains at least one 3-phase branch circuit breaker rated at 20A or 16A

Printing the Circuit Monitoring Worksheet

A Circuit Monitoring Worksheet is provided in this guide. See **Circuit Monitoring Worksheet** (on page 442). Use this worksheet to record the panel number of the branch circuits monitored by the Branch Circuit Monitor, and usage of each branch circuit.

As you add, remove or swap CTs and/or channels, keep the worksheet up-to-date.

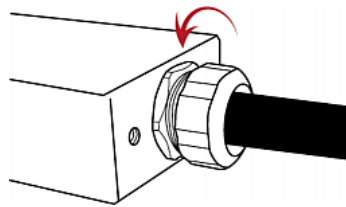
Connecting an Electrical Conduit

A conduit connector is shipped with and pre-installed on the Branch Circuit Monitor. You need to install an appropriate electrical conduit to protect your Branch Circuit Monitor's flexible cord.

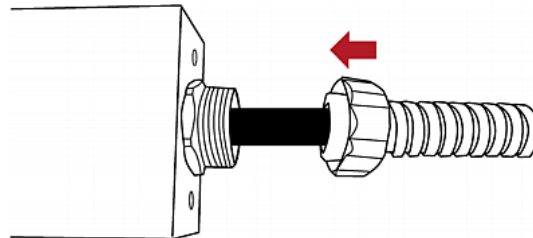
Note: Raritan does not provide the electrical conduit.

► **To attach an electrical conduit:**

1. Remove the conduit connector along with the inside plastic ring from the Branch Circuit Monitor.



2. Thread the electrical conduit through the opening of the conduit connector and the inside plastic ring.
3. Slowly thread the Branch Circuit Monitor's flexible cord into the electrical conduit.



Warning: Make sure the insulation of the flexible cord is not damaged or cut by the electrical conduit. Any damages to the insulation may result in electrical shock, fire, personal injury or death.

4. Tighten the conduit connector to the torque of 33.9 N·m (300 lbf-in).

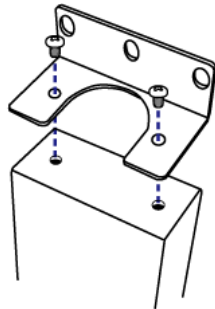
Mounting the Branch Circuit Monitor

Attach the L-brackets to the Branch Circuit Monitor so that it can be mounted on a rack or the equipment near the electrical panel that it will monitor.



► **To install L-brackets on two ends of this product:**

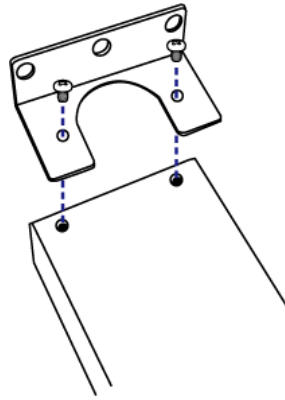
1. Attach an L-bracket to each end of the Branch Circuit Monitor with provided screws. The rackmount side of the bracket should face towards the rear of the Branch Circuit Monitor.



2. Using rack screws, fasten the Branch Circuit Monitor device to the rack through the L-brackets.

► **To install L-brackets on the rear of this product:**

1. Attach an L-bracket to two of the four screw holes on the rear of the Branch Circuit Monitor with provided screws.



2. If one L-bracket is not enough to mount this product, install an additional L-bracket on the other side of the rear panel.
3. Using rack screws, fasten the Branch Circuit Monitor device to the rack through the L-brackets.

Channel Convention

A channel on the Branch Circuit Monitor is used to monitor a circuit, which may be phase A, B or C. Channels are divided into two categories: MAINS and BRANCH CIRCUITS. MAINS channels are for monitoring the main circuits, and BRANCH CIRCUITS channels are for branch circuits.

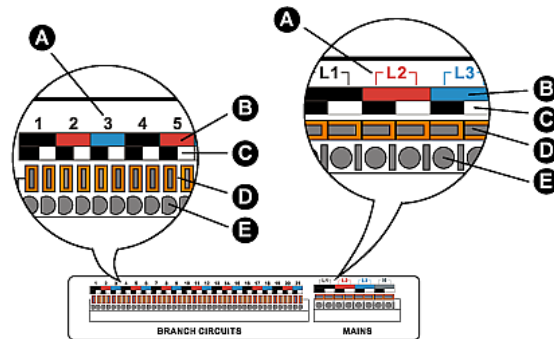
Important: Mains and branch circuits that are monitored by a Branch Circuit Monitor must belong to the same electrical panel.

A channel is identified with a number and a color. A Branch Circuit Monitor has three channel colors, which vary depending on the model you purchased. All channels marked with the same channel color are used to monitor the same phase. See the table below for which phase matches which channel color.

Phase	Black, red and blue	Brown, black and gray
A	Black	Brown
B	Red	Black
C	Blue	Gray

A channel, which is connected to a CT, comprises two CT terminals. Every CT terminal is marked with either black or white because a Raritan CT has a black lead and a white lead, and the terminal colors help indicate which CT lead to plug.

This diagram illustrates the channels on the BCM-2400 model, which uses black, red and blue channel colors.



Item	Description
A	Channel numbers.
B	Channel colors - three colors are available. Each color is used to monitor a specific phase.
C	Terminal colors - black or white. Connect a Raritan CT's black lead to a black terminal and the white lead to a white terminal.
D	Terminal buttons for controlling the springs inside the corresponding CT terminals.
E	CT terminals.

Setting Up a Power Monitoring System

Both the Branch Circuit Monitor and CTs are REQUIRED for establishing a power monitoring system on an electrical panel.

For the maximum current ratings supported by the MAINS and BRANCH CIRCUITS channels, see the nameplate or label affixed to your Branch Circuit Monitor.

The Branch Circuit Monitor contains a flexible cord containing the five wires for a 5-wire (3P+N+PE) AC connection. Make sure the electrical panel has a 3-phase branch circuit to power the Branch Circuit Monitor.

► **To set up a power monitoring system:**

1. Mount the Branch Circuit Monitor near the electrical panel that it will monitor. See **Mounting the Branch Circuit Monitor** (on page 11) for details.
2. Power OFF this electrical panel.
3. Connect the Branch Circuit Monitor to the electrical panel by wiring the 5-wire flexible cord as described below:
 - a. Connect the L1 wire to a phase A connection point in the panel.
 - b. Connect the L2 wire to a phase B connection point in the panel.
 - c. Connect the L3 wire to a phase C connection point in the panel.
 - d. Connect the N wire to the panel's neutral bus.
 - e. Connect the GND wire to the panel's ground bus.
4. Snap mains CTs onto the panel's mains circuit conductors, and then connect these CTs to the MAINS channels on the Branch Circuit Monitor. For details, see **Connecting Mains CTs** (on page 17).
 - a. Connect the phase A's CT to L1 on the Branch Circuit Monitor.
 - b. Connect the phase B's CT to L2 on the Branch Circuit Monitor.
 - c. Connect the phase C's CT to L3 on the Branch Circuit Monitor.

Note: The Branch Circuit Monitor does not support measuring the neutral bus so do NOT connect any CT to the channel labeled N.

5. Make sure the 1-pole or 3-pole circuit breakers that you want to monitor have been powered off.
6. Snap branch circuit CTs onto the conductors of these circuit breakers and connect the CTs to the BRANCH CIRCUITS channels on the Branch Circuit Monitor. For details, see **Connecting Branch Circuit CTs** (on page 19).

- Connect a phase A's CT to one of the channels for monitoring phase A on the Branch Circuit Monitor, such as channel #1, #4, #7, #10, and so on.
- Connect a phase B's CT to one of the channels for monitoring phase B on the Branch Circuit Monitor, such as channel #2, #5, #8, #11 and so on.
- Connect a phase C's CT to one of the channels for monitoring phase C on the Branch Circuit Monitor, such as channel #3, #6, #9, #12 and so on.
- For a 3-phase branch circuit connection, make sure all three CTs are connected to three consecutive channels comprising phase A, phase B and phase C in sequence. For example, all three CTs can be connected to channels #1 to #3, or #4 to #6, or #7 to #9, and the like.
- Record the panel numbers of the branch circuits and the channel numbers of CTs. This information is required for mapping the branch circuits with the Branch Circuit Monitor's channels. You can use the **Circuit Monitoring Worksheet** (on page 442) provided in the Branch Circuit Monitor User Guide to note down this information.

Warning: The Branch Circuit Monitor does not support measuring 2-pole branch circuit breakers so do not use the CT with a 2-pole breaker.

7. Use cable ties provided by Raritan to secure CT leads in place, and make sure the CT leads do not touch any wire terminals on the electrical panel.
8. Verify that all CTs have been properly connected to the Branch Circuit Monitor.
9. Power ON the electrical panel, and verify all circuit breakers where the Branch Circuit Monitor is connected and CTs are snapped are also switched on.

Important: You must log in to the web interface to enter correct information for these CTs, such as CT ratings or turns ratio. Otherwise the Branch Circuit Monitor may generate incorrect measurements. See *Configuring the Mains Channels* (on page 129) and *Configuring the Branch Circuit Channels* (on page 130) in the Branch Circuit Monitor User Guide

Raritan Current Transformers (Optional)

A current transformer (CT) can detect the current of the circuit conductor that passes through it and transmit the data to the Branch Circuit Monitor where it is connected.

Raritan provides different CTs with different ratings. The CTs are categorized into two types: mains CTs and branch circuit CTs. Both types are split-core CTs.

- Raritan mains CTs are for measuring main circuits rated up to 200A, 250A or higher. Contact Raritan Technical Support for additional information.
- Raritan branch circuit CTs are for branch circuits rated up to 60A or 100A.

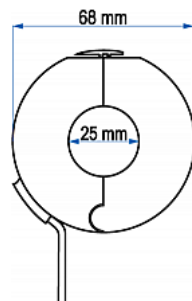
The Raritan CT has two leads to connect to two CT terminals of any channel on the Branch Circuit Monitor.

Warning: Do NOT use mains CTs to measure branch circuits or use branch circuit CTs to measure mains circuits. This is because the mains CTs must have built-in burden resistors but the branch circuit CTs must not have built-in burden resistors.

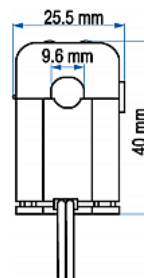
CT Dimensions

Sizes of different Raritan CTs are different.

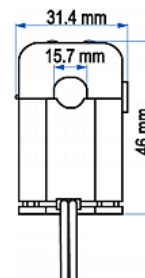
**Mains CT
rated at 200A or
250A**



**Branch circuit
CT rated at 60A**

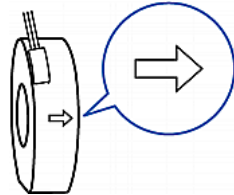


**Branch circuit
CT rated at 100A**



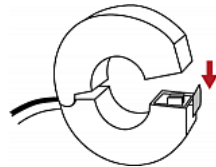
Connecting Mains CTs

When snapping the CT onto a circuit conductor, make sure the CT's arrow mark points towards the load. The arrow mark of a mains CT is located on the CT's side. Note that this arrow is NOT the one shown on the CT's release tab.

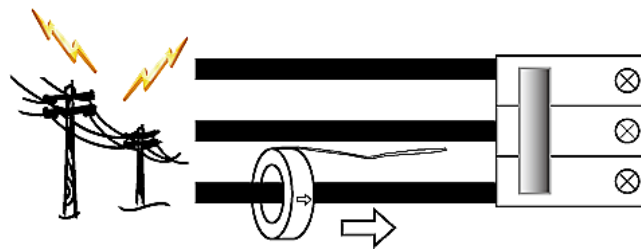


► To connect mains CTs:

1. Make sure the electrical panel has been powered off.
2. Open the CT by unlocking its release tab. An arrow marked on the release tab indicates the direction to open the mains CT.

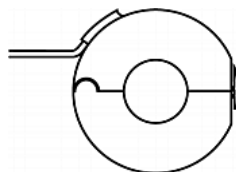


3. Slip the CT over the panel's mains phase A conductor and snap it.
 - Make sure the CT's arrow direction is the same as the following illustration.

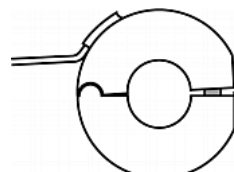


- Close the CT's release tab properly.

Proper



Improper

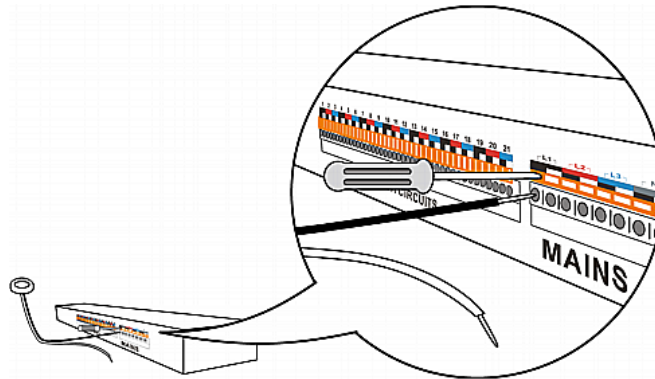


4. Strip the insulation of the CT leads around 6mm from the end.

5. Connect the CT leads to the corresponding CT terminals on the Branch Circuit Monitor.
 - a. Locate the L1 channel on the Branch Circuit Monitor.

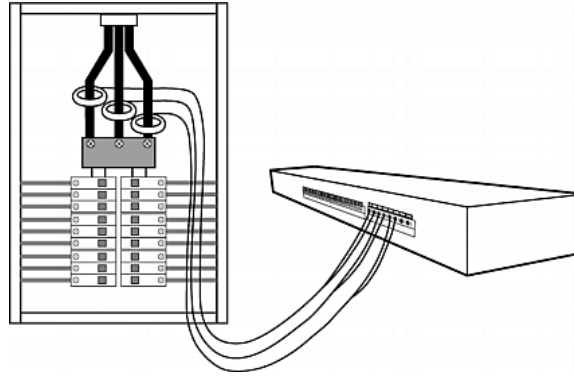
The channel comprises two CT terminals - one is black and the other is white.
 - b. Use a small flat head screwdriver to press and hold down the button above the black CT terminal.
 - c. Plug the CT's black lead into the black CT terminal.

*Important: The CT lead must be plugged into the CT terminal that has the same color. Otherwise, the CT signals are reversed and the Branch Circuit Monitor incorrectly measures the current values. See **Channel Convention** (on page 12) for terminal colors.*



- d. Release the button. Verify that the CT's black lead is securely fastened.
 - e. Repeat the above steps to plug the CT's white lead into the white CT terminal of the same channel.
6. Repeat the same steps to snap a mains CT onto the panel's mains phase B conductor and connect the CT to the L2 channel of the MAINS channel group on the Branch Circuit Monitor.

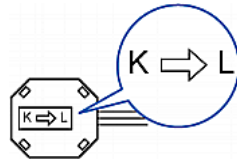
7. Repeat the same steps to snap a mains CT onto the panel's mains phase C conductor and connect the CT to the L3 channel of the MAINS channel group on the Branch Circuit Monitor.



Note: The Branch Circuit Monitor does not support measuring the neutral bus so do NOT connect any CT to the channel labeled N.

Connecting Branch Circuit CTs

When snapping the CT onto a circuit conductor, make sure the CT's arrow mark points towards the load. The arrow mark of a Raritan branch circuit CT is located on the bottom.



► To connect branch circuit CTs:

1. Make sure the 1-pole or 3-pole circuit breaker(s) where the branch circuit CTs will monitor are powered OFF.

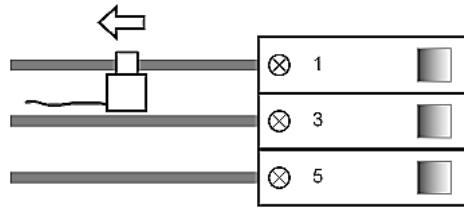
Warning: The Branch Circuit Monitor does not support measuring 2-pole branch circuit breakers so do not use the CT with a 2-pole breaker.

2. Open the CT by unlocking its release tab.



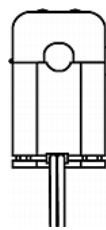
3. Slip the CT over the circuit breaker's phase A conductor and snap it.

- Make sure the CT's arrow direction is the same as the following illustration.

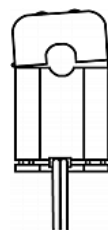


- Close the CT's release tab properly.

Proper



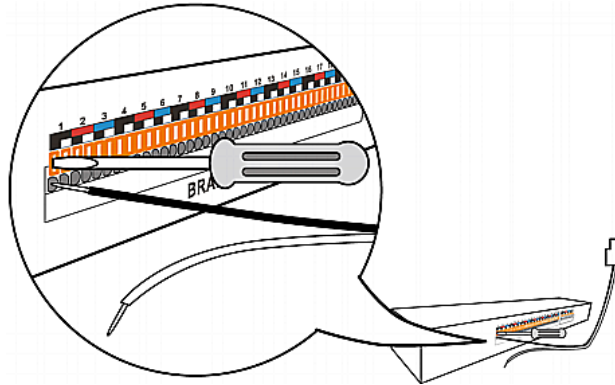
Improper



4. Strip the insulation of the CT leads around 6mm from the end.
5. Connect the CT leads to the corresponding CT terminals on the Branch Circuit Monitor.
 - a. Locate one of the Branch Circuit channels for monitoring phase A on the Branch Circuit Monitor. See **Channel Convention** (on page 12) for information on identifying a channel.

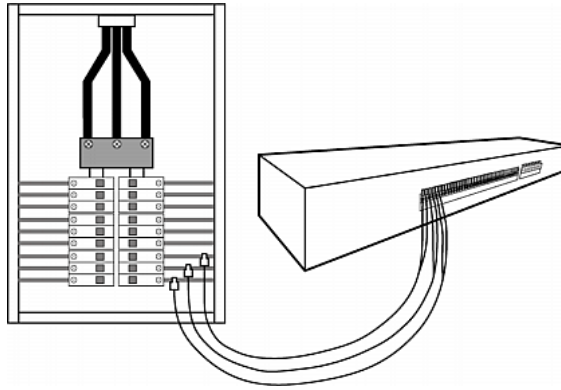
The channel comprises two CT terminals - one is black and the other is white.
 - b. Use a small flat head screwdriver to press and hold down the button above the black CT terminal.
 - c. Plug the CT's black lead into the black CT terminal.

*Important: The CT lead must be plugged into the CT terminal that has the same color. Otherwise, the CT signals are reversed and the Branch Circuit Monitor incorrectly measures the current values. See **Channel Convention** (on page 12) for terminal colors.*



- d. Release the button. Verify that the CT's black lead is securely fastened.
- e. Repeat the above steps to plug the CT's white lead into the white CT terminal of the same channel.
6. Repeat the same steps to snap a branch circuit CT onto the circuit breaker's phase B conductor, and connect the CT to one of the channels for monitoring phase B on the Branch Circuit Monitor.
 - For a 3-phase branch circuit connection, the phase B channel chosen must be next to the phase A channel. For example, if the phase A's CT is connected to the channel #4, the phase B channel must be the channel #5.
7. Repeat the same steps to snap a branch circuit CT onto the circuit breaker's phase C conductor, and connect the CT to one of the channels for monitoring phase C on the Branch Circuit Monitor.

- For a 3-phase branch circuit connection, the phase C channel chosen must be next to the phase B channel. For example, if the phase B's CT is connected to the channel #5, the phase C channel must be the channel #6.



8. Power on this circuit breaker.
9. To monitor additional branch circuits, repeat the above steps to snap branch circuit CTs onto other circuit breaker conductors, and connect these CTs to the remaining channels on the Branch Circuit Monitor.

Configuring the Branch Circuit Monitor

There are two ways to initially configure a Branch Circuit Monitor device:

- Connect the Branch Circuit Monitor device to a computer to configure it, using a serial or USB connection between the Branch Circuit Monitor and the computer.

The computer must have a communications program such as HyperTerminal or PuTTY.

For a serial connection, you need a null-modem cable with DB9 connectors on both ends (Raritan part number: 254-01-0006-00).

- Connect the Branch Circuit Monitor device to a TCP/IP network that supports DHCP, and use the IPv4 address and web browser to configure the Branch Circuit Monitor.

The IP address can be retrieved by operating the LCD display of the Branch Circuit Monitor. See **IP Address** (on page 77).

A Category 5e/6 UTP cable is required for a wired network connection.

Connecting the Branch Circuit Monitor to a Computer

To configure the Branch Circuit Monitor using a computer, it must be connected to the computer with an RS-232 serial interface. The computer must have a communications program such as HyperTerminal or PuTTY.

If your computer does not have a serial RS-232 port, use a regular USB cable to connect the Branch Circuit Monitor to the computer for initial configuration. The Branch Circuit Monitor device can emulate a serial port after the USB-to-serial driver is properly installed in the Windows® operating system.

Note: Not all serial-to-USB converters work properly with the Branch Circuit Monitor device so this section does not introduce the use of such converters.

Connect the Branch Circuit Monitor to a computer for initial configuration by following either of the procedures below.

► **To make a serial RS-232 connection:**

- Connect one end of the null-modem cable to the male RS-232 port labeled CONSOLE / MODEM on the Branch Circuit Monitor, and the other end to the serial port (COM) on a computer.

► **To make a 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 24).
2. Connect a USB cable between the Branch Circuit Monitor appliance's USB-B port and the computer's USB-A port.

Installing the USB-to-Serial Driver (Optional)

The Branch Circuit Monitor can emulate a USB-to-serial converter over a USB connection. A USB-to-serial driver named "Dominion Branch Circuit Monitor Serial Console" is required for Microsoft® Windows® operating systems.

Download the USB Driver file, which 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.

Note: This file is downloaded from the Raritan **PX2 Support Files page** (<https://www.raritan.com/support/product/px2/px2-support-files>).

► Automatic driver installation in Windows®:

1. Make sure the Branch Circuit Monitor 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 Branch Circuit Monitor to the computer via a USB cable. The driver is automatically installed.

Note: Manually install the driver only if the automatic installation fails. See the section titled "Installing the USB-to-Serial Driver (Optional)" in the online help for manual installation procedure.

► 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 Branch Circuit Monitor 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
```

Connecting the Branch Circuit Monitor to Your Network

To use the web interface to administer the Branch Circuit Monitor, you must connect the Branch Circuit Monitor to your local area network (LAN). The Branch Circuit Monitor can be connected to a wired or wireless network.

► **To make a wired connection:**

1. Connect a standard network patch cable to the ETHERNET port on the Branch Circuit Monitor.
2. Connect the other end of the cable to your LAN.

► **To make a wireless connection:**

Do one of the following:

- Plug a supported USB wireless LAN adapter into the USB-A port on your Branch Circuit Monitor.
- Connect a USB docking station to the USB-A port on the Branch Circuit Monitor and plug the supported USB wireless LAN adapter into the appropriate USB port on the docking station.

See **USB Wireless LAN Adapters** (on page 25) for a list of supported wireless LAN adapters.

USB Wireless LAN Adapters

The following table lists USB wireless LAN adapters that the Branch Circuit Monitor supports.

Wi-Fi LAN adapter	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 Branch Circuit Monitor matches the access point. The following is the wireless LAN configuration that the Branch Circuit Monitor 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: Raritan only supports specific wireless LAN adapters.

Supported 802.11 network protocols vary according to the wireless LAN adapter being used with the Branch Circuit Monitor. See *USB Wireless LAN Adapters* (on page 25).

Initial Network Configuration via CLI

After the Branch Circuit Monitor is connected to your network, you must provide it with an IP address and some additional networking information.

This section describes the initial configuration via a serial RS-232 or USB connection.

► To configure the Branch Circuit Monitor device:

1. On the computer connected to the Branch Circuit Monitor, open a communications program such as HyperTerminal or PuTTY.
2. Select the appropriate COM port, and set the following port settings:
 - 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 "Dominion PX2 Serial Console" under the Ports group.

3. In the communications program, press Enter to send a carriage return to the Branch Circuit Monitor.
4. The Branch Circuit Monitor prompts you to log in. Both user name and password are case sensitive.
 - a. Username: `admin`
 - b. Password: `raritan` (or a new password if you have changed it).
5. If prompted to change the default password, follow onscreen instructions to type your new password.
6. The # prompt appears.
7. Type `config` and press Enter.
8. To configure network settings, type appropriate commands and press Enter. All commands are case sensitive.
 - a. To set the networking mode, type this command:


```
network mode <mode>
```

 where `<mode>` is *wired* (default) or *wireless*.
 - b. For the wired network mode, you may configure the LAN interface settings. In most scenarios, the default setting (auto) works well and should not be changed unless required.

To set	Use this command
LAN interface speed	<pre>network interface LANInterfaceSpeed <option></pre> <p><code><option></code> = <i>auto</i>, <i>10Mbps</i>, or <i>100Mbps</i>.</p>
LAN interface duplex mode	<pre>network interface LANInterfaceDuplexMode <mode></pre> <p><code><mode></code> = <i>half</i>, <i>full</i> or <i>auto</i>.</p>

Tip: You can combine multiple commands to configure multiple parameters at a time. For example,

*network interface LANInterfaceSpeed <option>
LANInterfaceDuplexMode <mode>*

- c. For the wireless network mode, you must configure the Service Set Identifier (SSID) parameter.

To set	Use this command
SSID	<pre>network wireless SSID <ssid></pre> <p><code><ssid></code> = SSID string</p>

If necessary, configure more wireless parameters shown in the following table.

To set	Use this command
BSSID	network wireless BSSID <bssid> <bssid> = AP MAC address or <i>none</i>
Authentication method	network wireless authMethod <method> <method> = <i>psk</i> or <i>eap</i>
PSK	network wireless PSK <psk> <psk> = PSK string
EAP outer authentication	network wireless eapOuterAuthentication <outer_auth> <outer_auth> = <i>PEAP</i>
EAP inner authentication	network wireless eapInnerAuthentication <inner_auth> <inner_auth> = <i>MSCHAPv2</i>
EAP identity	network wireless eapIdentity <identity> <identity> = your user name for EAP authentication
EAP password	network wireless eapPassword When prompted to enter the password for EAP authentication, type the password.
EAP CA certificate	network wireless eapCACertificate When prompted to enter the CA certificate, open the certificate with a text editor, copy and paste the content into the communications program.

The content to be copied from the CA certificate does NOT include the first line containing "BEGIN CERTIFICATE" and the final line containing "END CERTIFICATE." If a certificate is installed, configure the following:

Whether to	Use this command
Verify the certificate	<pre>network wireless enableCertVerification <option1></pre> <p><i><option1> = true or false</i></p>
Accept an expired or not valid certificate	<pre>network wireless allowOffTimeRangeCerts <option2></pre> <p><i><option2> = true or false</i></p>
Make the connection successful by ignoring the "incorrect" system time	<pre>network wireless allowConnectionWithIncorrectC lock <option3></pre> <p><i><option3> = true or false</i></p>

- d. To determine which IP protocol (IPv4 or IPv6) is enabled and which IP address (IPv4 or IPv6) returned by the DNS server is used, configure the following parameters.

To set	Use this command
IP protocol	<pre>network ip proto <protocol></pre> <p><i><protocol> = v4Only, v6Only or both</i></p>
IP address returned by the DNS server	<pre>network ip dnsResolverPreference <resolver></pre> <p><i><resolver> = preferV4 or preferV6</i></p>

- e. After enabling the IPv4 or IPv6 protocol in the earlier step, configure the IPv4 or IPv6 network parameters.

To set	Use this command
IPv4 configuration method	<pre>network ipv4 ipConfigurationMode <mode></pre> <p><i><mode> = dhcp (default) or static</i></p>

To set	Use this command
IPv6 configuration method	<pre>network ipv6 ipConfigurationMode <mode></pre> <p><mode> = <i>automatic</i> (default) or <i>static</i></p>

- Configure the preferred host name for the IPv4 DHCP or IPv6 automatic configuration.

Note: The <version> variable in all of the following commands is either ipv4 or ipv6, depending on the type of the IP protocol you have enabled.

To set	Use this command
Preferred host name (optional)	<pre>network <version> preferredHostName <name></pre> <p><name> = preferred host name</p>

Tip: To override the DHCP-assigned DNS servers with those you specify manually, type this command:

```
network <version> overrideDNS <option>
```

where <option> is *enable* or *disable*. See the table below for the commands for manually specifying DNS servers.

- For static IP configuration, configure these parameters.

To set	Use this command
Static IPv4 or IPv6 address	<pre>network <version> ipAddress <ip address></pre> <p><ip address> = static IP address</p>
IPv4 subnet mask	<pre>network ipv4 subnetMask <netmask></pre> <p><netmask> = subnet mask</p>
IPv4 or IPv6 gateway	<pre>network <version> gateway <ip address></pre> <p><ip address> = gateway's IP address</p>

To set	Use this command
IPv4 or IPv6 primary DNS server	network <version> primaryDNSServer <ip address> <ip address> = IP address of the primary DNS server
IPv4 or IPv6 secondary DNS server (optional)	network <version> secondaryDNSServer <ip address> <ip address> = IP address of the secondary DNS server

9. To quit the configuration mode, type either of the following commands, and press Enter.

Command	Description
apply	Save all configuration changes and exit.
cancel	Abort all configuration changes and exit.

The # prompt appears, indicating that you have quit the configuration mode.

10. To verify whether all settings are correct, type the following commands one by one.

Command	Description
show network	Show network parameters.
show network ip all	Show all IP configuration parameters.
show network wireless details	Show all wireless parameters.

Tip: You can type "shownetwork wireless" to display a shortened version of wireless settings.

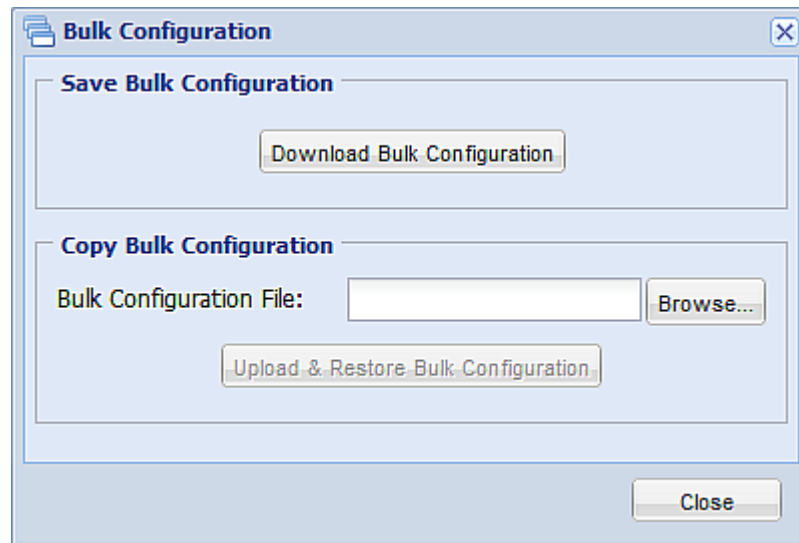
11. If all are correct, type `exit` to log out of the Branch Circuit Monitor. If any are incorrect, repeat Steps 7 to 10 to change network settings.

The IP address configured may take seconds to take effect.

Bulk Configuration

The Bulk Configuration feature lets you save the settings of a configured Branch Circuit Monitor device to your PC. You can use this configuration file to copy that configuration to other Branch Circuit Monitor devices of the same model and firmware version.

You must have the administrator privileges to save and copy the Branch Circuit Monitor 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 Branch Circuit Monitor device's all settings, use the Backup/Restore feature instead. See **Backup and Restore of Branch Circuit Monitor Device Settings** (on page 262).*

Saving a Branch Circuit Monitor Configuration

A source device is an already configured Branch Circuit Monitor device that is used to create a configuration file containing the settings that can be shared between Branch Circuit Monitor 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
- Mains channel name
- Branch circuit channel names
- Environmental sensor names
- Environmental sensor states and values
- SSL certificate

Because the date and time settings are saved in the configuration file, users should exercise caution when distributing the configuration file to the Branch Circuit Monitor 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 Branch Circuit Monitor Configuration

A target device is the Branch Circuit Monitor device that loads another Branch Circuit Monitor device's configuration file.

Copying a source Branch Circuit Monitor device's configuration to a target device adjusts the target Branch Circuit Monitor device's settings to match those of the source Branch Circuit Monitor device. In order to successfully copy a source Branch Circuit Monitor device's configuration:

- The user must be the Admin user. Or the Admin role is assigned to the user.
- The target Branch Circuit Monitor device must be running the same firmware version as the source Branch Circuit Monitor device.
- The target Branch Circuit Monitor device must be of the same model type as the source Branch Circuit Monitor device.

► **To copy a Branch Circuit Monitor 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 258).
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 Branch Circuit Monitor device resets and the Login page re-appears, indicating that the configuration copy is complete.

Note: On startup, the Branch Circuit Monitor 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.

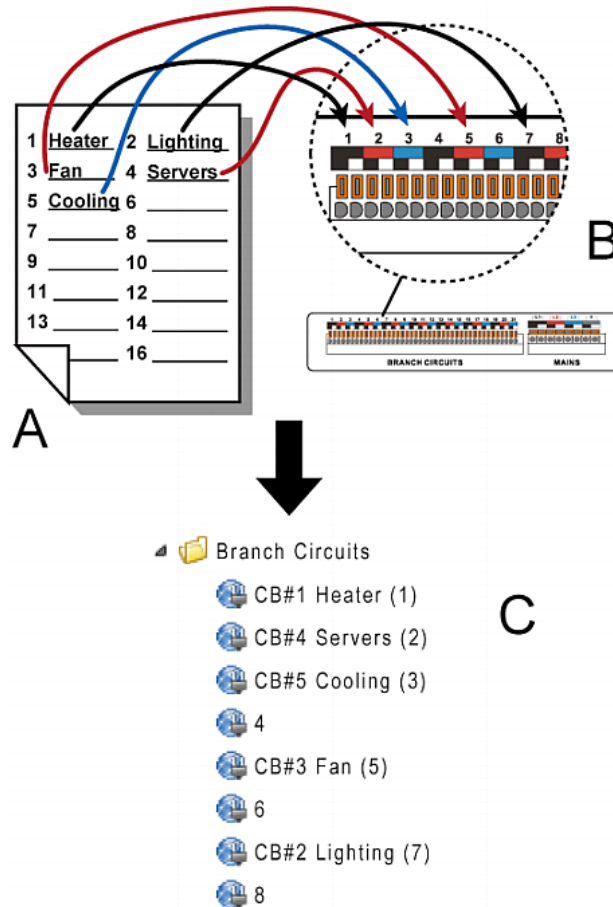
Mapping Channels with Branch Circuits

The best way to identify the branch circuit each channel is to customize the channel names in the web interface. A hard copy worksheet documenting the use of each branch circuit is usually affixed to the electrical panel. It is strongly recommended to contain this worksheet information when assigning the channel names.

► To map channels with monitored branch circuits:

1. You should have noted down every branch circuit's panel number and every CT's channel number in the procedure of **Setting Up a Power Monitoring System** (on page 14). If not yet, collect this information now.
2. Locate the electrical panel's worksheet, which is usually available on the panel's cover.
3. Log in to the web interface of the Branch Circuit Monitor. See **Login** (on page 80) in the User Guide.
4. Click the BCM folder in the navigation tree and then click Setup Circuits to configure branch circuits as single-phase or 3-phase circuits. See **Configuring the Branch Circuit Channels** (on page 130) in the User Guide.
5. Change the channel names according to the channel-mapping information and the panel's worksheet.
 - a. Click the desired channel in the navigation tree.
 - When there are no names assigned, a channel shows the channel number only.
 - For a 3-phase branch circuit, the channel number contains 3 numbers that are indicated with a dash, such as 1-3, 4-6, 7-9, 10-12 and so on.
 - b. Click Setup on the channel page to the right.
 - c. Type a name in the Name field. After assigning a channel name, the channel number is enclosed in parentheses, following the channel name.

Raritan strongly suggests including both of the panel number and the branch circuit's usage in the channel name. For example, if a CT attached to the branch circuit #2 (phase A) is connected to the channel #7 on the Branch Circuit Monitor and the panel worksheet indicates that the branch circuit #2 is used to power the lighting system, then you can name the channel 7 as "CB#2 Lighting."



Item	Description
A	Electrical panel's worksheet
B	Channels on the Branch Circuit Monitor
C	Channels shown in the web interface with customized channel names for channels #1, #2, #3, #5, and #7

Cascading the Branch Circuit Monitor via USB

Up to eight (8) Raritan devices are supported as part of a daisy chain. This daisy chain feature permits multiple Branch Circuit Monitor devices to be cascaded using USB cables, sharing the Ethernet connectivity accordingly. Different models can be cascaded as long as they are running a supported 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*. Therefore, you can access any device in the chain via the Web, SNMP, SSH, Telnet or Modbus interface.

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

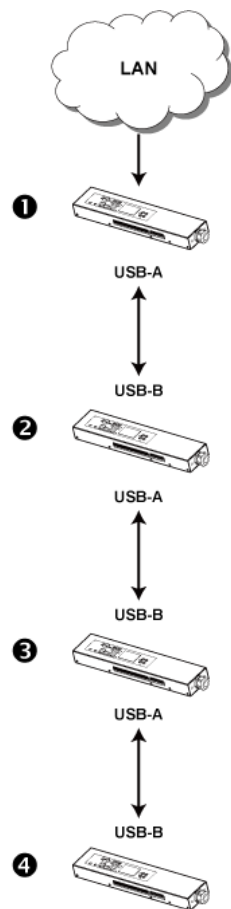
- The bridging mode supports the *wired* networking only.
- The port forwarding mode supports both the *wired* and *wireless* networking.

► To cascade the Branch Circuit Monitor devices via USB:

1. Verify that the Branch Circuit Monitor devices to be cascaded are running the following firmware version by choosing Maintenance > Device Information in the web interface or using CLI's `show bcm` command. If not, upgrade these devices. See **Updating the Branch Circuit Monitor Firmware** (on page 258).
 - Branch Circuit Monitor: version 2.3.1 or later
2. Select one of the devices as the master device.
 - When the port forwarding mode over wireless LAN is intended, a Raritan product with two USB-A ports must be the master device, such as PX3 or PX3TS.
3. 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 25).
4. Connect the USB-A port of the master device to the USB-B port of an additional Branch Circuit Monitor via a USB cable. This additional device is Slave 1.
5. Connect Slave 1's USB-A port to the USB-B port of an additional Branch Circuit Monitor via a USB cable. The second additional device is Slave 2.

6. Repeat the above 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, no connection of any standard network patch cable or USB wireless LAN adapter to the slave devices.
7. Log in to the master device to configure the cascading mode for this USB-cascading configuration. See Setting the Cascading Mode or **Configuring the Cascading Mode** (on page 392).
8. Configure the master and/or each slave device's networking settings.
- Bridging mode: Configure each cascaded device's network settings respectively.
- Port forwarding mode: Only the mater device's network settings must be configured.



Number	Device role
1	Master device

Number	Device role
②	Slave 1
③	Slave 2
④	Slave 3

Note: To remotely identify the master and slave devices and their positions in the USB-cascading configuration, see **Identifying Cascaded Devices** (on page 99).

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. For details, see the USB-Cascading Solution Guide, which is available on the **PX2 web page** (<http://www.raritan.com/support/product/px2/>).

Chapter 3

Connecting External Equipment
(Optional)

More features are available in addition to remotely monitoring and managing the Branch Circuit Monitor if you connect Raritan's or third-party external equipment to your Branch Circuit Monitor.

In This Chapter

Connecting Environmental Sensor Packages	40
Connecting a Logitech Webcam	61
Connecting a GSM Modem	62
Connecting an Analog Modem	62
Connecting an External Beeper	63
Connecting an RF Code PDU Sensor Tag.....	63

Connecting Environmental Sensor Packages

The Branch Circuit Monitor supports all types of Raritan environmental sensor packages, including DPX, DPX2 and DX series. For detailed information on each sensor package, refer to the Environmental Sensors Guide or Online Help on Raritan website's **PX2 Support Files page** (<https://www.raritan.com/support/product/px2/px2-support-files>).

The Branch Circuit Monitor supports a maximum of 32 managed sensors or actuators.

For information on connecting DPX packages, see DPX Sensor Packages.

For information on connecting DPX2 packages, see DPX2 Sensor Packages.

For information on connecting DX packages, see DX Sensor Packages.

DPX Sensor Packages

DPX sensors are first generation environmental sensors that are connected directly to the Branch Circuit Monitor SENSOR port or to the SENSOR port via a Raritan hub.

For more details on DX sensors, download the **Environmental Sensors Guide** from *Raritan's website*
<https://www.raritan.com/support/product/px2>.

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 for further illustrations.

DPX sensors cannot be daisy chained.

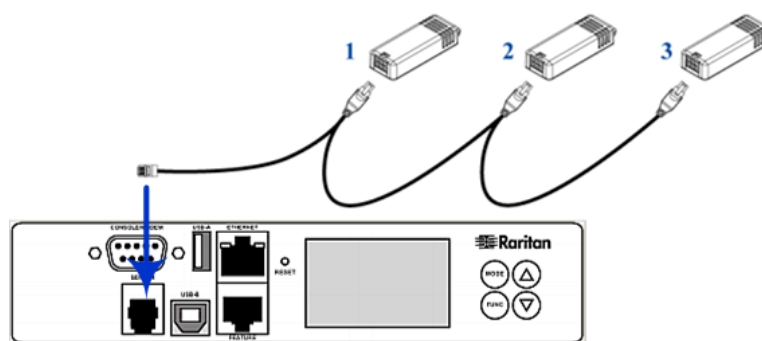
Once connected to Branch Circuit Monitor, the DPX port number is detected but DPX sensor packages do not provide chain position information.

The port number is available in the Branch Circuit Monitor web interface, and can be viewed in the Branch Circuit Monitor LCD display (see **Operating the LCD Display** (on page 71)).

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

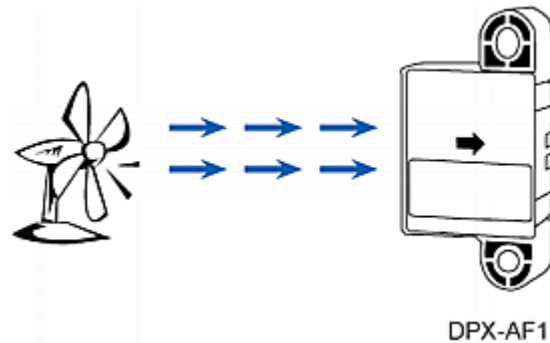
► To connect DPX environmental sensors directly to the Branch Circuit Monitor:

- Plug the DPX sensor into an RJ-12 SENSOR port on the Branch Circuit Monitor device using the Raritan-provided phone cable.



1	The Branch Circuit Monitor device
2	Raritan-provided phone cable
3	Raritan environmental sensor

If a DPX air flow sensor (DPX-AF1) is connected, make sure the sensor faces the source of the wind (such as a fan) in the appropriate orientation as indicated by the arrow on that sensor.



Connect a DPX Using an Optional Sensor Hub

Optionally, you can connect a Raritan sensor hub to the Branch Circuit Monitor. This allows you to connect up to four (4) DPX sensors to the Branch Circuit Monitor via the hub.

The Raritan sensor hub supports DPX sensor packages only. Do NOT connect DPX2 or DX sensor packages to the hub.

Raritan sensor hubs CANNOT be cascaded. You can only connect one sensor hub to each Branch Circuit Monitor SENSOR port.

► To connect DPX environmental sensors via an optional sensor hub:

1. Plug one end of the Raritan-provided RJ-12 cable into the SENSOR port on the Branch Circuit Monitor device.
2. Connect the other end to the RJ-12 cable into the IN port (Port 1) of the hub.

3. Connect the DPX environmental sensor(s) to any of the four OUT ports on the hub.



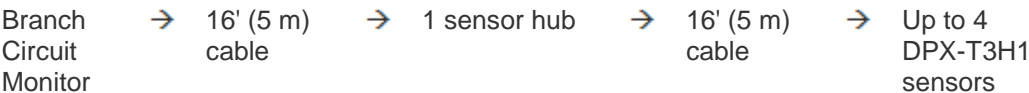
(A)	The Branch Circuit Monitor device
(B)	Raritan-provided 4-wire, 6-pin RJ-12 cable
(C)	Raritan sensor hub
(D)	Raritan environmental sensors

Supported Maximum DPX Sensor Distances

A maximum connection distance of 98' (30 m) is supported when connecting the following DPX sensor packages to the Branch Circuit Monitor. 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 Branch Circuit Monitor via a sensor hub:

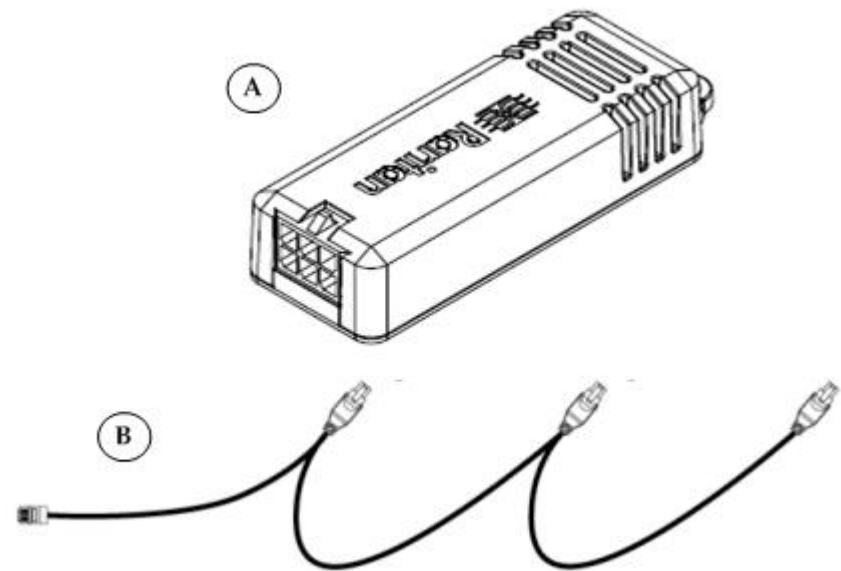


Branch Circuit Monitor	→	50' (15 m) cable	→	1 sensor hub	→	16' (5 m) cable	→	Up to 4 DPX-T3H1 sensors
Branch Circuit Monitor	→	82' (25 m) cable	→	1 sensor hub	→	16' (5 m) cable	→	Up to 4 DPX-T3H1 sensors

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 need to manually connect DPX2 sensors to the sensor cable.

For more information on DPX2 sensor packages, download the Environmental Sensors Guide from Raritan website's **PX2 Support Files** page (<https://www.raritan.com/support/product/px2/px2-support-files>).



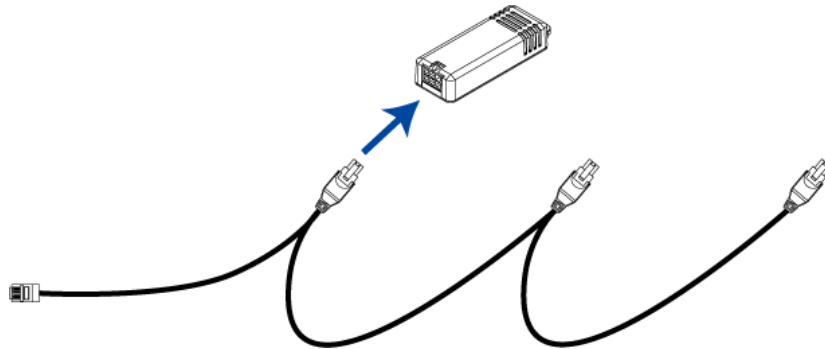
A	DPX2 sensor
B	DPX2 sensor cable with one RJ-12 connector and three head connectors

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

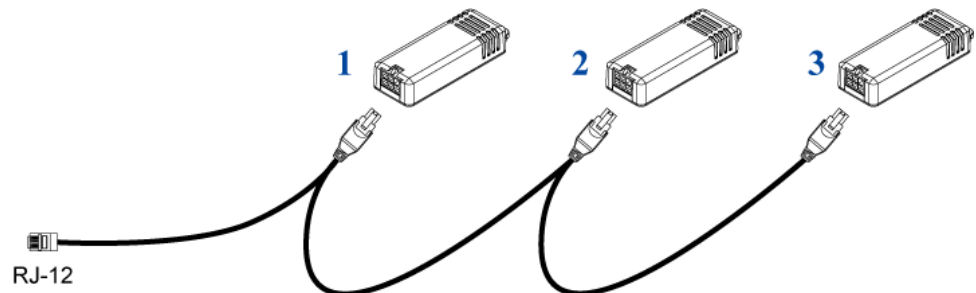
Warning: If there are free head connectors between a DPX2 sensor cable's RJ-12 connector and the final attached DPX2 sensor, the sensors following the free head connector(s) on the same cable do NOT work properly. Therefore, always occupy all head connectors prior to the final sensor with a DPX2 sensor.

► **To connect a DPX2 sensor package to the Branch Circuit Monitor:**

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

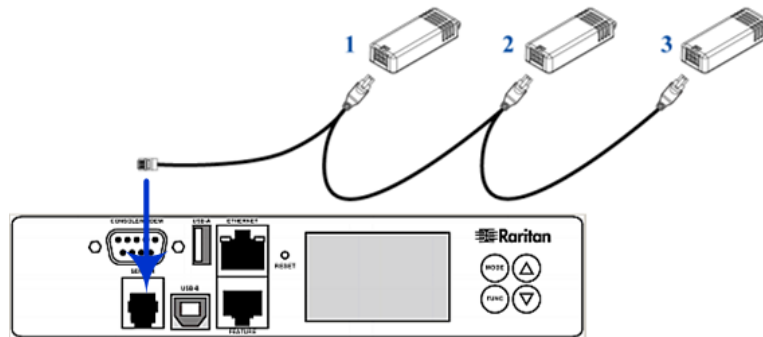


2. Connect remaining DPX2 sensors to the second and then the third head connector.



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 attached.

3. Plug the RJ-12 connector of the DPX2 sensor cable into a RJ-12 SENSOR port on the Branch Circuit Monitor.



DX Sensor Packages

Most DX sensor packages contain terminals for connecting detectors or actuators. For more details on the DX sensors, and for information on connecting actuators or detectors to DX terminals, download the **Environmental Sensors Guide** from **Raritan's website** <https://www.raritan.com/support/product/px2>.

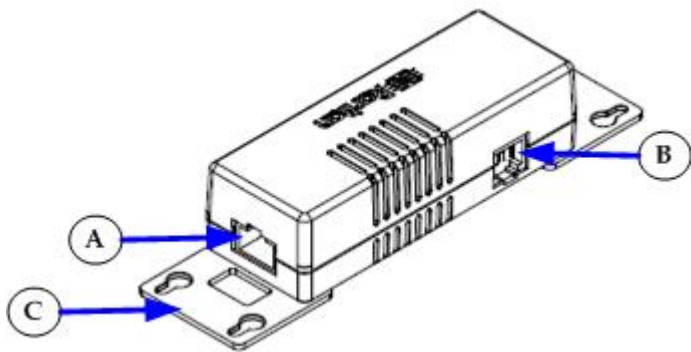
You can cascade up to 12 DX sensor packages.

When cascading DX, remember that the Branch Circuit Monitor only supports a maximum of 32 sensors or actuators.

If there are more than 32 sensors and/or actuators connected, every sensor and/or actuator after the 32nd one is ignored by Branch Circuit Monitor.

For example, if you cascade 12 DX packages, and each package contains 3 functions (a function is a sensor or actuator), Branch Circuit Monitor ignores the last 4 functions because the total 36 (12*3=36) exceeds 32 by 4.

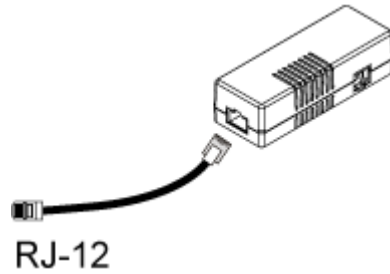
*Tip: To manage the last 4 functions, you can release 4 sensors or actuators that have been under management, and then manually bring the last 4 functions into management. See **Unmanaging Environmental Sensors or Actuators** (see "Unmanaging Environmental Sensors" on page 241) and **Managing Environmental Sensors or Actuators** (see "Managing Environmental Sensors and Actuators" on page 229).*



Components	
(A)	RJ-45 ports, each of which is located on either end of a DX sensor package.
(B)	RJ-12 port, which is reserved for future use.
(C)	Removable rackmount brackets.

► **To connect an RJ-12 to RJ-45 adapter cable to a DX sensor package.**

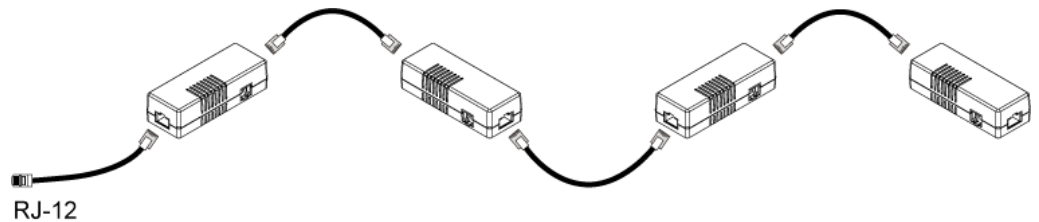
- Use an RJ-12 cable to connect the adapter's RJ-45 connector to one of the RJ-45 ports of the DX sensor package.



► **To cascade DX packages:**

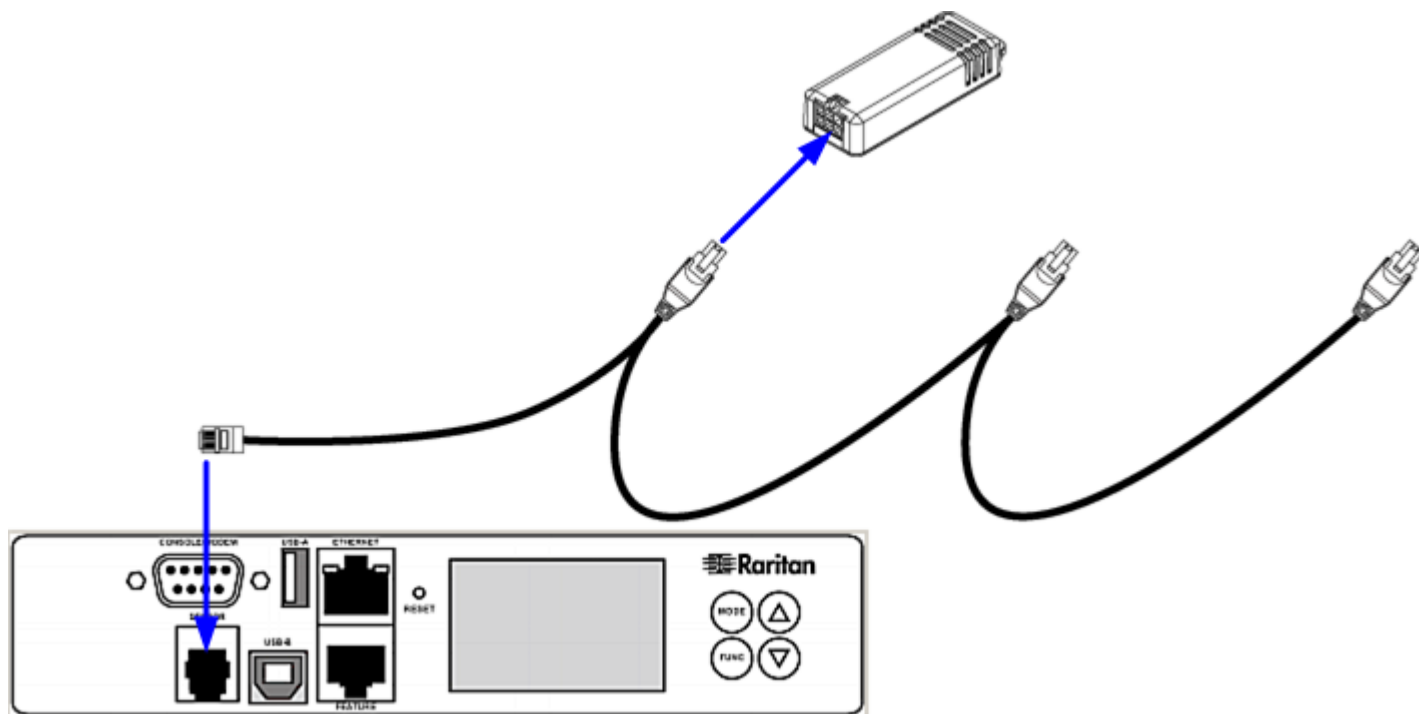
- Connect the DX packages through their RJ-45 ports using a standard network patch cable (CAT5 or higher).

Repeat the same steps to cascade more DX packages.



► **To connect the DX to the Branch Circuit Monitor, connect the first DX sensor package to the Branch Circuit Monitor:**

1. Plug the adapter cable's RJ-12 connector into a RJ-12 SENSOR port of the Branch Circuit Monitor.



2. If needed, connect a DPX2 sensor package to the end of the DX chain. See **Connecting a DPX2 Sensor Package to DX** (on page 50).

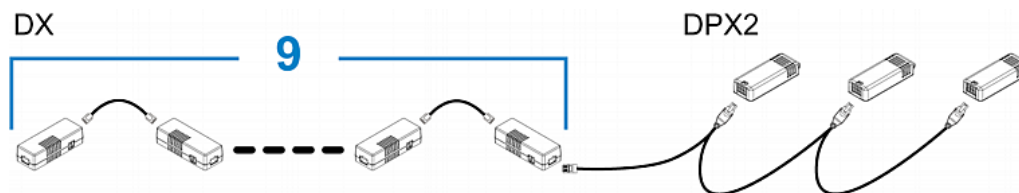
Connecting a DPX2 Sensor Package to DX

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.

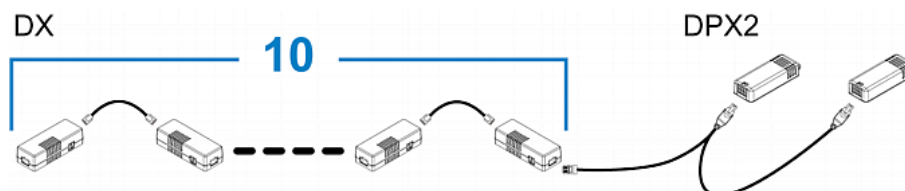
► **When connecting a DPX2 sensor package containing three DPX2 sensors:**

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



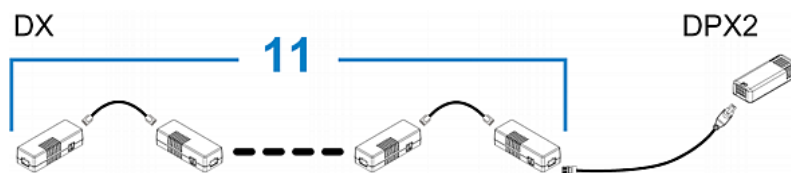
► **When connecting a DPX2 sensor package containing two DPX2 sensors:**

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



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

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



Connecting the Asset Management Sensor

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 Branch Circuit Monitor 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 Branch Circuit Monitor.
- Raritan asset tags: An asset tag is adhered to an IT device. The asset tag uses an electronic ID to identify and locate the device.

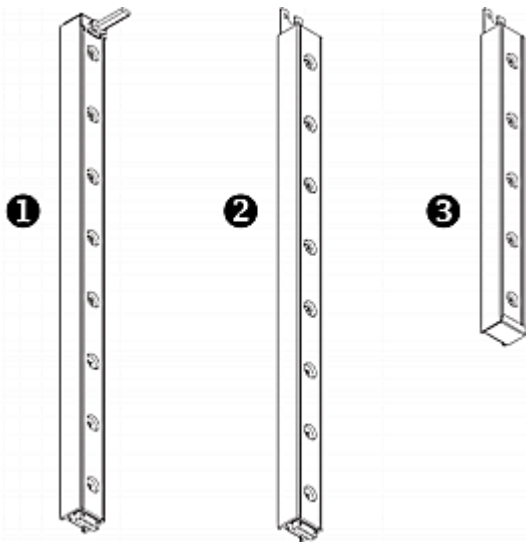
Combining Asset Sensors

Each tag port on the asset sensor corresponds to a rack unit and can be used to locate IT devices on 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.

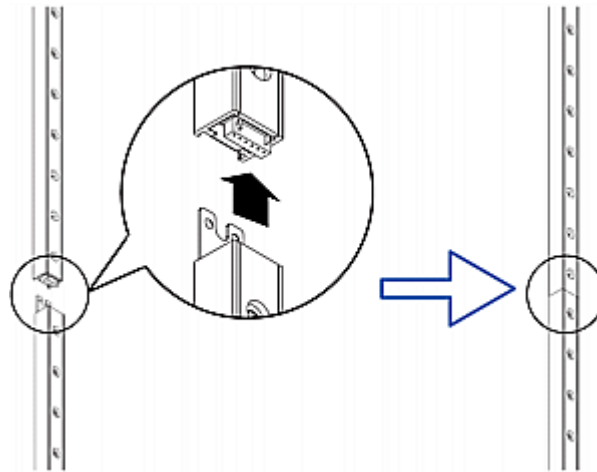


①	8U MASTER asset sensor with 8 tag ports
②	8U SLAVE asset sensor with 8 tag ports
③	5U "ending" SLAVE asset sensor with 5 tag ports

Note: Unlike regular 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.

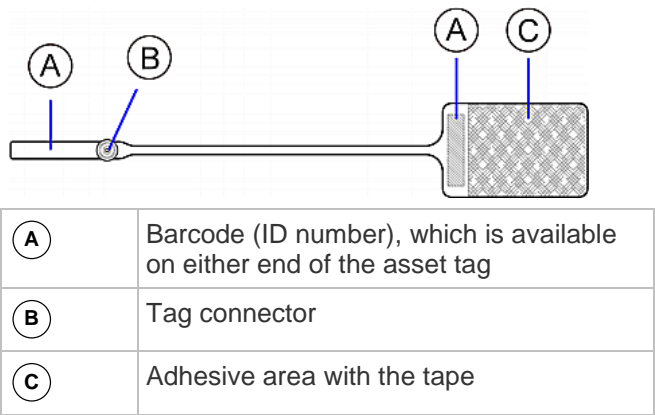
Connecting Asset Sensors to the Branch Circuit Monitor

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 management sensor at the other.

The asset sensor is connected to a Branch Circuit Monitor, and the asset tag transmits the ID and positioning information to the asset sensor.

The following diagram illustrates an asset tag.



Note: The barcode of each asset tag is unique and is displayed in the Branch Circuit Monitor device's web interface so it can easily be identified.

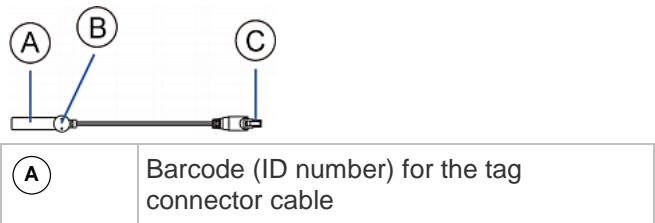
Connecting Blade Extension Strips

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 to a tag port on the regular or composite asset sensor. The blade extension strip contains 4 to 16 tag ports, depending on which model you purchased.

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

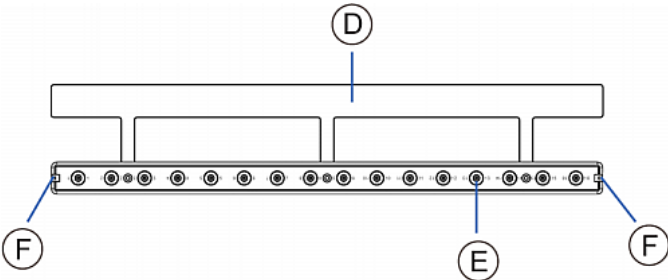
Tag connector cable



(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 Branch Circuit Monitor device's web interface for identifying each blade extension strip where it is connected.

Blade extension strip

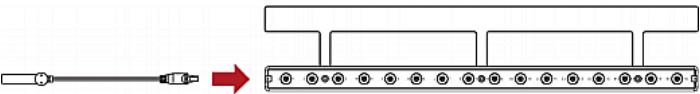


(D)	Mylar section with the adhesive tape
(E)	Tag ports
(F)	Cable socket(s) for connecting the tag connector cable

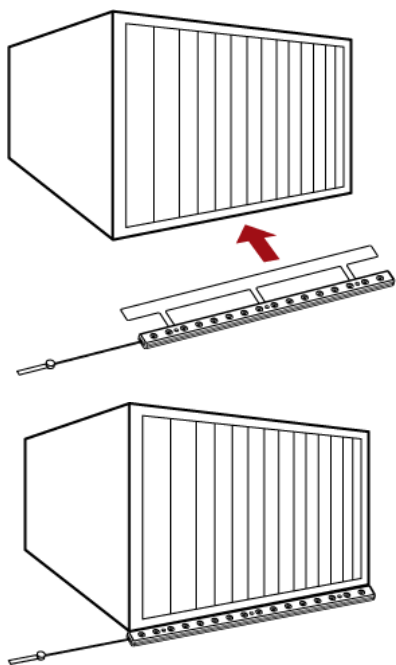
Note: Each tag port on the blade extension strip is labeled a number, which is displayed as the slot number in the Branch Circuit Monitor device's web interface.

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

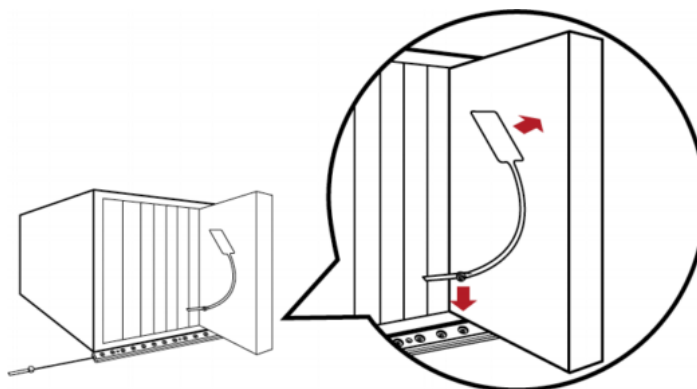
1. Connect the tag connector cable to the blade extension strip.
 - Plug the cable's connector into the socket at either end of the blade extension strip.



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.

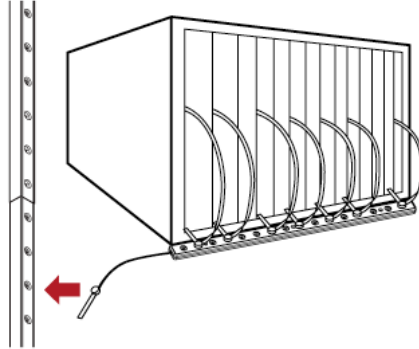


3. Connect one end of an asset tag to a blade server and connect the other end to the blade extension strip.
 - a. Affix the adhesive part of the asset tag to one side of a blade server through the tag's tape.
 - b. Plug the tag connector of the asset tag into the tag port on the blade extension strip.



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 and asset tags. 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 Branch Circuit Monitor device may not detect it.

Connecting Composite Asset Sensors to BCM

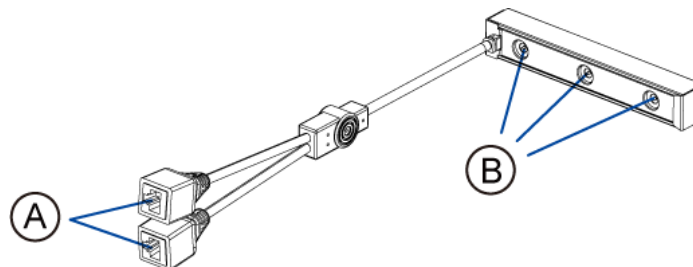
A composite asset sensor is named AMS-Mx-Z, where x is a number, such as AMS-M2-Z or AMS-M3-Z. It is a type of asset sensor that functions the same as regular MASTER asset sensors except for the following differences:

- 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 Branch Circuit Monitor device:**

1. Connect a composite asset sensor to the Branch Circuit Monitor 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 Branch Circuit Monitor 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. See **Connecting Asset Sensors to the Branch Circuit Monitor** (on page 53) for details.
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 59) 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.

Connecting Composite Asset Sensors Using an X Cable

Raritan's EMX-111 products support a maximum of four composite asset sensors in a chain. For details, see ***Daisy-Chain Limitations of Composite Asset Sensors*** (on page 59).

If you need to exceed the daisy-chain limitation, use Raritan's X cable to connect composite asset sensors. This allows you to expand the maximum number of composite asset sensors from four units per chain to six units per chain.

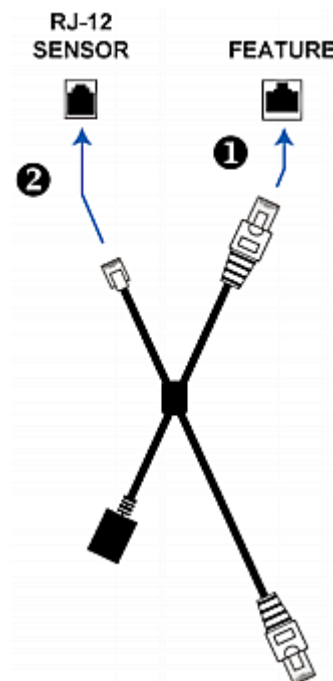
An X cable is a combination of two RJ-45 connectors, one Raritan-defined phone connector, and one RJ-12 sensor port.

The X cable supplies 12V voltage from the SENSOR port of the EMX-111 to the connected composite asset sensors, enhancing the asset sensor signals accordingly.

Note: An X cable does not help enhance the asset sensor signals for Raritan's EMX-888, so do not use this cable with them.

► To connect composite asset sensors via an X cable:

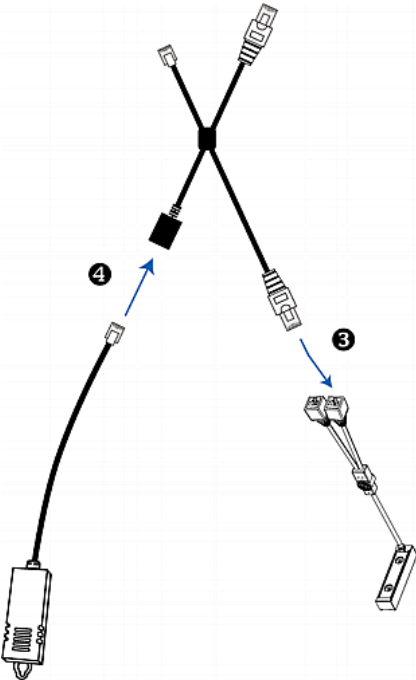
1. Plug the RJ-45 connector at the shorter end of the X cable into the FEATURE port of the Branch Circuit Monitor device.
2. Plug the phone connector of the X cable into the RJ-12 SENSOR port of the Branch Circuit Monitor device. **This step is required for improving the asset sensor signal strength.**



3. Plug the RJ-45 connector at the longer end of the X cable into the RJ-45 port labeled "Input" on the composite asset sensors.

Note: Though the X cable can also connect to a regular asset sensor, usually it is not necessary to make such a connection.

- A maximum of 5 additional composite asset sensors can be connected to the first composite asset sensor being attached to the X cable. See Connecting Composite Asset Sensors (AMS-Mx-Z) for step-by-step instructions.
4. Connect any Raritan environmental sensor package or hub to the RJ-12 sensor port of the X cable if environmental sensor packages are needed. Note that a DX sensor requires an RJ-12 to RJ-45 adapter to connect the X cable. See **Connecting Environmental Sensor Packages** (on page 40) for more information.



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.
- 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,	Up to 4 composite asset sensors

Raritan devices	Maximum sensors per chain
PX2 PDUs BCM	are supported.
EMX2-888, PX3 PDUs, PX3TS transfer switches	Up to 6 composite asset sensors are supported.

Tip: To increase the maximum number of composite asset sensors attached to a Raritan PX2 PDU or EMX2-111, you can use Raritan's X adapter cable to strengthen the asset sensor signals in the chain. See Using an X Cable.

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 Branch Circuit Monitor in order to view video 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>**).

Branch Circuit Monitor has only one USB-A port to connect a webcam, but you can use a "powered" USB hub to connect up to two webcams.

After connecting a webcam, visually monitor environmental conditions near the Branch Circuit Monitor through the Branch Circuit Monitor web interface from anywhere. 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 Branch Circuit Monitor device. The Branch Circuit Monitor 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 Branch Circuit Monitor web interface after the connection is complete. See **Viewing Webcam Snapshots or Videos** (on page 251).

Connecting a GSM Modem

A Cinterion® MC52iT or MC55iT GSM modem can be connected to the Branch Circuit Monitor in order to send SMS messages containing event information. See **Creating Actions** (on page 181) for more information on SMS messages.

Note: Branch Circuit Monitor cannot receive SMS messages.

► **To connect the GSM modem:**

1. Connect the GSM modem to the DB9 serial port on the Branch Circuit Monitor.
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 Branch Circuit Monitor.
 - 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 Branch Circuit Monitor supports remote dial-in communications to access the CLI through an analog modem. This dial-in feature provides an additional alternative to access the Branch Circuit Monitor when the LAN access is not available. To dial in to the Branch Circuit Monitor, the remote computer must have a modem connected and dial the correct phone number.

Below are the analog modems that the Branch Circuit Monitor supports for sure:

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

The Branch Circuit Monitor may also support other analog modems which Raritan did not test.

Note that the Branch Circuit Monitor 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 Branch Circuit Monitor.

You need to enable the modem dial-in support to take advantage of this feature, see **Configuring the Serial Port** (on page 123).

Connecting an External Beeper

The Branch Circuit Monitor supports the use of an external beeper for audio alarms. After having an external beeper connected, you can create event rules for the Branch Circuit Monitor to switch on or off the external beeper when specific events occur. See **Creating an Event Rule** (on page 181).

► **To connect an external beeper:**

1. Connect a standard network patch cable to the FEATURE port of the Branch Circuit Monitor.
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 Branch Circuit Monitor.

Connecting an RF Code PDU Sensor Tag

The RF Code R170 PDU sensor tag sends BCM power data to the RF Code management software for monitoring the energy utilization status. See **RF Code Energy Monitoring Solution** (on page 460) for more information.

► **To send the power data of the Branch Circuit Monitor to RF Code software:**

- Plug an RF Code R170 PDU sensor tag into the SENSOR port of the Branch Circuit Monitor.

Chapter 4 Panel Components

This chapter explains how to use the Branch Circuit Monitor. It describes the ports and channels on the device, and explains how to use the LCD display panel. The Branch Circuit Monitor comes with the following components on the outer panels.

- Line cord
- Connection ports
- LCD display
- Reset button
- Channels (CT terminals)

In This Chapter

Line Cord.....	64
Channels	65
Connection Ports.....	67
LCD Display Panel	68
Reset Button	78

Line Cord

The Branch Circuit Monitor contains a flexible cord containing the five wires for a 5-wire (3P+N+PE) AC connection. The cord is to connect to a 3-phase branch circuit for electricity input. Make sure you switch OFF the breaker of the branch circuit that will power the Branch Circuit Monitor before connecting the cord.

Connect the Branch Circuit Monitor's line cord by following the procedure below:

- Connect the L1 wire to a phase A connection point in the panel.
- Connect the L2 wire to a phase B connection point in the panel.
- Connect the L3 wire to a phase C connection point in the panel.
- Connect the N wire to the panel's neutral bus.
- Connect the GND wire to the panel's ground bus.

See the label or nameplate of your Branch Circuit Monitor model for appropriate input voltage ratings.

There is no power switch on the Branch Circuit Monitor. To power cycle it, power OFF the branch circuit breaker that supplies power to this product, wait 10 seconds and then power on the breaker.

Channels

A channel on the Branch Circuit Monitor is used to monitor a circuit, which may be phase A, B or C. Channels are divided into two categories: MAINS and BRANCH CIRCUITS. MAINS channels are for monitoring the main circuits, and BRANCH CIRCUITS channels are for branch circuits. For example, the BCM-2400 can monitor the mains rated at a maximum of 250A (or higher, depending on the mains CT used), and 21 branch circuits rated at a maximum of 100A.

The total number of channels is included in the first two numeric digits of the model name. For example, a BCM-2400 model can measure up to 24 circuits, including 21 branch circuits and 1 three-phase Wye-connected mains (L1, L2 and L3).

The Branch Circuit Monitor uses both a number and a color to identify a channel. Available channel colors vary from model to model.

- All channels using the same color as channel #1 are used to monitor the phase A circuit.
- All channels using the same color as channel #2 are used to monitor the phase B circuit.
- All channels using the same color as channel #3 are used to monitor the phase C circuit.

For more information, see **Channel Convention** (on page 12).

Mains Channels

Mains channels, which are used to measure the mains conductors, are labeled MAINS on the Branch Circuit Monitor. See the nameplate or label affixed to your Branch Circuit Monitor for the rating supported by the Mains channels.

Mains channel numbers are referred to as L1, L2 and L3. Use L1 to monitor phase A, L2 to phase B, and L3 to phase C.

Note: The Branch Circuit Monitor does not support measuring the neutral bus so do NOT connect any CT to the channel labeled N.

Branch Circuit Channels

Branch circuit channels, which are used to measure branch circuits, are labeled BRANCH CIRCUITS on the Branch Circuit Monitor.

Branch Circuit channel numbers are integer numbers that start at 1.

Every channel is marked with a color. All channels sharing the same channel color are used to monitor the same phase. Note that different models may have different channel colors. See **Channel Convention** (on page 12) for details.

For example, if your model uses black, red and blue as the channel colors and has 21 Branch Circuit channels, then:

- Channels for monitoring phase A are 1, 4, 7, 10, 13, 16, and 19, and all of these channels are marked with the black color.
- Channels for monitoring phase B are 2, 5, 8, 11, 14, 17 and 20, and all of these channels are marked with the red color.
- Channels for monitoring phase C are 3, 6, 9, 12, 15, 18 and 21, and all of these channels are marked with the blue color.

See the nameplate or label affixed to your Branch Circuit Monitor for the rating supported by the Branch Circuit channels.

CT Terminals and Buttons

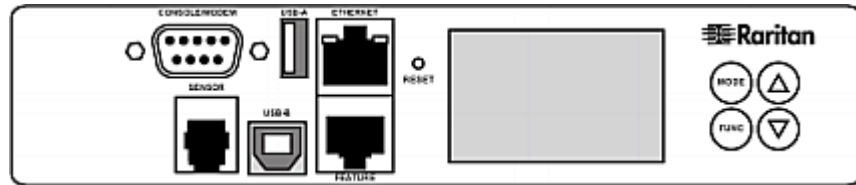
A channel, which is connected to a CT, comprises two CT terminals. A Raritan CT has two leads, which transmit different signals and are marked with different colors: black or white. The CT terminals on the Branch Circuit Monitor are also marked with either color to identify which CT lead to connect.

Make sure the CT terminal's color is identical to the Raritan CT lead's color when connecting a CT lead, or the signals are reversed, resulting in incorrect measurement of power.

The tiny orange button above each CT terminal controls the spring inside the terminal. Press and hold down the button above the corresponding terminal before plugging or unplugging a CT lead from the terminal.

For more information, see **Connecting Mains CTs** (on page 17) or **Connecting Branch Circuit CTs** (on page 19).

Connection Ports



The table below explains the function of each port.

Port	Used for...
USB-B	Establishing a USB connection between a computer and the Branch Circuit Monitor device. This port can be used for disaster recovery of the Branch Circuit Monitor device. Contact Raritan Technical Support for instructions.
USB-A	Connecting a USB device, such as a Logitech® webcam. This is a "host" port, which is powered, per USB 2.0 specifications.
FEATURE	Connecting a power CIM, asset sensor, or external beeper using an Category 5e/6 cable. <i>Warning: This is not an RS-232 port so do NOT plug in an RS-232 device, or damages can be caused to the device.</i>
CONSOLE/ MODEM	Establishing a serial connection between a computer and the Branch Circuit Monitor device: This is a standard DTE RS-232 port. You can use a null-modem cable with two DB9 connectors on both ends to connect the Branch Circuit Monitor device to the computer.
SENSOR	Connection to Raritan's environmental sensor packages. A Raritan sensor hub may be required if you want to connect multiple environmental sensors. However, Raritan does sell multiple sensors connecting to the SENSOR port through a single RJ-12 connector. For example, a DPX-T3H1 (3 temperature and 1 humidity sensor) uses only one RJ-12 port connection.
ETHERNET	Connecting the Branch Circuit Monitor device to your company's network: Connect a standard Cat5e/6 UTP cable to this port and connect the other end to your network. This connection is necessary to administer or access the Branch Circuit Monitor device remotely using the web interface. There are two small LEDs adjacent to the port: <ul style="list-style-type: none"> Green indicates a physical link and activity. Yellow indicates communications at 10/100 BaseT speeds. For a USB-cascading configuration in the bridging mode, the wired network

Port	Used for...
	connection is a must for the <i>master</i> Branch Circuit Monitor. See Cascading the Branch Circuit Monitor via USB (on page 37) for details.
	<i>Note: Connection to this port is not required if connection to a wireless network is preferred.</i>

LCD Display Panel

The LCD display panel shows different sensors' reading or status, and the device's MAC address.

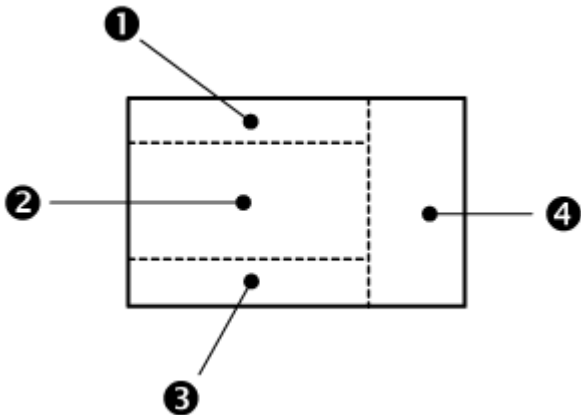


It consists of:

- A character LCD display
- Control buttons

LCD Display

Different types of information are shown in different sections of the character LCD display. The diagram indicates the sections.



Section	Information shown
1	<p>This section shows the selected mode and the target. The Branch Circuit Monitor has four modes as listed below:</p> <ul style="list-style-type: none"> • Mains mode - displayed as 'INLET.' There is only one mains so only 'INLET 1' is available. • Branch Circuit mode and the selected channel - displayed as 'OUTLET.' OUTLET 1 is channel# 1, OUTLET 2 is channel# 2, and so on. • Sensor mode - indicated by the word <i>SENSOR</i>, which is followed by the selected environmental sensor's ID number. For a sensor whose ID number is below 100, it is displayed as "SENSOR X" or "SENSOR XX," where X and XX are numeric digits. • Device mode, which is indicated by a letter <i>d</i>. When displaying the IPv4 address, 'i4' is also displayed to the top-right corner.
2	<p>Depending on your selection, the information displayed includes:</p> <ul style="list-style-type: none"> • Readings of the selected branch circuit or mains circuits, including current, power and unbalanced load. • Reading of the selected environmental sensor, which consists of numeric digits, or sensor state comprised of alphabetical characters. • X, Y or Z coordinates of the selected environmental sensor. • Serial number of the selected environmental sensor. • IP address of the Branch Circuit Monitor. • MAC address of the Branch Circuit Monitor.

<p>3</p>	<p>This section shows the selected mains channel, the selected line of a 3-phase branch circuit, or an 'ALARM.'</p> <p>Three mains channels are available -</p> <ul style="list-style-type: none"> • L1, L2 or L3 when showing current or power values. • L1-L2, L2-L3 or L3-L1 when showing voltage values. <p>When a branch circuit is configured as a 3-phase circuit using the web interface, three lines are available -</p> <ul style="list-style-type: none"> • L1, L2 or L3 when showing current or power values. • L1-L2, L2-L3 or L3-L1 when showing voltage values. <p>The word "ALARM" may appear to indicate any of the following scenarios:</p> <ul style="list-style-type: none"> • For the branch circuit (OUTLET) and mains (INLET) channels, it means the displayed reading reaches or crosses the upper or lower thresholds if these thresholds have been enabled. • For a numeric sensor, such as a temperature sensor, it means the sensor reading reaches or crosses the upper or lower thresholds if these thresholds have been enabled. • For a discrete (on/off) environmental sensor, such as a contact closure sensor, it means the sensor enters the abnormal state.
<p>4</p>	<p>The measurement unit for the selected target appears in this area. The measurement unit varies according to the sensor type:</p> <ul style="list-style-type: none"> • A is displayed for the current reading. A means Amp. • V is displayed for the voltage reading. V means Volt. • W is displayed for the power reading. W means Watt. • % is displayed for a humidity sensor. % is also displayed when showing the unbalanced current reading of a mains or 3-phase branch circuit. • °C is displayed for a temperature sensor.

Control Buttons

There are four control buttons.

- Up and Down buttons for selecting a specific channel, ID number or a device setting
- MODE button for switching between different modes, including:
 - Mains mode, displayed as INLET, for showing mains channel information
 - Branch Circuit mode, displayed as OUTLET, for showing branch circuit channel information
 - Sensor mode, displayed as SENSOR, for showing environmental sensor information
 - Device mode, indicated by a letter 'd,' for showing device settings
- FUNC (Function) button for switching between different data of the selected target, such as the current, voltage or power readings of a particular channel

Operating the LCD Display

After turning on or resetting this product, the display panel shows the current reading of the first branch circuit channel (that is, OUTLET 1) by default before you select a different channel or a different target.

Branch Circuit Information

The branch circuit information is displayed as "OUTLET" in the LCD display. By default the Branch Circuit Monitor displays the current reading of the channel 1 (that is, OUTLET 1) in the LCD display.

Important: Measurements of the branch circuit CTs may be incorrect if you have not properly configured your branch circuit CTs using the web interface. See *Configuring the Branch Circuit Channels* (on page 130).

► To display a single-phase branch circuit channel's information:

1. By default this product enters the Branch Circuit mode, indicated by 'OUTLET' in the upper left corner of the LCD display. If not, press the MODE button until the word "OUTLET" is displayed.
2. Press the Up or Down button until the desired channel number is displayed at the top of the LCD display.

Depending on whether any branch circuit is configured as a 3-phase circuit in the web interface, the channel numbers shown in the display may or may not be identical to the physical channel numbers labeled on the Branch Circuit Monitor.

For information on configuring branch circuits using the web interface, see **Configuring the Branch Circuit Channels** (on page 130).

For information on accurately identifying branch circuit channel numbers in the display, see **Identifying Branch Circuit Channel Numbers** (on page 73).

3. Press the FUNC button to switch between voltage, active power and current readings of the selected target.
 - A is displayed for the current reading. A means Amp.
 - V is displayed for the voltage reading. V means Volt.
 - W is displayed for the power reading. W means Watt.

If the word "ALARM" appears below the reading, it means the currently displayed reading already reaches or crosses the upper or lower thresholds.

► **To display a 3-phase branch circuit channel's information:**

1. Press the Up or Down button until the desired 3-phase branch circuit channel is selected.

For information on accurately identifying branch circuit channel numbers in the display, see **Identifying Branch Circuit Channel Numbers** (on page 73).

2. While that 3-phase channel is being selected, press the Up or Down button to switch between each line, indicated by L1, L2 or L3 at the bottom of the display.
3. When any line is being displayed, press the FUNC button to switch between voltage, active power and current readings of this particular line.
 - A is displayed for the current reading. A means Amp.
 - V is displayed for the voltage reading. V means Volt. When voltage is selected, L1-L2, L2-L3, or L3-L1 is displayed at the bottom of the display.
 - W is displayed for the power reading. W means Watt.
4. To show the unbalanced load and active power of this 3-phase branch circuit, do the following:
 - a. Switch to the current reading of L1.
 - b. Press the Down button until '%' or 'W' is displayed to the right of the display. Make sure NONE of the line is displayed at the bottom of the display.

- Unbalanced load - % is displayed for the unbalanced current value.
- Active power - W is displayed for the power reading. W means Watt.

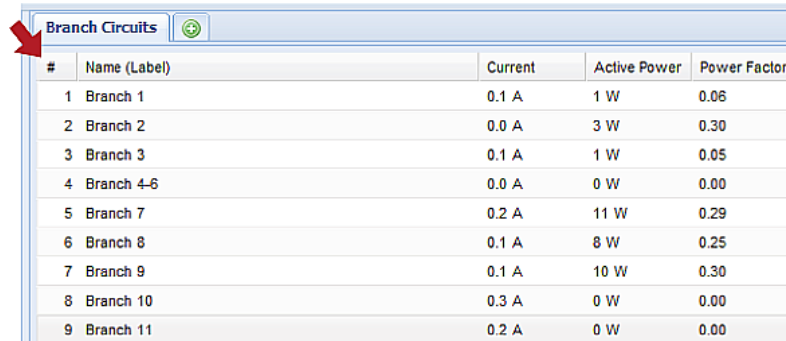
Identifying Branch Circuit Channel Numbers

A branch circuit channel is shown as *OUTLET <n>* in the LCD display.

- <n> is the index number of the selected branch circuit channel.

This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the chassis of the Branch Circuit Monitor.

See the diagram below for the index number column on the Branch Circuits page.



#	Name (Label)	Current	Active Power	Power Factor
1	Branch 1	0.1 A	1 W	0.06
2	Branch 2	0.0 A	3 W	0.30
3	Branch 3	0.1 A	1 W	0.05
4	Branch 4-6	0.0 A	0 W	0.00
5	Branch 7	0.2 A	11 W	0.29
6	Branch 8	0.1 A	8 W	0.25
7	Branch 9	0.1 A	10 W	0.30
8	Branch 10	0.3 A	0 W	0.00
9	Branch 11	0.2 A	0 W	0.00

- Index numbers may differ each time when you change the configuration of any branch circuit CTs using the web interface. See **Configuring the Branch Circuit Channels** (on page 130) for proper configuration.

When all branch circuit channels are configured as *single-phase* branch circuits, the channel numbers shown in the LCD display are completely identical to the physical channel numbers labeled on the chassis of the Branch Circuit Monitor. For example, OUTLET 3 refers to the branch circuit channel labeled 3, and OUTLET 10 refers to the one labeled 10 on the Branch Circuit Monitor.

When any branch circuit channels are configured as a *3-phase* branch circuit, the channel numbers shown on the LCD display may not be identical to the physical channel numbers labeled on the Branch Circuit Monitor, and you need to refer to the index number column for correct channel numbers.

Mains Information

The mains-related information is displayed as "INLET" in the LCD display. Because there is only one MAINS channel group on the Branch Circuit Monitor, only "INLET 1" is available.

Important: Measurements of the mains CTs may be incorrect if you have not properly configured your mains CTs using the web interface. See *Configuring the Mains Channels* (on page 129).

► **To display a mains channel's information:**

1. Press the MODE button until the term "INLET" is displayed.
2. When in the Mains mode, press the Up or Down button until the desired mains channel number (L1, L2 or L3) is shown at the bottom of the LCD display.
 - Pressing the Δ (UP) button moves up one selection.
 - Pressing the ∇ (DOWN) button moves down one selection.

L1 or L1-L2 refers to the L1 channel on the Branch Circuit Monitor, L2 or L2-L3 refers to the L2 channel, and L3 or L3-L1 refers to the L3 channel.
3. Press the FUNC button to switch between voltage, active power and current readings of the selected target.
 - A is displayed for the current reading. A means Amp.
 - V is displayed for the voltage reading. V means Volt.
 - W is displayed for the power reading. W means Watt.

If the word "ALARM" appears below the reading, it means the currently displayed reading already reaches or crosses the upper or lower thresholds.

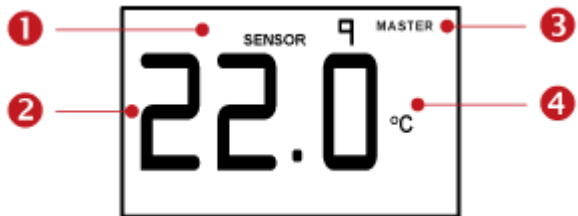
► **To display the unbalanced load and active power of the mains:**

1. Switch to the current reading of any mains channel.
2. Press the Up or Down button until 'W' or '%' is displayed to the right of the LCD display. Make sure NONE of the mains channel number is displayed at the bottom of the display.
 - Unbalanced load - % is displayed for the unbalanced current value.
 - Active power - W is displayed for the power reading. W means Watt.

Environmental Sensor Information

The environmental sensor mode is displayed as "SENSOR" on the LCD display. Basic information about a specific environmental sensor is available through the LCD display, including the sensor's reading or state, X, Y, Z coordinates or its serial number.

Below illustrates the environmental sensor information shown on the LCD display.



Number	Example information
1	The selected target is the environmental sensor whose ID number is 9 (SENSOR 9).
2	The selected environmental sensor's reading is 22 °C .
3	The word "MASTER" indicates the Branch Circuit Monitor is the master device in a USB-cascading configuration. See Cascading the Branch Circuit Monitor via USB (on page 37). For a standalone Branch Circuit Monitor, this word is NOT displayed.
4	The measurement unit is °C (degrees in Celsius).

► **To display the environmental sensor information:**

1. Press the MODE button until this product enters the Sensor mode, as indicated by "SENSOR" at the top of the LCD display.
2. Press the Up or Down button until the desired environmental sensor's ID number is displayed. For example, "SENSOR 1" refers to the sensor #1 listed on the Peripheral Devices page of the web interface.
3. The LCD display shows the reading or state of the selected sensor in the middle of the LCD display.

For a numeric sensor's reading, the appropriate measurement unit is displayed to the right of the reading.

- % is displayed for a humidity sensor.
- °C is displayed for a temperature sensor.
- m/s is displayed for an air flow sensor.

- Pa is displayed for an air pressure sensor.

For a discrete sensor, either of the following states is displayed.

- nor: The sensor is in the normal state.
- ALA (accompanied with the word "ALARM" below it): The sensor is in the alarmed state.

For a dry contact signal actuator (DX series), either of the following states is displayed.

- On: The actuator is turned on.
- Off: The actuator is turned off.

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.

4. Press the FUNC button to show the sensor's port position. There are two types of information.
 - *P:n* (where n is the SENSOR port's number): This information indicates the SENSOR port number.
 - *C:x* (where x is the sensor's position in a sensor chain): This information indicates the sensor's position in a chain. This information is available for DPX2 and DX sensors only. The LCD display will cycle between the port information (*P:n*) and chain position information (*C:x*).
5. Press the FUNC button to display the X, Y and Z coordinates of the sensor respectively.
 - X coordinate is shown as "x:XX," where XX are the first two numeric digits entered for the X coordinate in the web interface.
 - Y coordinate is shown as "y:XX," where XX are the first two numeric digits entered for the Y coordinate in the web interface.
 - Z coordinate is shown as "z:XX," where XX are the first two numeric digits entered for the Z coordinate in the web interface.

If one or both of the first two digits for a specific coordinate are alphabetical characters, one or two dashes (-) are displayed in place of the alphabetical characters.

6. Press the FUNC button to display the serial number of the sensor, which is shown as "s:XX," where XX are two digits of the serial number. The LCD will cycle through the serial number from the first two digits to the final two.

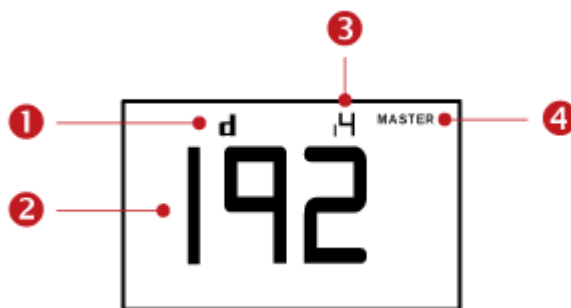
For example, if the serial number is AE17A00022, the LCD display shows the following information one after another:

s:AE --> s:17 --> s:A0 --> s:00 --> s:22

IP Address

The IP address is available in the Device mode, which is indicated by the alphabet 'd' shown at the top of the LCD display. Note that the LCD display only shows the IPv4 address (if available).

Below illustrates the IP address information shown on the LCD display.



Section	Example information
①	"d" means the LCD display has entered the Device mode.
②	The LCD display is showing 192, which is one of the IP address octets. It will cycle through four octets of the IP address.
③	"i4" indicates that the IP address shown on the LCD display is an IPv4 address.
④	The word "MASTER" indicates the Branch Circuit Monitor is the master device in a USB-cascading configuration. See <i>Cascading the Branch Circuit Monitor via USB</i> (on page 37). For a standalone Branch Circuit Monitor, this word is NOT displayed.

If you connect your Branch Circuit Monitor to the wireless network, a Wi-Fi icon is displayed at the bottom-right corner.



► To retrieve the IP address:

1. Press the MODE button until device settings are displayed, indicated by a 'd' in at the top left of the display.

2. The LCD display cycles between the four octets of the IPv4 address, indicated by "i4" at the upper right corner of the display.

For example, if the IPv4 address is 192.168.84.4, the LCD display cycles through it as shown below:

192 --> 168 --> 84 --> 4

MAC Address

The Branch Circuit Monitor's MAC address is available by operating the LCD display, and in Device mode. Contact your LAN administrator for assistance.

► To display the MAC address:

1. Press the MODE button until device settings are displayed, indicated by a 'd' in at the top left of the display.
2. Press the FUNC button until the MAC address is displayed. The character "M" appears in the left side of the LCD display.
3. The MAC address is displayed as "M:XX", where XX are two digits of the MAC address. The LCD will cycle through the MAC address from the first two digits to the final two.

For example, if the MAC address is 00:0d:5d:03:5E:1A, the LCD display shows the following information one after another:

M 00 --> M:0d --> M:5d --> M:03 --> M:5E --> M:1A

Note that 'M' is NOT followed by the colon symbol when showing the first two digits of the MAC address.

Reset Button

The reset button is located inside a small hole which is labeled RESET.



The Branch Circuit Monitor device can be reset to its factory default values using this button when a serial connection is available. See **Resetting to Factory Defaults** (on page 443).

Without the serial connection, pressing this reset button restarts the Branch Circuit Monitor device's software.

Chapter 5 Using the Web Interface

This chapter explains how to use the web interface to administer a Branch Circuit Monitor.

In This Chapter

Supported Web Browsers.....	79
Logging in to the Web Interface	80
Logout.....	82
Introduction to the Web Interface	83
Viewing the Dashboard	95
Device Management.....	97
Channel or CT Configuration.....	128
Setting Power Thresholds	136
User Management	141
Setting Up Roles.....	147
Access Security Control	150
Setting Up a TLS Certificate	165
Setting Up External Authentication.....	171
Event Rules and Actions	180
Viewing Connected Users	219
Monitoring Server Accessibility.....	220
Managing Event Logging.....	223
Environmental Sensors and Actuators	225
Asset Management.....	243
Webcam Management	249
Firmware Upgrade	258
Viewing the Communication Log	260
Network Diagnostics	260
Downloading Diagnostic Information	262
Backup and Restore of Branch Circuit Monitor Device Settings	262
Accessing the Help	263

Supported Web Browsers

The following web browsers can be used to access the Branch Circuit Monitor web interface:

- 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

Logging in to the Web Interface

To log in to the web interface, you must enter a user name and password. The first time you log in to the Branch Circuit Monitor, use the default user name (admin) and password (raritan). You are then prompted to change the password for security purposes.

Exception: If you already changed the password for the admin account, use the new password instead for login, and the Branch Circuit Monitor will NOT prompt you to change the password.

After successfully logging in, you can create user profiles for your other users. These profiles define their login names and passwords. See **Creating a User Profile** (on page 142).

Login

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

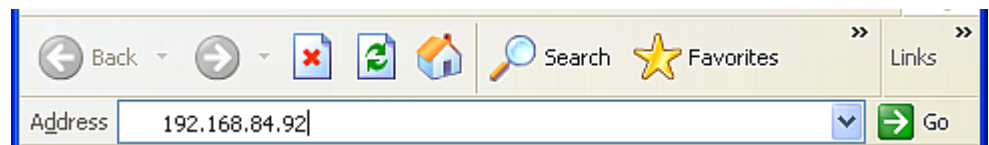
You must enable JavaScript in the web browser for proper operation.

► **To log in to the web interface:**

1. Open a browser, such as Microsoft Internet Explorer or Mozilla Firefox, and type this URL:

http(s)://<ip address>

where <ip address> is the IP address of the Branch Circuit Monitor.



2. If a security alert message appears, click OK or Yes to accept. The Login page then opens.
3. Type your user name in the User Name field, and password in the Password field.

A screenshot of a web browser window displaying a "Login" page. The page has a light blue background. At the top left is a small icon of a person and the word "Login". Below this are two text input fields: "User Name:" and "Password:". At the bottom right are two buttons: "Login" and "Clear".

Note: Both the user name and password are case sensitive. If needed, click Clear to clear either the inputs or any error message that appears.

- If a security agreement is displayed on the Login page, accept it. To select the agreement checkbox using the keyboard, press the Space bar.

Note: If you do not accept the security agreement, you cannot log in successfully.

- Click Login or press Enter. The Branch Circuit Monitor page opens.

Note: Depending on your hardware configuration, elements shown on the web interface may appear slightly different from this image.

The screenshot shows the Raritan Dominion PX web interface. The top navigation bar includes 'User Management', 'Device Settings', and 'Maintenance'. The left sidebar shows 'Dominion PX Explorer' with options: Dashboard, my PX (192.168.84.9), Branch Circuits, External Sensors, and Feature Port. The main content area is titled 'Dashboard' and displays the following data:

- Main:**
 - L1 RMS Current: 0.0 A / 200.0 A
 - L2 RMS Current: 0.0 A / 200.0 A
 - L3 RMS Current: 0.0 A / 200.0 A
 - Unbalanced Current: 0 %
 - L1-L2 / L2-L3 / L3-L1 Voltage: 111 V / 0 V / 111 V
 - Active Power: 0 W
 - Apparent Power: 4 VA
 - Power Factor: 1.00
 - Active Energy: 130 Wh
- Alarmed Sensors:** (Empty table)
- External Sensors (4 managed, 0 unmanaged):**

Name	Reading	State
Humidity 1	65 %	normal
Humidity 2	67 %	normal
Temperature 1	72.4 °F	normal
Temperature 2	72.5 °F	normal

The bottom status bar shows 'my PX (192.168.84.9)', 'Administrator (admin)', and 'Last Login: 1/16/13 4:25 PM'.

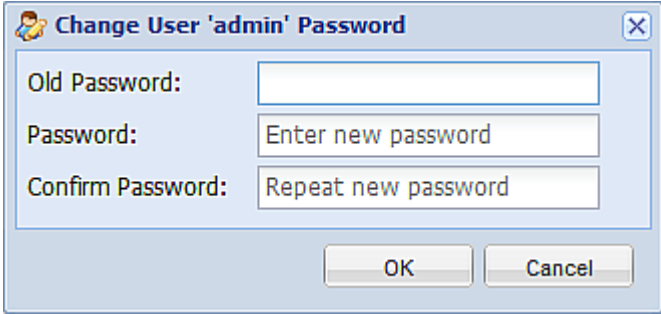
Changing Your Password

Normal users can change their own passwords if they have the Change Own Password permission. See **Setting Up Roles** (on page 147).

If you are the administrator (admin), the Branch Circuit Monitor web interface automatically prompts you to change the password if this is your first time to log in to the Branch Circuit Monitor. If you have the Administrator Privileges, you can change other users' passwords, as well. See **Modifying a User Profile** (on page 145).

► To change your password:

1. Choose User Management > Change Password. The Change User Password dialog appears.



A screenshot of a web-based dialog box titled "Change User 'admin' Password". The dialog has a light blue header with a small icon of a person and a close button (X) in the top right corner. The main area contains three labeled text input fields: "Old Password:" with an empty field, "Password:" with the placeholder text "Enter new password", and "Confirm Password:" with the placeholder text "Repeat new password". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

2. Type the current password in the Old Password field.
3. Type your new password in the Password and Confirm Password fields. The password can be 4 to 64 characters long. It is case sensitive.
4. Click OK.

Logout

After finishing your tasks with the Branch Circuit Monitor, you should log out to prevent others from accessing the web interface.

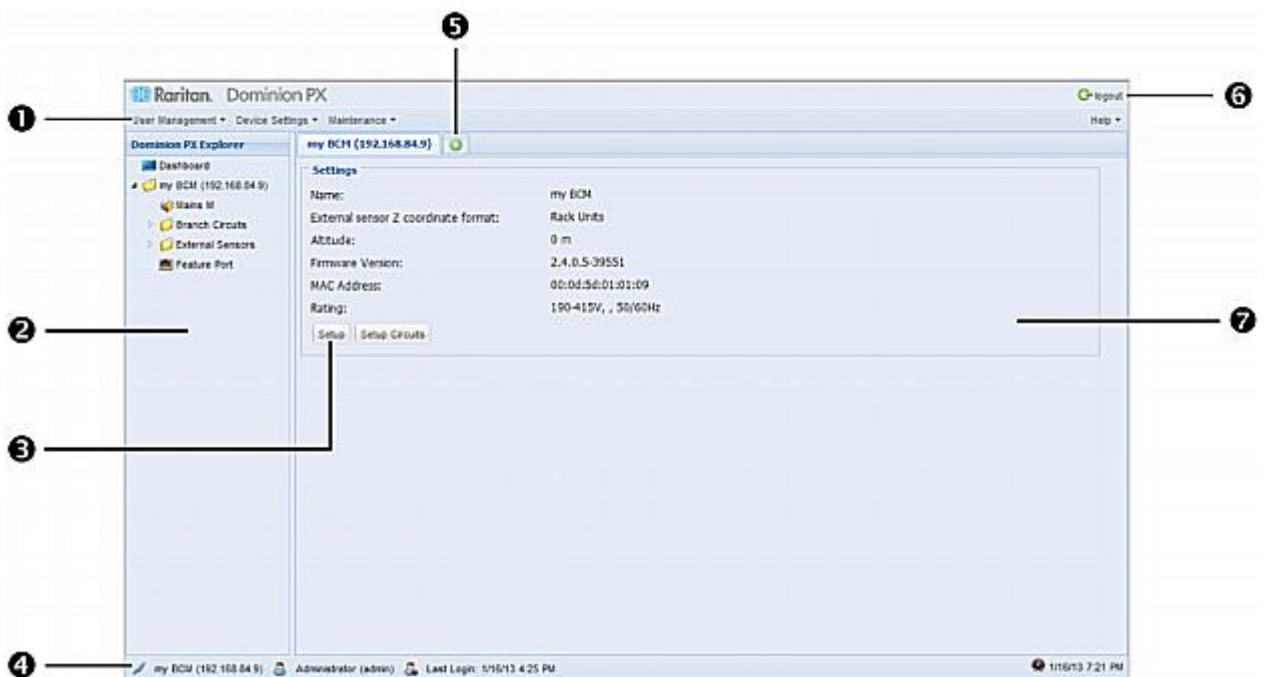
► To log out of the web interface:

1. Do one of these:
 - Click "logout" on the top-right corner of the web interface.
The image shows a green circular icon with a white arrow pointing right, followed by the text "logout" in a bold, sans-serif font.
 - Close the web browser by clicking the Close button () on the top-right corner of the browser.

- Close the web browser by choosing File > Close, or File > Exit. The command varies according to the version of the browser you use.
 - Choose the Refresh command or click the Refresh button on the web browser.
2. Either the login page opens or the browser is closed, depending on your choice in the previous step.

Introduction to the Web Interface

The web interface provides two panes, a menu bar, a status bar, an Add Page icon, and a logout button throughout every page.



Number	Web interface element
1	Menus
2	PX Explorer pane
3	Setup button*
4	Status bar
5	Add Page icon
6	Logout button
7	Data pane

* The Setup button is not available on some pages, such as the *Dashboard* page.

For detailed information about these web interface elements, see the sections that follow.

Menus

There is a menu bar across the top of the page. You can click any menu to select the desired menu item from the drop-down list.

Four menus are available for managing different tasks or showing information.

- **User Management** contains menu items for managing user profiles, permissions (roles), and password.
- **Device Settings** deals with device-related settings, such as the device name, network settings, security settings, and system time.
- **Maintenance** provides tools that are helpful for maintaining the Branch Circuit Monitor, such as the event log, hardware information, firmware upgrade and so on.
- **Help** displays information regarding the firmware and all open source packages embedded on the Branch Circuit Monitor. In addition, you can access the online help from this menu.

Explorer Pane

The hierarchical tree to the left displays the Branch Circuit Monitor you are accessing as well as all physical components connected to or associated with this device, such as mains channels, branch circuit channels, and environmental sensors. In addition, an icon named Dashboard is available for displaying the device's summary information.

The tree structure comprises three hierarchical levels.

First level	Second level	Third level
Dashboard	None	None
BCM folder*	Mains M	None
	Branch Circuits folder	1 to n**
	External Sensors folder	A list of connected environmental sensors

First level	Second level	Third level
	Feature Port folder	One of the following is displayed, depending on your configuration: <ul style="list-style-type: none"> • None • Power CIM • Asset Sensor • External Sensor
	Webcam Management***	<ul style="list-style-type: none"> • Snapshots • Webcam

* The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).

** n represents the final number of that component.

*** A Webcam icon appears only when a supported Logitech® webcam is connected to the Branch Circuit Monitor. See **Connecting a Logitech Webcam** (on page 61).

Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.

► **To navigate through the tree:**

1. To expand any folders, see **Expanding the Tree** (on page 85).
2. To show any tree item's data, click on that item. See **Add Page Icon** (on page 89).

Expanding the Tree

The icons representing all components connected to or associated with the Branch Circuit Monitor are expanded by default. If they are hidden, you may expand the tree manually to show all component icons.

► **To expand the tree:**

1. By default, the BCM folder has been expanded.

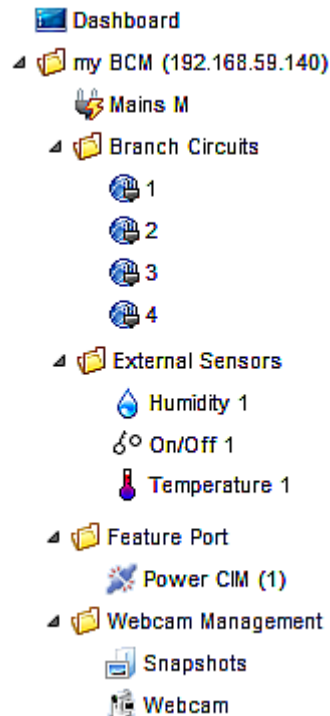
*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

If it is not expanded, click the white arrow ▸ prior to the folder icon, or double-click the folder. The arrow then turns into a black, gradient arrow ▲, and icons of components or component groups appear below the BCM folder.

2. To expand any component group at the second level, click the white arrow ▸ prior to the folder icon, or double-click the folder.

The arrow then turns into a black, gradient arrow ▲, and icons representing individual components appear below the group folder.

3. Repeat Step 2 for other component groups you want to expand. The expanded tree looks similar to this image.



*Note: A Webcam icon appears only when a supported Logitech® webcam is connected to the Branch Circuit Monitor. See **Connecting a Logitech Webcam** (on page 61).*

Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.

Collapsing the Tree

You can collapse the whole tree structure or a specific component group to hide all or partial tree items.

► To collapse the whole tree:

- Click the black, gradient arrow ▲ prior to the BCM folder icon, or double-click the folder.

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

The arrow then turns into a white arrow ▷, and all items below the BCM folder disappear.

► To hide some tree items:

1. Click the black, gradient arrow ▲ prior to the component group folder that you want to collapse, or double-click the folder.

The arrow then turns into a white arrow ▷, and all items below the folder disappear.

2. Repeat Step 1 for other component groups you want to collapse.

Adjusting the Pane

You can change the width of the pane to make the area larger or smaller.

► To adjust the pane's width:

1. Move the mouse pointer to the right border of the Explorer pane.
2. When the mouse pointer turns into a two-way arrow, drag the border horizontally to widen or shrink the pane.

Setup Button

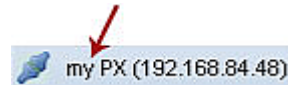
The Setup button is available for most tree items. It triggers a setup dialog where you can change settings for the selected tree item.

Status Bar

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

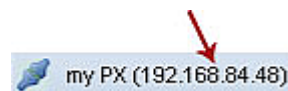
- **Device name:**


This is the name assigned to the Branch Circuit Monitor device. The default is "my PX." See **Naming the Branch Circuit Monitor** (on page 103).



- **IP address:**

The numbers enclosed in parentheses is the IP address assigned to the Branch Circuit Monitor device. See **Initial Network Configuration via CLI** (on page 26) or **Modifying Network Settings** (on page 107).



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

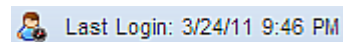
- **Login name:**

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 Branch Circuit Monitor 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:

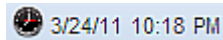
- Web GUI: Refers to the Branch Circuit Monitor web interface.
- CLI: Refers to the command line interface (CLI).

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.




Sometimes a flag icon (🚩) may appear to the far right of the bar when a communication error between the Branch Circuit Monitor device and the graphical user interface (GUI) occurs. When the icon appears, you can click the icon to view the communications log. See **Viewing the Communication Log** (on page 260).

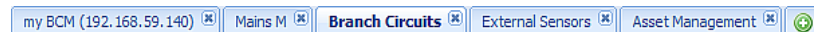
Add Page Icon

The Add Page icon , located on the top of the data pane, lets you open data pages of multiple tree items without overriding any opened page.

► To open new data pages:



1. Click the Add Page icon . A new tab along with a blank data page appears.
2. Click a tree item whose data page you want to open. The data of the selected tree item is then displayed on the blank page.
3. To open more data pages, repeat the above steps. All tabs representing opened pages are shown across the top of the page.


The following diagram shows a multi-tab example.



4. With multiple pages opened, you can take these actions:

- To switch to one of the opened data pages, click the corresponding tab.

If there are too many tabs to be all shown, two arrows ( and ) appear at the left and right borders of the pane. Click either arrow to navigate through all tabs.

- To close any data page, click the Close button () on the corresponding tab.

Logout Button

Click the logout button when you want to log out of the web interface.



Data Pane

The right pane shows the data page of the selected tree item. The data page includes the item's current status, settings and a Setup button (if available).

All tabs above the pane represent the opened data pages. The highlighted tab indicates the current selection.

You can change the width of the pane to make the area larger or smaller.

► **To adjust the pane's width:**

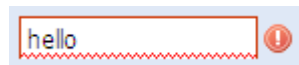
1. Move the mouse pointer to the left border of the right pane.
2. When the mouse pointer turns into a two-way arrow, drag the border horizontally to widen or shrink the pane.

More Information

This section explains additional web interface elements or operations that are useful.

Warning Icon

If the value you entered in a specific field is invalid, a red warning icon appears to the right and the field in question is surrounded by a red frame as shown in this illustration.



When this occurs, position your mouse pointer over the warning icon to view the reason and modify the entered value accordingly.

The Yellow- or Red-Highlighted Sensors

When a numeric sensor's reading crosses any upper or lower threshold, the background color of the whole row turns to yellow or red for alerting users.

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 falls between the lower and upper warning thresholds. For a discrete (on/off) sensor, the sensor state is normal. The sensor is unavailable.
Yellow	<p>The reading drops below the lower warning threshold or rises above the upper warning threshold.</p>
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.

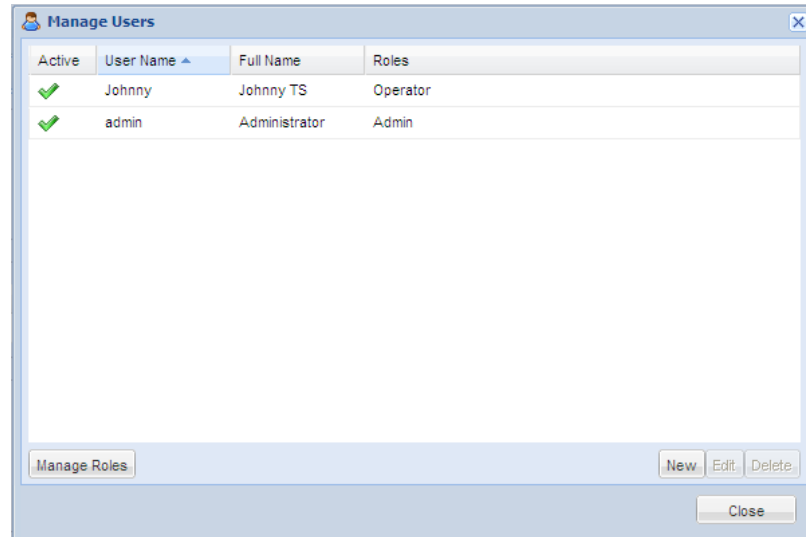
To find the exact meaning of the alert, read the information shown in the State (or Status) column:

- 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 136).

Changing the View of a List

Some dialogs and data pages contain a list or table, such as the Manage Users dialog shown below. You may change the number of displayed columns or re-sort the list for better viewing the data. Note the column or sorting changes are not saved when quitting the dialog or data page. Next time when the dialog or page re-opens, the list returns to the default view.




Note: Not all dialogs support the sorting or column change functions.

Changing the Column

You can hide some columns of a list or table, or adjust a specific column's width.

► To change displayed columns:

1. Hover your mouse pointer over any column header. A black triangle  appears to the far right of this column header.
2. Click the black triangle, and a drop-down menu appears.
3. Point to Columns. A submenu showing all columns appears.
4. Click any column you want to deselect or select.
 - To hide a column, have its checkbox deselected.
 - To show a column, have its checkbox selected.

► To change the column width:

1. Hover the mouse pointer to the right border of the desired column.

2. When the mouse pointer turns to a two-way arrow, drag the border horizontally to widen or shrink the column.

Changing the Sorting

By default, a list or table is sorted against the first column in the ascending order. You can re-sort the list in a reverse order or against a different column.

► **To re-sort the list by doing either of the following:**

- Click the column header against which you want to sort the list.
 - a. The first click sorts the list in the ascending order, indicated by a blue upward-pointing triangle ▲.
 - b. The second click reverses the sorting to the descending order, indicated by a blue downward-pointing triangle ▼.
- Select a sorting command from the column menu.
 - a. Hover your mouse pointer over the column header against which you want to sort the list. A black triangle ▼ appears to the far right of this column header.
 - b. Click the black triangle, and a drop-down menu appears.
 - c. Select Sort Ascending or Sort Descending.

The newly selected column header is marked with the upward- or downward-pointing triangle.

Resizing a Dialog

Most dialogs cannot be resized except for a few ones (such as the Event Log dialog), which can be resized to display more information at a time.

► **To resize a dialog:**

1. Hover your mouse pointer over any border of the dialog.
2. When the mouse pointer turns to a double-headed arrow, drag the border vertically or horizontally to make the dialog bigger or smaller.

Browser-Defined Shortcut Menu

A shortcut menu, which is built in the web browser, may appear when right-clicking anywhere in the Branch Circuit Monitor web interface.

The shortcut menu functions are defined by the browser. For example, the Back command on the Internet Explorer® (IE) shortcut menu works the same as the Back button in the IE browser. Both of these functions take you to the previous page.

For information on each shortcut menu command or item, see the online help or documentation accompanying your web browser.

Below is the illustration of the IE browser's shortcut menu. Available menu commands or items may slightly differ based on your web browser version.



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 Branch Circuit Monitor device's status.


The page is divided into various sections according to the component type, such as Mains and External Sensors.

*Note: 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 91.*


After clicking any other icon in the hierarchical tree, the Dashboard page is overridden. To return to the Dashboard page, click the Dashboard icon.

When the Dashboard page is opened, you can do the following to uncover or hide specific data.

► **To collapse any section:**

1. Locate the section you want to collapse.
2. Click the upward arrow  prior to the section title. The data specific to the section is hidden.

► **To expand a collapsed section:**

1. Locate the section you want to expand.
2. Click the downward arrow  prior to the section title. The data specific to the section appears.

Important: Measurements of the mains CTs may be incorrect if you have not properly configured your mains CTs using the web interface. See *Configuring the Mains Channels* (on page 129).

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

Alerted Sensors		
Sensor	Reading	State
Mains M L1-L2 RMS Voltage	111 V	below lower critical
Mains M L3-L1 RMS Voltage	111 V	below lower critical
Temperature 1	21.6 °C	above upper warning

For the background color meanings, see **The Yellow- or Red-Highlighted Reading** (see "**The Yellow- or Red-Highlighted Sensors**" on page 91).

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 181).

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.

Alarms						
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.

Column	Description
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.

*Tip: When browsing through all events, you can sort the list of all events shown in the dialog by clicking the header row. See **Changing the View of a List** (on page 92).*

Device Management

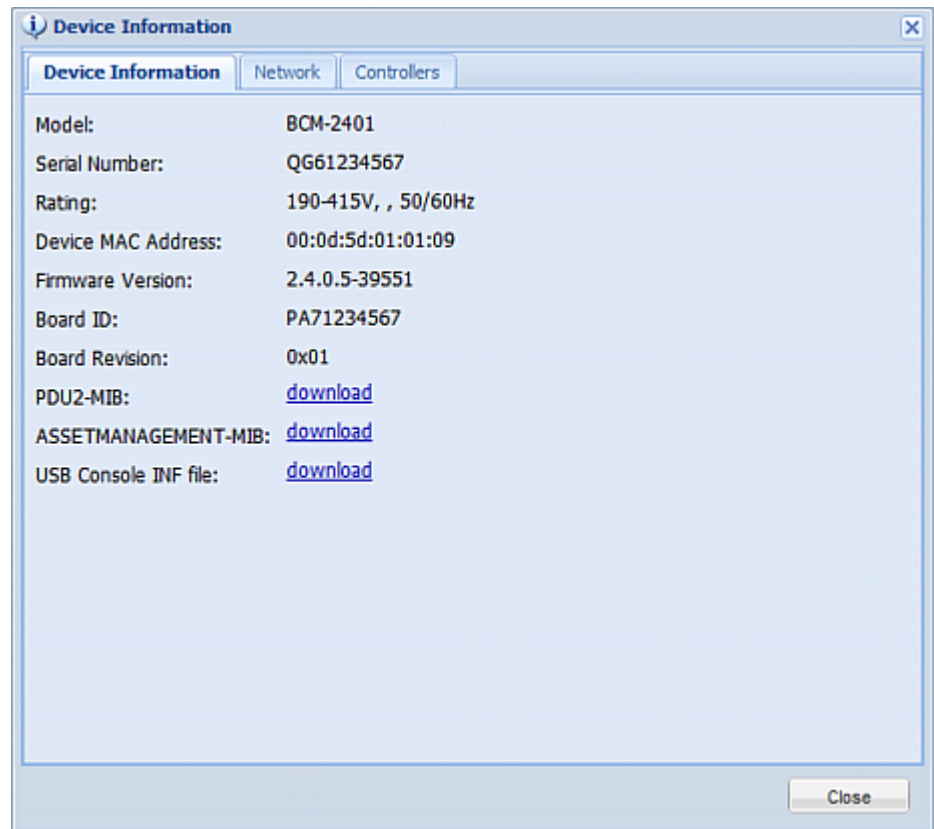
Using the web interface, you can retrieve basic hardware and software information, give the Branch Circuit Monitor a new device name, set the system date and time, and modify network settings that were entered during the initial configuration process.

Displaying the Device Information

To display information specific to the Branch Circuit Monitor that you are using, such as its serial number, model name and rating, trigger the Device Information dialog.

► **To display the device information:**

1. Choose Maintenance > Device Information. The Device Information dialog appears.



2. Click the tab containing the information you want to view.

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 Branch

Tab	Information shown
	Circuit Monitor is part of an USB-cascading configuration. See Identifying Cascaded Devices (on page 99).
Controllers	The device controller's information, including its serial number, firmware version, and hardware revision.

Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.

3. Enlarge the dialog if necessary.
4. You can re-sort the list or change the columns displayed.
5. Click Close to quit the dialog.

Tip: The firmware version is also available by clicking the BCM folder in the Dominion PX Explorer pane.

Identifying Cascaded Devices

This section explains how to identify a cascaded Branch Circuit Monitor in the Device Information dialog.

For information on how to cascade devices using USB cables, see **Cascading the Branch Circuit Monitor via USB** (on page 37).

*Note: For more information on the USB-cascading configuration, see the USB-Cascading Solution Guide, which is available on the **PX2 web page** (<http://www.raritan.com/support/product/px2/>) of the Raritan website.*

► To identify the USB-cascading status of a Branch Circuit Monitor device:

1. Choose Maintenance > Device Information. The Device Information dialog appears.
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	<p>Indicates how the Branch Circuit Monitor is connected to the LAN.</p> <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 25). 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.
Cascade Position	<p>Indicates the position of the Branch Circuit Monitor 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 Branch Circuit Monitor.</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.

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

Networking Mode:	Wired
Cascading Mode:	Bridging
Cascade Position:	0 (Master)
Cascaded Device Connected:	yes

Below the Interface section, the IPv4 and IPv6 sections are also visible. The IPv4 section shows Address: 192.168. X .X, Gateway: 192.168. X .X, and DNS Servers: 192.168. X .X , 192.168. X .X. The IPv6 section shows Address: n/a, Routes: n/a, and DNS Servers: n/a. A "Close" button is located at the bottom right of the window.

- 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 screenshot shows a web interface window titled "Device Information" with a "Network" tab selected. Under the "Interface" section, the following settings are displayed:

Networking Mode:	Wired (USB)
Cascading Mode:	Bridging
Cascade Position:	1 (Slave 1)
Cascaded Device Connected:	yes

Below the Interface section, the IPv4 and IPv6 sections are visible. The IPv4 section shows Address: 192.168. X .X, Gateway: 192.168. X .X, and DNS Servers: 192.168. X .X , 192.168. X .X. The IPv6 section shows Address: n/a, Routes: n/a, and DNS Servers: n/a. A "Close" button is located at the bottom right of the window.

- 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.

Device Information

Device Information | **Network**

Interface

Networking Mode: Wired (USB)

Cascading Mode: Bridging

Cascade Position: 2 (Slave 2)

Cascaded Device Connected: no

IPv4

Address: 192.168. X.X

Gateway: 192.168. X.X

DNS Servers: 192.168. X.X , 192.168. X.X

IPv6

Address: n/a

Routes: n/a

DNS Servers: n/a

Close

Naming the Branch Circuit Monitor

The default name for Branch Circuit Monitor is *my PX*. You may give it a unique device name.

► To change the device name:

1. Click the BCM folder.

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Setup in the Settings section. The BCM 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 Branch Circuit Monitor supports two types of network interfaces: wired and wireless. You should configure the network interface settings according to the networking mode that applies. See **Connecting the Branch Circuit Monitor to Your Network** (on page 25).

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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 via the web interface.

*Note for USB-cascading configuration: Port forwarding mode over wireless LAN is supported as of release 3.1.0. You must upgrade all devices in the chain to version 3.1.0 or later if wireless networking is preferred. See **Cascading the Branch Circuit Monitor via USB** (on page 37).*

► **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 Branch Circuit Monitor 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 **Connecting the Branch Circuit Monitor to Your Network** (on page 25).
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 Branch Circuit Monitor to verify the validity of the TLS certificate that will be installed. For example, the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor has once been powered off for a long time.
9. Click OK.

Modifying Network Settings

The Branch Circuit Monitor was configured for network connectivity during the installation and configuration process. See **Configuring the Branch Circuit Monitor** (on page 22). If necessary, you can modify any network settings using the web interface.

Selecting the Internet Protocol

The Branch Circuit Monitor 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 107).

► **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 Branch Circuit Monitor, select DHCP. 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 Branch Circuit Monitor 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 for illustrations.</p>

- Click OK.

Note: The Branch Circuit Monitor supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the Branch Circuit Monitor 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 107).

► To modify IPv6 settings:

- Choose Device Settings > Network. The Network Configuration dialog appears.
- Click the IPv6 Settings tab.
- 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 Branch Circuit Monitor, 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>

Option	Description
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 ▪ 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 Branch Circuit Monitor 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 for illustrations.</p>

4. Click OK.

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

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 Branch Circuit Monitor may fail to connect to the given host.

Therefore, DNS server settings are important for external authentication. With appropriate DNS settings, the Branch Circuit Monitor 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 171).

Modifying Network Service Settings

The Branch Circuit Monitor 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 276).

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 Branch Circuit Monitor 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 Branch Circuit Monitor device so it is a more secure protocol than HTTP.

By default, any access to the Branch Circuit Monitor 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 Branch Circuit Monitor 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 142).

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 the SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the Branch Circuit Monitor device. Enabling SNMP communication allows the manager to retrieve the status of the Branch Circuit Monitor 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 180).

► To configure the SNMP communication:

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 "Notifications" tab is also visible. The "SNMP v1 / v2c Settings" section has a checked "enable" checkbox, a "Read Community String" field with the value "public", and an empty "Write Community String" field. The "SNMP v3 Settings" section has an unchecked "enable" checkbox. The "MIB-II System Group" section has three empty fields for "sysContact:", "sysName:", and "sysLocation:". At the bottom, there is a "Download MIB" button and "OK" and "Cancel" buttons.

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 Branch Circuit Monitor via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** (on page 267).*

4. Enter the MIB-II system group information, if applicable:
 - a. sysContact - the contact person in charge of the system being contacted
 - 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 Branch Circuit Monitor is used by the SNMP manager.

*Important: You must download the SNMP MIB for your Branch Circuit Monitor 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 273).*

6. Click OK.

► **To configure SNMP notification destinations:**

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
2. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
3. Click the Notifications tab.
4. Select the Enabled checkbox.
5. Select an SNMP notification type - SNMP v2c Trap, SNMP v2c Inform, SNMP v3 Trap, and SNMP v3 Inform.
6. 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 268) for details.
7. Click OK.

*Tip: The SNMP notification destinations can be also set in the Event Rule Settings dialog. See **Modifying an Action** (on page 217).*

Changing Modbus/TCP Settings

You can enable or disable the Modbus/TCP access to the Branch Circuit Monitor 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 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.

Enabling Service Advertisement

The Branch Circuit Monitor advertises all enabled services that are reachable using the IP network. This feature uses DNS-SD (Domain Name System-Service Discovery) and mDNS (multicast DNS). 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

This feature is enabled by default. 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 Branch Circuit Monitor. 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 107).*

► **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 Branch Circuit Monitor device manually, or link to a Network Time Protocol (NTP) server and let it set the date and time for the Branch Circuit Monitor.

► **To set the date and time:**

1. Choose Device Settings > Date/Time. The Configure Date/Time Settings dialog appears.
2. In the Time Zone field, click the drop-down arrow, and 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.
 - To set the date, delete existing numbers in the Date field and type new ones, or click the calendar icon  to select a date.
 - The time is measured in 24-hour format so enter 13 for 1:00pm, 14 for 2:00pm, and so on. You can enter the time by deleting existing numbers and typing new ones in the hour, minute and second fields, or clicking the arrows   to adjust each number.
 - 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.
You may click Check NTP Servers to verify the validity and accessibility of the specified NTP servers.


Note: If the Branch Circuit Monitor 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 Branch Circuit Monitor follows the NTP server sanity check per the IETF RFC. If your Branch Circuit Monitor has problems synchronizing with a Windows NTP server, see Windows NTP Server Synchronization Solution.

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

How to Use the Calendar

The calendar icon  next to the Date field is a convenient tool to quickly change the year, month and date.



► **To select a date using the calendar:**

1. To change the year shown in the calendar, do either of the following:
 - Press Ctrl+Up arrow or Ctrl+Down arrow to switch between years.
 - Click ▼, which is adjacent to the year, to show a list of years and months. Select the desired year from the list to the right and click OK. If the list does not show the desired year, click ◀ or ▶ to show additional years.



2. To change the month shown in the calendar, do one of the following:
 - Press Ctrl+Right arrow or Ctrl+Left arrow to switch between months.
 - Click ◀ or ▶ on the top of the calendar to switch between months.
 - Click ▼, which is adjacent to the year, to show a list of years and months. Select the desired month from the list to the left and click OK.
3. To select a date, click that date on the calendar.
 - Click Today if you want to select today.

Note: On the calendar, the date for today is marked with a red frame.

Setting Default Measurement Units

Default measurement units are applied to the Branch Circuit Monitor web and CLI interfaces across all users, including users accessing the device via external authentication servers. Default units apply only when users have not set their own preferred measurement units or the administrator has not changed preferred units for any user.

*Note: To set preferred measurement units for your own, see **Setting Up Your Preferred Measurement Units** (on page 146). If your preferences are different from the default measurement units, your preferences rather than the defaults apply to the Branch Circuit Monitor 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 Branch Circuit Monitor device supports connecting one of the following devices to its FEATURE port:

- Raritan Computer Interface Module (CIM) for KVM access. See Dominion KX II Configuration.

By default, the FEATURE port can automatically detect and display the device connected to the FEATURE port. You can change the mode applied to the FEATURE port so that the Branch Circuit Monitor web interface only displays the device in the manner you wish.

► **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 Branch Circuit Monitor automatically detects and displays the device connected to the FEATURE port. This is the default.
- Disabled: The FEATURE port is disabled so the Branch Circuit Monitor does not detect and display the connected device.
- A specific device type: The Branch Circuit Monitor 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
Power CIM	<p>Select this type when connecting the following Raritan product:</p> <ul style="list-style-type: none"> ▪ Raritan power CIM, D2CIM-PWR. This CIM is used to connect the Branch Circuit Monitor to the Raritan digital KVM switch, Dominion KX II.
Asset Strip	<p>Raritan asset sensors.</p> <hr/> <p><i>Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.</i></p>

4. Click OK.

Configuring the Serial Port

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

The Branch Circuit Monitor supports the use of one of the following devices via the serial interface:

- A computer or a Raritan's KVM product for console management.
- 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 Branch Circuit Monitor through the serial port, or there are communication problems.

Note: The serial port bit-rate change is needed when the Branch Circuit Monitor works in conjunction with Raritan's Dominion LX KVM switch. The Dominion LX only supports 19200 bps for communications over the serial interface.

You can set diverse bit-rate settings for console and modem operations. The Branch Circuit Monitor can detect the type of the connected device, 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 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 Branch Circuit Monitor, leave it at the default (115200 bps).

3. In the Modem Baud Rate field, select the baud rate used for the modem connected to the Branch Circuit Monitor.

► 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 Branch Circuit Monitor 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.

Specifying the Device Altitude

You must specify the Branch Circuit Monitor device's altitude above sea level if a Raritan 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 461).

The default altitude measurement unit is meter. You can have the measurement unit vary between meter and foot according to user credentials. See **Setting Up Your Preferred Measurement Units** (on page 146).

► **To specify the altitude of the Branch Circuit Monitor device:**

1. Click the BCM folder.

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Setup in the Settings section. The BCM 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor device's SNMP agent must be enabled for this feature to work. See **Enabling SNMP** (on page 266) for more details. In addition, using an NTP time server ensures accurately time-stamped measurements.*

Enabling Data Logging

By default, data logging is disabled. Only users having the "Administrator" or "Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration" permissions can enable or disable this feature. See **Setting Up Roles** (on page 147).

► **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 Branch Circuit Monitor in Step 4, it is NOT recommended and this capability may be removed in the future.

Configuring SMTP Settings

The Branch Circuit Monitor 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 223).

*Note: See **Event Rules and Actions** (on page 180) 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.

Checking the Internal Beeper State

The internal beeper can alert you if any overcurrent protector, including fuses and circuit breakers, has tripped or blown on the Branch Circuit Monitor. See *Beeper*. You can remotely check its state.

► To check the Branch Circuit Monitor beeper's state:

1. Click the BCM folder.

*Note: The PDU folder is named "BCM" by default. The name can be customized. See **Naming the Branch Circuit Monitor** (on page 103).*

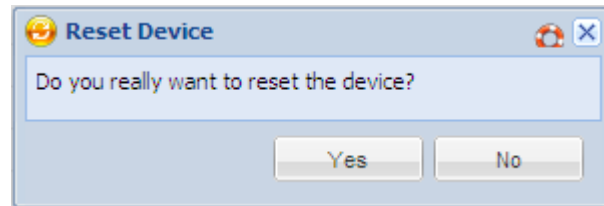
2. Locate the "Internal Beeper" section in the right pane. Either of the following states is displayed.
 - Off: The beeper is turned off.
 - Active: The beeper is turned on. A field titled "Activation reason" appears below the beeper state, indicating why the beeper sounds an alarm.
-
-

Rebooting the Branch Circuit Monitor Device

You can remotely reboot the Branch Circuit Monitor device via the web interface.

► **To reboot the device:**

1. Choose Maintenance > Unit Reset. The Reset Device dialog appears.



2. Click Yes to reset the Branch Circuit Monitor.
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 Branch Circuit Monitor 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.

Channel or CT Configuration

You can configure the CT settings, name each channel of the mains and branch circuits, or monitor their status remotely.

Important: Make sure the CTs are configured properly via the web interface, such as the maximum rating and turns ratio of each CT. Otherwise, the measurements generated may be incorrect.

Configuring the Mains Channels

To configure the mains channels properly, you must know the specifications of the CTs snapped onto the mains circuits. For information on the specifications of Raritan CTs, see **Raritan CT Specifications** (on page 408).

Warning: The information entered for the CT determines whether the Branch Circuit Monitor generates correct power measurements. Make sure you type or select the correct information. For any questions on the Raritan CT specifications, consult Raritan Technical Support.

► To configure the mains channels:

1. Click the BCM folder.

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Setup Circuits in the Settings section. The Circuit Setup dialog appears.
3. Select the channel group labeled "Mains: L1, L2, L3" and click Edit or simply double-click that channel group. The "Mains: L1, L2, L3 Configuration" dialog appears.
4. In the Transformer Type field, select the type of the mains CT you are using from the list. For Raritan mains CT, select Voltage.
5. In the Full-Scale Current (A) field, type the maximum current rating of your mains CT.

There are two types of Raritan mains CTs at the time of writing - one is rated at 200A and the other is rated at 250A. Other CTs (including CTs with higher ratings) may be available later. Check Raritan Technical Support for information.

- 200A CT - Type 200 because this CT's rating is 200A.
 - 250A CT - Type 250 because this CT's rating is 250A.
6. In the Full-Scale Voltage (mV) field, type the voltage supported by your mains CT. Both 200A- and 250A-rated Raritan mains CT have a full-scale voltage of 333mV so type 333 in this field.
 7. Click OK in the configuration dialog to retain the changes.
 8. Click OK.
 9. The Branch Circuit Monitor prompts you to restart this device for the new configuration to take effect. Click Continue to restart it.

Important: Clicking OK in the Circuit Setup dialog is required, or the channel configuration changes are not saved.

Configuring the Branch Circuit Channels

To configure the branch circuit channels, you must know the specifications of the CTs snapped onto the branch circuits and whether the monitored branch circuit is single-phase or 3-phase. For information on the specifications of Raritan CTs, see **Raritan CT Specifications** (on page 408).

Warning: The information entered for the CT determines whether the Branch Circuit Monitor generates correct power measurements. Make sure you type or select the correct information. For any questions on the Raritan CT specifications, consult Raritan Technical Support.

► **To configure the branch circuit channels:**

1. Click the BCM folder.

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Setup Circuits in the Settings section. The Circuit Setup dialog appears.
3. The branch circuit channels in this dialog are divided into various channel groups, each of which comprises 3 consecutive channels. Select the desired channel group and click Edit, or simply double-click that channel group. The "Branch Circuit: n1, n2, n3 Configuration" dialog appears (where n1, n2 and n3 are physical channel numbers).
4. In the Transformer Type field, select the type of the branch circuit CT you are using from the list. For Raritan branch circuit CTs, select Turns Ratio.
5. In the Turns Ratio field, type the turns ratio of the CTs connected to the selected channel group.

There are two types of Raritan branch circuit CTs at the time of writing - one is rated at 60A and the other is rated at 100A.

- 60A CT - Type 2000 because the turns ratio of this CT is 1:2000.
 - 100A CT - Type 4000 because the turns ratio of this CT is 1:4000.
6. Leave the Burden Resistor (Ohm) field at the default value (10) because the Branch Circuit Monitor has a built-in burden resistor of 10 ohm for branch circuit channels.
 7. Specify the type of circuit (line) monitored by each channel group. There are two ways to set the circuit types:

- a. If the selected channel group is monitoring three single-phase branch circuits, do the following and the three channels will be displayed as three "separate" single-phase channels in the navigation tree:
 - Make sure the 3-Phase Wiring checkbox is deselected.
 - Select the appropriate circuit type (L1, L2 or L3) in the Phase A Connection field. The Phase A refers to the channel that uses the same channel color as channel #1 on the Branch Circuit Monitor. See **Channel Convention** (on page 12) for available channel colors. The Phase A channels include channels #1, #4, #7, #10, #13 and so on.
 - Select the appropriate circuit type (L1, L2 or L3) in the Phase B Connection field. The Phase B refers to the channel that uses the same channel color as channel #2 on the Branch Circuit Monitor. The Phase B channels include channels #2, #5, #8, #11, #14 and so on.
 - Select the appropriate circuit type (L1, L2 or L3) in the Phase C Connection field. The Phase C refers to the channel that uses the same channel color as channel #3 on the Branch Circuit Monitor. The Phase C channels include channels #3, #6, #9, #12, #15 and so on.
 - If any channel is not connected to a CT or the CT connected to it is not snapped onto any conductor, select Unconnected instead.
- b. If the selected channel group is monitoring one 3-phase branch circuit, do the following and the three channels will be displayed as "one" 3-phase channel in the navigation tree:
 - Select the 3-Phase Wiring checkbox. The Phase A, B and C fields are automatically set to L1, L2 and L3 respectively.

The Branch Circuit Monitor will measure and display the unbalance load of a 3-phase channel.

8. Click OK in the configuration dialog to retain the changes.
9. To configure additional branch circuit channels, repeat Steps 3 to 7.
10. Click OK.
11. The Branch Circuit Monitor prompts you to restart this device for the new configuration to take effect. Click Continue to restart it.

Important: Clicking OK in the Circuit Setup dialog is required, or the channel configuration changes are not saved.

Naming the Mains Channels

You can customize the mains' name for identification. The customized name is followed by the label in parentheses.

Note: In this context, the label refers to the character used to identify the mains, that is, M.

► **To name the Mains:**

1. If the BCM folder is not expanded, expand it to show all components and component groups. See **Expanding the Tree** (on page 85).

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Mains M in the Dominion PX Explorer pane, and the Mains M page opens in the right pane.
3. Click Setup. The Mains M Setup dialog appears.
4. Type a new name in the Name field.
5. Click OK.

Naming Branch Circuit Channels

You can name each branch circuit channel for easily identifying their usage.

The customized name is followed by the label in parentheses.

*Note: In this context, the label refers to the physical channel number(s) associated with a branch circuit channel. For a single-phase branch circuit channel, the label is an individual channel number, such as 1, 2, 3 and so on. For a 3-phase branch circuit channel, the label consists of 3 channel numbers, such as 1-3, 4-6, 7-9 and so on. See **Configuring the Branch Circuit Channels** (on page 130).*

► **To name a branch circuit channel:**

1. Expand the Branch Circuits folder to show all branch circuit channels in the Dominion PX Explorer pane. See **Expanding the Tree** (on page 85).
2. Click the desired branch circuit channel in the Dominion PX Explorer pane, and the page for this branch circuit channel opens in the right pane.
3. Click Setup. The Branch Circuit N Setup dialog appears, where N is a channel number or a range of channel numbers.

Tip: This dialog can be also triggered by clicking Setup on the Branch Circuits page when the Branch Circuits folder is selected in the Dominion PX Explorer pane.

4. Type a new name in the Name field. It is strongly recommended to contain the panel number and usage of the monitored circuit in the customized channel name. See **Mapping Channels with Branch Circuits** (on page 35).
5. Click OK.

Monitoring the Mains Channels

You can view the mains' details, including its:

- Label (M)
- Customized name
- Mains sensor readings:
 - RMS current per line (A)
 - RMS voltage per line pair (V)
 - Active power (W)
 - Apparent power (VA)
 - Power factor
 - Active energy (Wh)
 - Unbalanced load percentage (for 3-phase models)

*Note: If a sensor row is colored, it means the sensor reading already crosses one of the thresholds or the sensor enters the alarmed state. See **The Yellow- or Red-Highlighted Sensors** (on page 91).*

There are two ways to access the mains information.

► **To get the overview of the mains status:**

1. Click the Dashboard icon in the PX Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the Mains section on the Dashboard page.

► **To view the mains' details:**

1. If the BCM folder is not expanded, expand it to show all components and component groups. See **Expanding the Tree** (on page 85).

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Mains M in the Dominion PX Explorer pane, and the Mains M page opens in the right pane.

Important: Measurements of the mains CTs may be incorrect if you have not properly configured your mains CTs using the web interface. See *Configuring the Mains Channels* (on page 129).

Monitoring the Branch Circuit Channels

The Dominion PX Explorer pane provides quick access to the branch circuit information. The branch circuit information, such as RMS current, active power, and power factor, is displayed immediately after a branch circuit channel's icon is selected in the navigation tree.

Note: RMS refers to Root Mean Square, a statistical method for measuring certain types of variables. In this context, it gives the value of current that is equivalent to a DC value.

Important: Measurements of the branch circuit CTs may be incorrect if you have not properly configured your branch circuit CTs using the web interface. See *Configuring the Branch Circuit Channels* (on page 130).

Monitoring All Channels

You can view the status of all branch circuit channels at a time.

► **To monitor all channels:**

1. If the BCM folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 85).

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click the Branch Circuits folder, and the Branch Circuits page opens in the right pane, showing all branch circuit channels with the following information:
 - Index number (#)
 - Channel name
 - Physical channel numbers in parentheses
 - Each channel's sensor readings:
 - RMS current (A)
 - Active power (W)

- Power factor

*Tip: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds. See **The Yellow- or Red-Highlighted Reading** (see "The Yellow- or Red-Highlighted Sensors" on page 91).*

Monitoring a Channel

To view a particular branch circuit channel's detailed information, follow this procedure.

► To monitor a channel:

1. If the Branch Circuits folder is not expanded, expand it to show all branch circuit channels. See **Expanding the Tree** (on page 85).
2. Click the branch circuit channel you want in the Dominion PX Explorer pane, and the channel's details are shown in the right pane, including:
 - Label (that is, channel number)
 - Channel name
 - Line(s) associated with this channel
 - Channel's sensor readings:
 - RMS current (A)
 - RMS voltage (V)
 - Active power (W)
 - Apparent power (VA)
 - Power factor
 - Active energy (Wh)
 - Line frequency (Hz), if available on your model
 - Unbalanced load percentage (for a 3-phase branch circuit only)

*Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds. See **The Yellow- or Red-Highlighted Reading** (see "The Yellow- or Red-Highlighted Sensors" on page 91).*

Setting Power Thresholds

Setting and enabling the thresholds causes the Branch Circuit Monitor 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 91).

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 reaches the critical level.

To avoid generating a large amount of alert events, the deassertion hysteresis for each threshold is enabled. You can change the default hysteresis value if necessary. For more information on the deassertion hysteresis, see **What is Deassertion Hysteresis?** (on page 139).

*Note: After setting the thresholds, remember to configure event rules. See **Event Rules and Actions** (on page 180).*

Setting the Mains Thresholds

You can set the mains thresholds so that the alerts are generated when any mains measurement, such as RMS current or voltage, crosses the thresholds.

► **To set the mains thresholds:**

1. If the BCM folder is not expanded, expand it to show all components and component groups. See **Expanding the Tree** (on page 85).

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Mains M in the Dominion PX Explorer pane, and the Mains M page opens in the right pane.
3. Click Setup. The Mains M Setup dialog appears.
4. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.

Click Edit or double-click the desired sensor. A threshold 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 enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 139).
 7. To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 141).
 8. Click OK in the threshold setup dialog to retain the changes.
 9. To set the thresholds for additional sensors, repeat Steps 4 to 9.
 10. Click OK.

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

Setting the Branch Circuit Thresholds

You can set up the thresholds, deassertion hysteresis and assertion timeout for a particular branch circuit channel.

The threshold values set for an individual branch circuit channel will override the bulk threshold values stored on that channel.

*Tip: To set up the thresholds, deassertion hysteresis and assertion timeout for multiple branch circuit channels at a time, see **Bulk Configuration for Branch Circuit Thresholds** (on page 138).*

► To set the thresholds for a branch circuit channel:

1. If the Branch Circuits folder is not expanded, expand it to show all branch circuit channels. See ***Expanding the Tree*** (on page 85).
2. Click the desired branch circuit channel in the Dominion PX Explorer pane, and the page for this branch circuit channel opens in the right pane.
3. Click Setup. The Branch Circuit N Setup dialog appears, where N is a channel number or a range of channel numbers.

Tip: This dialog can be also triggered by clicking Setup on the Branch Circuits page when the Branch Circuits folder is selected in the Dominion PX Explorer pane.

4. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.

Click Edit or double-click the desired sensor. A threshold 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 enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See **What is Deassertion Hysteresis?** (on page 139).
7. To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See **What is Assertion Timeout?** (on page 141).
8. Click OK in the threshold setup dialog to retain the changes.
9. To set the thresholds for additional sensors, repeat Steps 4 to 9.
10. Click OK.

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

Bulk Configuration for Branch Circuit Thresholds

The Branch Circuit Monitor allows you to set the power thresholds for multiple branch circuits at a time so that you can save time when configuring a number of branch circuit thresholds.

*Note: To set the power thresholds for an individual branch circuit channel, you can either follow the instructions below or those described in the section **Setting the Branch Circuit Thresholds** (on page 137).*

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

1. If the BCM folder is not expanded, expand it to show all components and component groups. See **Expanding the Tree** (on page 85).

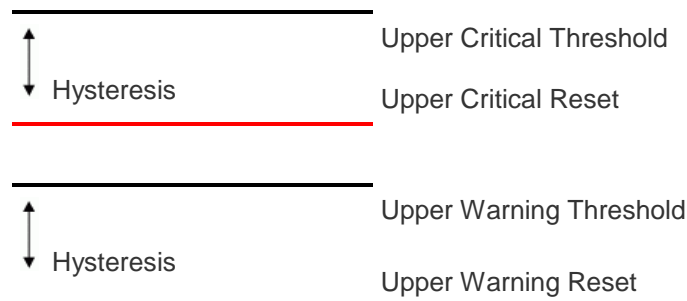
*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

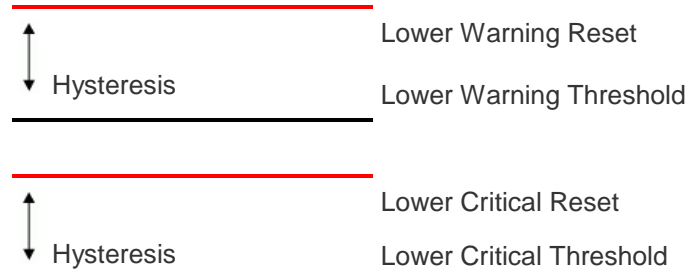
2. Click the Branch Circuits folder. The Branch Circuits page opens.
3. Click Bulk Setup. The Branch Circuit Threshold Bulk Setup dialog appears, with a list of all branch circuit channels.

4. In the Show Outlet Sensors of Type field, select the type of power thresholds you want to configure.
5. Select desired branch circuit channels by having their corresponding checkboxes selected.
 - To select all channels, select the checkbox labeled Sensor in the header row, and all checkboxes are selected.
 - To select partial channels, select the corresponding checkboxes of those channels by clicking on their checkboxes.
 - To deselect any channel, just click on the checkbox once again.
6. Click Edit Thresholds. The threshold bulk setup dialog appears.
7. 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.
8. To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 139).
9. To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 141).
10. Click OK.

What is Deassertion Hysteresis?

The hysteresis setting determines when a threshold condition is reset. This diagram illustrates how hysteresis values relate to thresholds:





The hysteresis values define a reset threshold. For upper thresholds, the measurement must fall past this reset threshold before a deassertion event is generated. For lower thresholds, the measurement must rise above this reset threshold before a deassertion event is generated.

Example: When Hysteresis is Useful

This example demonstrates when a deassertion hysteresis is useful.

The current critical threshold for L1 is set to 10 amps (A). The current draw rises to 11A, triggering a Current Critical alert. The current then continues to fluctuate between 9.1A and 11A.

With the hysteresis set to 1A, the Branch Circuit Monitor continues to indicate that the current on the branch circuit L1 is above critical. Without the hysteresis (that is, the hysteresis is set to zero), the Branch Circuit Monitor would de-assert the condition each time the current dropped to 9.9A, and re-assert the condition each time the current reached 10A or higher. With the fluctuating current, this could result in a number of repeating SNMP traps, and/or an e-mail account full of repeating SMTP alert notifications.

Example: When to Disable Hysteresis

This is an example of when you want to disable the hysteresis for a branch circuit channel #1. Hysteresis is disabled when its value is set to zero.

The upper warning threshold for current in the branch circuit channel #1 is set to 8A. In normal usage, the branch circuit #1 draws 7.6A of current. A spike in demand causes the current to reach 9A, triggering an alert. The current then settles to the normal draw of 7.6A.

With the hysteresis disabled, the Branch Circuit Monitor de-asserts the condition once the current drops to 7.9A. With the hysteresis enabled and set to 1A, the branch circuit #1 would still be considered above the warning threshold as long as the current never dropped to 7A. The condition would not de-assert, even if the current returns to normal.

What is Assertion Timeout?

When the assertion timeout is enabled, the Branch Circuit Monitor device asserts any warning or critical condition only after either of the following occurs:

- The Branch Circuit Monitor generates a specified number of consecutive samples crossing a particular threshold.
- The Branch Circuit Monitor generates samples crossing a particular threshold for a specified period of time.

This prevents a number of threshold alerts from being generated if the measurements return to normal immediately after rising above any upper threshold or dropping below any lower threshold.

User Management

The Branch Circuit Monitor 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 147).

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

Creating a User Profile

Creating new users adds a new login to the Branch Circuit Monitor.

► 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	<p>The name the user enters to log in to the Branch Circuit Monitor.</p> <ul style="list-style-type: none"> ▪ The name can be 4 to 32 characters long. ▪ It is case sensitive. ▪ Spaces are NOT permitted
Full Name	The user's first and last names.
Password, Confirm Password	<p>The password the user enters to log in. Type it first in the Password field and then again in the Confirm Password field.</p> <ul style="list-style-type: none"> ▪ The password can be 4 to 64 characters long. ▪ It is case sensitive. ▪ Spaces are permitted.
Telephone Number	A phone number where the user can be reached.
eMail Address	<p>An email address where the user can be reached.</p> <ul style="list-style-type: none"> ▪ The email can be up to 64 characters long. ▪ It is case sensitive.

4. Select the Enabled checkbox. This is required so the user can log in to the Branch Circuit Monitor 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** (see "**Configuring the SNMP Settings**" on page 114).*

- 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>

Field	Description
Privacy Pass Phrase	Type the privacy pass phrase in this field if the "Use Authentication Pass Phrase as Privacy Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII printable characters.
Confirm Privacy Pass Phrase	Re-type the same privacy pass phrase for confirmation.
Authentication Protocol	Click the drop-down arrow and select the desired authentication protocol from the list. Two protocols are available: <ul style="list-style-type: none"> ▪ MD5 ▪ SHA-1 (default)
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 112).
 - 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 147) 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 148).
 - *Create a new role by clicking the Manage Roles button:* See **Creating a Role** (on page 147).

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 146).*

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 142).
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 148).
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.

Changing the User List View

You may change the number of displayed columns or re-sort the list for better viewing the data. See **Changing the View of a List** (on page 92).

Setting Up Your Preferred Measurement Units

The measurement units used in your Branch Circuit Monitor 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 142).*

*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 121) for information on changing default measurement units.*

► **To change the measurement units applied to your Branch Circuit Monitor graphical 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 Branch Circuit Monitor 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:
 - Acknowledge Alarms
 - View Event Settings
 - View Local Event Log
 - Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
 - Change Own Password

The Operator role is assigned to a newly created user profile by default. See **Creating a User Profile** (on page 142).

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 142) or **Modifying a User Profile** (on page 145).

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.

Changing the Role List View

You may re-sort the list for better viewing the data. See **Changing the View of a List** (on page 92).

Access Security Control

The Branch Circuit Monitor 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 165) and **Setting Up External Authentication** (on page 171).*

Forcing HTTPS Encryption

You can force all accesses to the Branch Circuit Monitor via HTTP to be redirected to HTTPS. See **Changing HTTP(S) Settings** (on page 111).

Configuring the Firewall

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

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

By default the firewall is disabled.

► **To configure the firewall:**

1. Enable the firewall. See **Enabling the Firewall** (on page 151).
2. Set the default policy. See **Changing the Default Policy** (on page 151).
3. Create firewall rules specifying which addresses to accept and which ones to discard. See **Creating Firewall Rules** (on page 152).

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 Branch Circuit Monitor 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 Branch Circuit Monitor or receive any data from the Branch Circuit Monitor.

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 Branch Circuit Monitor to all IP addresses.
- Drop: Discards traffic sent from the Branch Circuit Monitor to all IP addresses, without sending any failure notification to the destination host.
- Reject: Discards traffic sent from the Branch Circuit Monitor 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 Branch Circuit Monitor, 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 Branch Circuit Monitor 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 Branch Circuit Monitor.

- **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
<p>Insert a rule between two existing rules</p>	<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: Accept

#	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: Accept

#	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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 401).*

► 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 Branch Circuit Monitor 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 Branch Circuit Monitor, 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 Branch Circuit Monitor.

Enabling Strong Passwords

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor restricted service agreement (security banner) if you want to require users to read and accept a security agreement when they log in to the Branch Circuit Monitor.

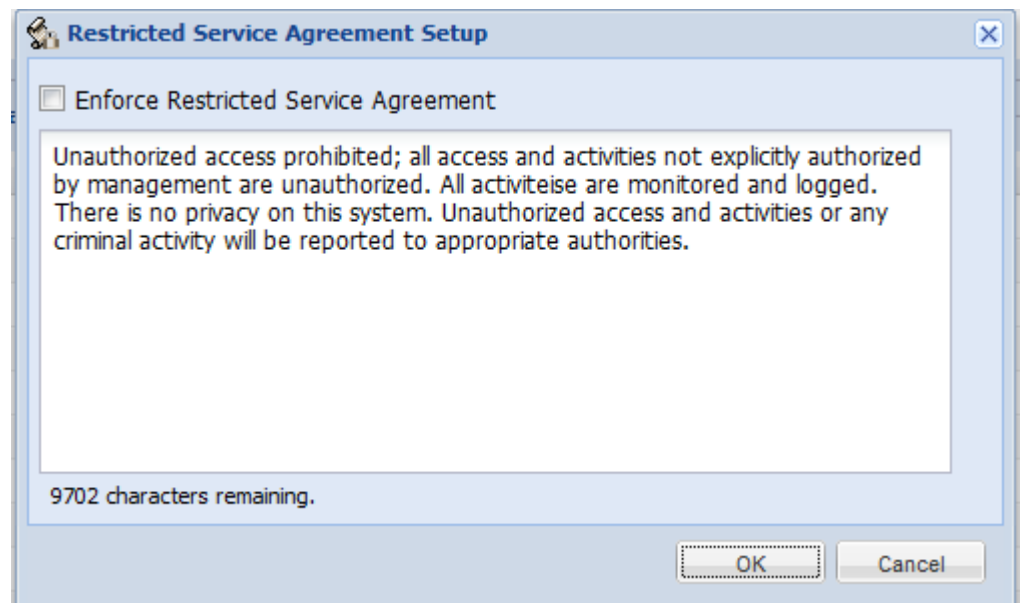
A default agreement is provided. You can edit or replace the default text as needed by typing directly in the security dialog or pasting text into it.

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

► 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 Branch Circuit Monitor. Do either of the following, or you cannot successfully log in to the Branch Circuit Monitor:

- 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 161).
2. Set the default policy. See **Changing the Default Policy** (on page 162).
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 162).

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 role

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

- 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:

- Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
- To modify the IPv4 firewall rules, click the IPv4 tab. To modify the IPv6 firewall rules, click the IPv6 tab.
- 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.
- Select the rule to be modified in the rules list.
- Click Edit or double-click the rule. The Edit Rule dialog appears.
- Make changes to the information shown.
- 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:

- Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
- To sort the IPv4 firewall rules, click the IPv4 tab. To sort the IPv6 firewall rules, click the IPv6 tab.
- 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.
- Select a specific rule by clicking it.
- 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 Branch Circuit Monitor, 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 Branch Circuit Monitor 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 150) for instructions on forcing users to employ TLS when connecting to the Branch Circuit Monitor.*

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

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

Certificate Signing Request

When appropriate certificate and key files for the Branch Circuit Monitor are NOT available, one of the alternatives is to create a CSR and private key on the Branch Circuit Monitor 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 Branch Circuit Monitor 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.

Field	Type this information
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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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.

- 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 Branch Circuit Monitor device.

► To install the certificate:

- Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
- Click the New SSL Certificate tab.
- In the Certificate File field, click Browse to select the certificate file provided by the CA.
- Click Upload. The certificate is installed on the Branch Circuit Monitor device.

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

- Click Close to quit the dialog.

Creating a Self-Signed Certificate

When appropriate certificate and key files for the Branch Circuit Monitor 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:

- Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
- Click the New SSL Certificate tab.
- 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.

Field	Type this information
Common Name	The fully qualified domain name (FQDN) of your Branch Circuit Monitor device.
Email Address	An email address where you or another administrative user can be reached.
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 Branch Circuit Monitor 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 Branch Circuit Monitor device, click "Delete Key and Certificate".
6. If you installed the self-signed certificate in Step 5, after the installation completes, the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor device for backup or other operations. For example, you can install the files on a replacement Branch Circuit Monitor device, add the certificate to your browser and so on.

► **To download the certificate and key files from the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor must be authenticated. The Branch Circuit Monitor supports the access using one of the following authentication mechanisms:

- Local database of user profiles on the Branch Circuit Monitor device
- Lightweight Directory Access Protocol (LDAP)
- Remote Access Dial-In User Service (RADIUS) protocol

By default, the Branch Circuit Monitor 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 Branch Circuit Monitor with information about the external Authentication and Authorization (AA) server.

If both local and external authentication is needed, create user profiles on the Branch Circuit Monitor in addition to providing the external AA server's data.

When configured for external authentication, all Branch Circuit Monitor users must have an account on the external AA server.

Local-authentication-only users will have no access to the Branch Circuit Monitor except for the admin, who always can access the Branch Circuit Monitor.

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 Branch Circuit Monitor 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 Branch Circuit Monitor. 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 223).

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. LDAP over SSL - Select this checkbox if you would like to use Transport Layer Security (TLS) encryption. TLS is a cryptographic protocol that allows the Branch Circuit Monitor to communicate securely with the LDAPS server.
7. Port - The default Port is 389. Either use the standard LDAP TCP port or specify another port.

8. SSL Port - The default is 636. Either use the default port or specify another port. This field is enabled when the "LDAP over SSL" checkbox is selected.
9. Enable verification of LDAP Server Certificate - Select this checkbox if you would like the Branch Circuit Monitor to verify the validity of the selected LDAP server certificate. For example, the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor, 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 445).

For more information on RADIUS configuration, see **RADIUS Configuration Illustration** (on page 414).

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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor device successfully connects to one of the listed servers.

Note: After successfully connecting to one external authentication server, the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor authenticates users against the local database stored on the Branch Circuit Monitor 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 Branch Circuit Monitor follows these rules for authentication:

- When any of the remote authentication servers in the access list is accessible, the Branch Circuit Monitor authenticates against the connected authentication server only.
- When the connection to all remote authentication servers fails, the Branch Circuit Monitor 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 Branch Circuit Monitor is shipped with four built-in event rules, which cannot be deleted.

- **System Event Log Rule:** This causes ANY event occurred to the Branch Circuit Monitor 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 Branch Circuit Monitor. It is disabled by default.
- **System Tamper Detection Alarmed:** This causes the Branch Circuit Monitor to send alarm notifications if a DX tamper sensor has been connected and the Branch Circuit Monitor detects that the tamper sensor enters the alarmed state.
- **System Tamper Detection Unavailable:** This causes the Branch Circuit Monitor to send alarm notifications if a DX tamper sensor has been connected and the Branch Circuit Monitor 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 Branch Circuit Monitor does in certain situations and is composed of two parts:

- **Event:** This is the situation where the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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.

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 183).

Action	Function
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 183).
External beeper	Enables or disables the connected external beeper, or causes it to enter an alarm cycle. See External Beeper (on page 185).
Log event message	Records the selected events in the internal log. See Log an Event Message (on page 186).
Send snapshots via email	Emails the snapshots captured by a connected Logitech® webcam (if available). See Send a Snapshot via Email (on page 187).
Send email	Emails a textual message. See Send Email (on page 188).
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See Send an SNMP Notification (on page 189).
Syslog message	Makes the Branch Circuit Monitor automatically forward event messages to the specified syslog server. See Syslog Message (on page 191).
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See Send Sensor Report (on page 193).
Send SMS message	Sends a message to a mobile phone. See Send SMS Message (on page 195).
Record snapshots to webcam storage	Makes a connected webcam start or stop taking snapshots. See Record Snapshots to Webcam Storage (on page 197).

- 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 Branch Circuit Monitor 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.

► **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 Branch Circuit Monitor 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 Branch Circuit Monitor, the Branch Circuit Monitor 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 Branch Circuit Monitor, you can configure the Branch Circuit Monitor 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*.

*Tip: To send the asset sensor data at a regular interval, schedule this action. See **Scheduling an Action** (on page 203). 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.
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 126) 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 Branch Circuit Monitor placeholders. The placeholders represent information is pulled from the Branch Circuit Monitor 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 210) 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 126) for the information of each field. Default messages are sent based on the event. See Default Log Messages 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 210) 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 223).

► 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 Branch Circuit Monitor 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.

- Inlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor and active energy.
- Outlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor, active energy and outlet state (for outlet-switching capable PDUs only).
- Overcurrent protector sensors, including RMS current and tripping state.
- Peripheral device sensors, which can be any Raritan environmental sensor packages connected to the Branch Circuit Monitor, 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 the Add button  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 the Delete button . 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 210).*

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 Branch Circuit Monitor placeholders. The placeholders represent information which is pulled from the Branch Circuit Monitor and inserted into the message.

A supported modem, such as the Cinterion® GSM MC52i modem, must be plugged in to the Branch Circuit Monitor in order to send SMS messages.

Note: The Branch Circuit Monitor 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 210) 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 210) 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 Branch Circuit Monitor 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 Branch Circuit Monitor, you can set up the Branch Circuit Monitor 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 Branch Circuit Monitor, see DX Sensor Packages.

► 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 Branch Circuit Monitor is ten (10). If you set it for a number greater than ten and the storage location is on the Branch Circuit Monitor, after the tenth snapshot is taken and stored, the oldest snapshots are overwritten.

*Tip: By default, the storage location is on the Branch Circuit Monitor. You can specify a remote server to store the snapshots. See **Configuring Webcam Storage** (on page 257).*

- 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 when each snapshot is 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 Branch Circuit Monitor 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 Branch> refers to all branch circuit channels.

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	<p>Available radio buttons include "Asserted," "Deasserted" and "Both."</p> <ul style="list-style-type: none"> ▪ Asserted: The Branch Circuit Monitor takes the action only when the event occurs. This means the status of the described event transits from FALSE to TRUE. ▪ Deasserted: The Branch Circuit Monitor takes the action only when the event condition disappears. This means the status of the described event transits from TRUE to FALSE. ▪ Both: The Branch Circuit Monitor 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	<p>Available radio buttons include "Alarmed," "No longer alarmed" and "Both."</p> <ul style="list-style-type: none"> ▪ Alarmed: The Branch Circuit Monitor takes the action only when the chosen sensor enters the alarmed state, that is, the abnormal state. ▪ No longer alarmed: The Branch Circuit Monitor takes the action only when the chosen sensor returns to normal. ▪ Both: The Branch Circuit Monitor takes the action both when the chosen sensor enters or quits the alarmed state.
Sensor availability	<p>Available radio buttons include "Unavailable," "Available" and "Both."</p> <ul style="list-style-type: none"> ▪ Unavailable: The Branch Circuit Monitor takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: The Branch Circuit Monitor takes the action only when the chosen sensor is detected and becomes available. ▪ Both: The Branch Circuit Monitor takes the action both when the chosen sensor becomes unavailable or available.

Event types	Radio buttons
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 Branch Circuit Monitor takes the action only when the network link state changes from down to up. ▪ Link state is down: The Branch Circuit Monitor takes the action only when the network link state changes from up to down. ▪ Both: The Branch Circuit Monitor 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 Branch Circuit Monitor takes the action only when the chosen function is enabled. ▪ Disabled: The Branch Circuit Monitor takes the action only when the chosen function is disabled. ▪ Both: The Branch Circuit Monitor 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 Branch Circuit Monitor takes the action only when the selected user logs in. ▪ Logged out: The Branch Circuit Monitor takes the action only when the selected user logs out. ▪ Both: The Branch Circuit Monitor 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 Branch Circuit Monitor takes the action only when the specified user accepts the restricted service agreement. Declined: The Branch Circuit Monitor takes the action only when the specified user rejects the restricted service agreement. Both: The Branch Circuit Monitor 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 Branch Circuit Monitor takes the action only when the monitoring of any specified server starts. Monitoring stopped: The Branch Circuit Monitor takes the action only when the monitoring of any specified server stops. Both: The Branch Circuit Monitor 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 Branch Circuit Monitor takes the action only when any specified server becomes inaccessible. Reachable: The Branch Circuit Monitor takes the action only when any specified server becomes accessible. Both: The Branch Circuit Monitor takes the action when any specified server becomes either inaccessible or accessible.

Event types	Radio buttons
RF Code tag connection or disconnection	<p>Available radio buttons include "Connected," "Disconnected" and "Both."</p> <ul style="list-style-type: none"> Connected: Branch Circuit Monitor takes the action only when an RF Code tag is physically connected to it. Disconnected: Branch Circuit Monitor takes the action only when an RF Code tag is physically disconnected from it. Both: Branch Circuit Monitor takes the action both when the RF Code tag is physically connected to it and when it is disconnected

Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.

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 Branch Circuit Monitor 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 Branch Circuit Monitor 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	<p>The hourly option sets the frequency to either of the following:</p> <ul style="list-style-type: none"> One hour - then set the Minute field to 0 (zero). Between one and two hours, such as one hour and one minute, one hour and thirty minutes, or one hour and 59 minutes. In this case, specify a non-zero number in the Minute field.
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 every day.
Weekly	Both the day and time must be specified for the weekly option. Days range from Sunday to Monday.
Monthly	<p>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.</p> <p>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.</p>
Yearly	<p>This option requires three settings:</p> <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 181).

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.

Default Log Messages

Following are default log messages triggered and emailed to specified recipients when Branch Circuit Monitor events occur (are TRUE) or, in some cases, do not occur (are FALSE). See **Send Email** (on page 188) 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*
Device > System started	System started.	
Device > System reset	System reset performed by user '[USERNAME]' from host '[USERIP]'.	
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].	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > System started	System started.	
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.	
Device > Sending SNMP inform failed or no response	Sending SNMP inform to manager [SNMPMANAGER]:[SNMPMANAGERPORT] 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.	
User Activity > * > User logon state	User '[USERNAME]' from host	User '[USERNAME]' from host '[USERIP]'

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > System started	System started.	
	'[USERIP]' logged in.	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]'.	
Mains > * > Sensor > * > Unavailable	Sensor '[MAINSSENSOR]' on inlet '[MAINS]' unavailable.	Sensor '[MAINSSENSOR]' on inlet '[MAINS]' available.
Mains > * > Sensor > * > Above upper critical threshold	Sensor '[MAINSSENSOR]' on inlet '[MAINS]' asserted 'above upper critical'.	Sensor '[MAINSSENSOR]' on inlet '[MAINS]' deasserted 'above upper critical'.
Mains > * > Sensor > * > Above	Sensor '[MAINSSENSOR]' on inlet	Sensor '[MAINSSENSOR]' on inlet '[MAINS]'


Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > System started	System started.	
upper warning threshold	'[MAINS]' asserted 'above upper warning'.	deasserted 'above upper warning'.
Mains > * > Sensor > * > Below lower warning threshold	Sensor '[MAINSENSOR]' on inlet '[MAINS]' asserted 'below lower warning'.	Sensor '[MAINSENSOR]' on inlet '[MAINS]' deasserted 'below lower warning'.
Mains > * > Sensor > * > Below lower critical threshold	Sensor '[MAINSENSOR]' on inlet '[MAINS]' asserted 'below lower critical'.	Sensor '[MAINSENSOR]' on inlet '[MAINS]' deasserted 'below lower critical'.
Mains > * > Pole > * > Sensor > * > Unavailable	Sensor '[POLESENSOR]' on pole '[MAINPOLE]' of inlet '[MAINS]' unavailable.	Sensor '[POLESENSOR]' on pole '[MAINPOLE]' of inlet '[MAINS]' available.
Mains > * > Pole > * > Sensor > * > Above upper critical threshold	Sensor '[POLESENSOR]' on pole '[MAINPOLE]' of inlet '[MAINS]' asserted 'above upper critical'.	Sensor '[POLESENSOR]' on pole '[MAINPOLE]' of inlet '[MAINS]' deasserted 'above upper critical'.
Mains > * > Pole > * > Sensor > * > Above upper warning threshold	Sensor '[POLESENSOR]' on pole '[MAINPOLE]' of inlet '[MAINS]' asserted 'above upper warning'.	Sensor '[POLESENSOR]' on pole '[MAINPOLE]' of inlet '[MAINS]' deasserted 'above upper warning'.
Mains > * > Pole > * > Sensor > * > Below lower warning threshold	Sensor '[POLESENSOR]' on pole '[MAINPOLE]' of inlet '[MAINS]' asserted 'below lower warning'.	Sensor '[POLESENSOR]' on pole '[MAINPOLE]' of inlet '[MAINS]' deasserted 'below lower warning'.
Mains > * > Pole > * > Sensor > * > Below lower critical threshold	Sensor '[POLESENSOR]' on pole '[MAINPOLE]' of inlet '[MAINS]' asserted 'below lower critical'.	Sensor '[POLESENSOR]' on pole '[MAINPOLE]' of inlet '[MAINS]' deasserted 'below lower critical'.
Branch Circuits > * > Sensor > * > Unavailable	Sensor '[BRANCHSENSOR]' on outlet '[BRANCH]' unavailable.	Sensor '[BRANCHSENSOR]' on outlet '[BRANCH]' available.
Branch Circuits > * > Sensor > * > Above upper critical threshold	Sensor '[BRANCHSENSOR]' on outlet '[BRANCH]' asserted 'above upper critical'.	Sensor '[BRANCHSENSOR]' on outlet '[BRANCH]' deasserted 'above upper critical'.
Branch Circuits > * > Sensor > * > Above upper warning threshold	Sensor '[BRANCHSENSOR]' on outlet '[BRANCH]' asserted 'above upper warning'.	Sensor '[BRANCHSENSOR]' on outlet '[BRANCH]' deasserted 'above upper warning'.
Branch Circuits > * > Sensor > * > Below lower warning threshold	Sensor '[BRANCHSENSOR]' on outlet '[BRANCH]' asserted 'below lower warning'.	Sensor '[BRANCHSENSOR]' on outlet '[BRANCH]' deasserted 'below lower warning'.
Branch Circuits > * > Sensor > * > Below lower critical threshold	Sensor '[BRANCHSENSOR]' on outlet '[BRANCH]' asserted 'below lower critical'.	Sensor '[BRANCHSENSOR]' on outlet '[BRANCH]' deasserted 'below lower critical'.
Branch Circuits > * > Pole > * > Sensor > Unavailable	Sensor '[POLESENSOR]' on pole '[BRANCHPOLE]' of outlet	Sensor '[POLESENSOR]' on pole '[BRANCHPOLE]' of outlet '[BRANCH]'

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > System started	System started.	
	'[BRANCH]' unavailable.	available.
Branch Circuits > * > Pole > * > Sensor > Above upper critical threshold	Sensor '[POLESENSOR]' on pole '[BRANCHPOLE]' of outlet '[BRANCH]' asserted 'above upper critical'.	Sensor '[POLESENSOR]' on pole '[BRANCHPOLE]' of outlet '[BRANCH]' deasserted 'above upper critical'.
Branch Circuits > * > Pole > * > Sensor > Above upper warning threshold	Sensor '[POLESENSOR]' on pole '[BRANCHPOLE]' of outlet '[BRANCH]' asserted 'above upper warning'.	Sensor '[POLESENSOR]' on pole '[BRANCHPOLE]' of outlet '[BRANCH]' deasserted 'above upper warning'.
Branch Circuits > * > Pole > * > Sensor > Below lower warning threshold	Sensor '[POLESENSOR]' on pole '[BRANCHPOLE]' of outlet '[BRANCH]' asserted 'below lower warning'.	Sensor '[POLESENSOR]' on pole '[BRANCHPOLE]' of outlet '[BRANCH]' deasserted 'below lower warning'.
Branch Circuits > * > Pole > * > Sensor > Below lower critical threshold	Sensor '[POLESENSOR]' on pole '[BRANCHPOLE]' of outlet '[BRANCH]' asserted 'below lower critical'.	Sensor '[POLESENSOR]' on pole '[BRANCHPOLE]' of outlet '[BRANCH]' deasserted 'below lower critical'.
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 threshold	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 threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Below lower warning threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning' at [READING].

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > System started	System started.	
Peripheral Device Slot > * > Numeric Sensor > Below lower critical threshold	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].
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.	
RF Code Tag > Connected	RF Code tag has been connected.	RF Code tag has been disconnected.

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

Placeholder	Definition
[AMSBLADESLOTPOSITION]	The (horizontal) slot position, an action applies to
[AMSLEDCOLOR]	The RGB LED color
[AMSLEDMODE]	The LED indication mode
[AMSLEDOPMODE]	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
[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
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSORSLLOT]	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

Placeholder	Definition
[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
[RADIUSERRORDESC]	A Radius error occurred
[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

Placeholder	Definition
[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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 268).*

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.

Sample Branch Circuit-Level Event Rule

In this example, we want the Branch Circuit Monitor to send SNMP traps to the SNMP manager for any sensor change event of the branch circuit channel #3.

*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 268).*

The event rule is set like this:

- Event: Branch Circuits > Branch 3 > Sensor > Any sub-event
- Actions: System SNMP Notification Action

► To create the above event rule:

1. Select Event > Branch Circuits to indicate we are specifying an event at the branch circuit level.
2. Select "Branch 3" from the submenu because that is the branch circuit channel in question.
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 branch circuit 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 branch circuit channel 3's 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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

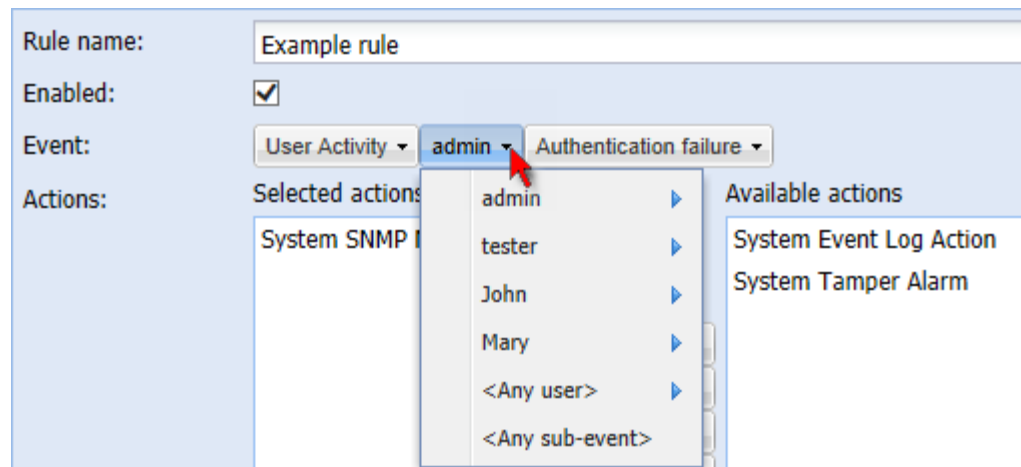
You can change an event rule's event, action, trigger condition and other settings, if any.


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 181) 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 Branch Circuit Monitor to generate an alert. The measurement then returns to a value within the threshold, but the Branch Circuit Monitor does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the Branch Circuit Monitor uses. See ***What is Deassertion Hysteresis*** (see "***What is Deassertion Hysteresis?***" on page 139).

Viewing Connected Users

You can see which users are connected to the Branch Circuit Monitor device and their status. If you have administrator privileges, you can terminate any user's connection to the Branch Circuit Monitor 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 Branch Circuit Monitor. <ul style="list-style-type: none"> ▪ Web GUI: Refers to the Branch Circuit Monitor 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. <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. You may change the sorting order of the list if necessary. See **Changing the Sorting** (on page 93).
4. 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 253).*

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the Branch Circuit Monitor 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.

Adding IT Devices for Ping Monitoring

Branch Circuit Monitor can monitor the accessibility of any type of IT equipment, such as database servers, remote authentication servers, power distribution units (PDUs), and so on.

Branch Circuit Monitor 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 Branch Circuit Monitor 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 180).*

► 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.
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.

Field	Description
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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor can declare that the monitored device is reachable or unreachable.

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 Branch Circuit Monitor 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 Branch Circuit Monitor device and the monitored equipment is not reliably established yet.

4. You may change the sorting order of the list if necessary. Or hide some columns. See **Changing the View of a List** (on page 92).
5. Click Close to quit the dialog.

Managing Event Logging

By default, the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor can monitor the environmental conditions, such as temperature and humidity, where environmental sensors are placed. If an actuator is connected to the Branch Circuit Monitor, you can use it to control a system or mechanism.

► **To add environmental sensors and actuators:**

1. Physically connect environmental sensor packages to the Branch Circuit Monitor device. See **Connecting Environmental Sensor Packages** (on page 40).
2. Log in to the Branch Circuit Monitor web interface. The Branch Circuit Monitor 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** (see "**Identifying Environmental Sensors**" on page 226).
4. The Branch Circuit Monitor 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** (see "**Managing Environmental Sensors and Actuators**" on page 229).
5. Configure the sensors and actuators. See **Configuring Environmental Sensors or Actuators** (see "**Configuring Environmental Sensors**" on page 231). 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

A DPX environmental sensor package includes a serial number tag on the sensor cable.



A DPX2 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 Branch Circuit Monitor.

► To identify each detected environmental sensor:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See **Expanding the Tree** (on page 85).

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Peripheral Devices in the Explorer pane, and the Peripheral Devices page opens in the right pane.

Peripheral Devices									
<input type="checkbox"/>	ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
<input type="checkbox"/>	1	Temperature 1	Port 1	AEI7A00022	Temperature			24.2 °C	normal
<input type="checkbox"/>	2	Humidity 1	Port 1	AEI7A00022	Humidity			60 %	normal
<input type="checkbox"/>	3	Temperature 2	Port 1	AEI7A00021	Temperature			24.4 °C	normal
<input type="checkbox"/>	4	Humidity 2	Port 1	AEI7A00021	Humidity			59 %	normal
<input type="checkbox"/>	5	On/Off 1	Port 1	PRC0190292	Contact (On/Off)	1			normal
<input type="checkbox"/>	6	On/Off 2	Port 1	PRC0190292	Contact (On/Off)	2			normal

3. 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 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 Branch Circuit Monitor.

► **To identify each detected environmental sensor or actuator via serial numbers:**

1. Click Peripheral Devices in the Explorer pane, and the Peripheral Devices page opens in the right pane.
2. Match the serial number from the tag to those listed in the sensor table.

Peripheral Devices									
<input type="checkbox"/>	ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
<input type="checkbox"/>	1	Temperature 1	Port 1	AEI7A00022	Temperature			24.2 °C	normal
<input type="checkbox"/>	2	Humidity 1	Port 1	AEI7A00022	Humidity			60 %	normal
<input type="checkbox"/>	3	Temperature 2	Port 1	AEI7A00021	Temperature			24.4 °C	normal
<input type="checkbox"/>	4	Humidity 2	Port 1	AEI7A00021	Humidity			59 %	normal
<input type="checkbox"/>	5	On/Off 1	Port 1	PRC0190292	Contact (On/Off)	1			normal
<input type="checkbox"/>	6	On/Off 2	Port 1	PRC0190292	Contact (On/Off)	2			normal

Matching the Position

Both DPX2 and DX sensor packages can be daisy chained. The Branch Circuit Monitor 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:**

1. Click Peripheral Devices in the Explorer pane, and the Peripheral Devices page opens in the right pane.
2. Locate the Position column, which shows one or two pieces of position information - the sensor port number and, if the sensor package is DPX2 or DX series, the sensor or actuator's location in a chain.

Peripheral Devices									
	ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
<input type="checkbox"/>	1	Temperature 1	Port 1	AEI7A00022	Temperature			24.2 °C	normal
<input type="checkbox"/>	2	Humidity 1	Port 1	AEI7A00022	Humidity			60 %	normal
<input type="checkbox"/>	3	Temperature 2	Port 1	AEI7A00021	Temperature			24.4 °C	normal
<input type="checkbox"/>	4	Humidity 2	Port 1	AEI7A00021	Humidity			59 %	normal
<input type="checkbox"/>	5	On/Off 1	Port 1	PRC0190292	Contact (On/Off)	1			normal
<input type="checkbox"/>	6	On/Off 2	Port 1	PRC0190292	Contact (On/Off)	2			normal

- For DPX sensor series, the Branch Circuit Monitor only displays the sensor port where it is physically connected.

For example, if a DPX environmental sensor package is connected to the SENSOR port numbered 1, its Position column shows "Port 1."

Note: For the Branch Circuit Monitor devices with only one SENSOR port, it always shows "Port 1."

- For DPX2 and DX sensor series, the Branch Circuit Monitor displays the sensor package's position in the chain in addition to the sensor port number.

For example, if a 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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.

Peripheral Devices									
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 and Actuators

The Branch Circuit Monitor 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 Branch Circuit Monitor device can manage a maximum of 32 environmental sensors or actuators.

When there are less than 32 managed sensors or actuators, the Branch Circuit Monitor 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](#).

► To manually manage an environmental sensor or actuator:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See **Expanding the Tree** (on page 85).

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Peripheral Devices in the Explorer pane, and the Peripheral Devices page opens in the right 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** (see "Identifying Environmental Sensors" on page 226).*

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 Branch Circuit Monitor 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 Branch Circuit Monitor 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** (see **"Unmanaging Environmental Sensors"** on page 241).*

Configuring Environmental Sensors

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. If the BCM folder is not expanded, expand it to show all components and component groups. See **Expanding the Tree** (on page 85).

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Peripheral Devices in the Explorer pane, and the Peripheral Devices page opens in the right pane.
3. Select the sensor or actuator that you want to configure.
4. Click Setup. 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).

Tip: You can also trigger the same setup dialog by selecting the desired environmental sensor or actuator icon in the navigation tree and then clicking Setup in the right pane.

5. If the selected environmental sensor is a Raritan contact closure sensor connected with a third-party detector/switch, select the appropriate sensor type in the Binary Sensor Subtype field.
 - 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.
6. Type a new name in the Name field.
7. Describe the sensor or actuator's location by assigning alphanumeric values to the X, Y and Z coordinates. See **Describing the Sensor or Actuator's Location** (on page 234).

Note: 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.

8. If the selected environmental sensor is a numeric sensor, its threshold settings are displayed in the dialog. 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 enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 139).
- To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 141).

9. To use the default threshold settings, select the Use Default Thresholds radio button. To modify the default threshold settings, see Threshold Information.

- 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 enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 139).
- To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 141).

Note: The Upper Critical and Lower Critical values are points at which the Branch Circuit Monitor considers the operating environment critical and outside the range of the acceptable threshold.

10. Click OK.
11. Repeat the same steps to configure additional environmental sensors.

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 BCM folder.

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Setup in the Settings section. The BCM 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 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 Branch Circuit Monitor MIB. To configure and retrieve these values over the CLI, see **Using the Command Line Interface** (on page 276).*

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** (see "**Configuring Environmental Sensors**" on page 231).

► To change the default threshold settings:

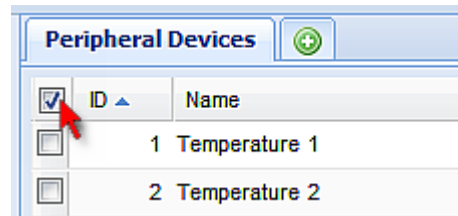
1. Click Peripheral Devices in the Explorer pane, and the Peripheral Devices page opens in the right pane.
2. Click Default Thresholds Setup on the Peripheral Devices page. A dialog appears, showing a list of all numeric environmental sensor types.
3. Select the desired sensor type.
4. Click Edit or 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.
 - To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See "To Assert" and Assertion Timeout.
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 Explorer pane, and the Peripheral Devices page opens in the right 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 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** (see "Configuring Environmental Sensors" on page 231).
5. Click OK.

Viewing Sensor Data and 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 PDU where a specific environmental sensor package is connected. DPX sensor packages show this information.
- **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 Reading** (see "**The Yellow- or Red-Highlighted Sensors**" on page 91).

► To view managed environmental sensors only:

1. Click the Dashboard icon in the PX 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 of managed and unmanaged environmental sensors:

1. If the BCM folder is not expanded, expand it to show all components and component groups. See **Expanding the Tree** (on page 85).

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

- Click Peripheral Devices in the Explorer pane, and the Peripheral Devices page opens in the right 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 Branch Circuit Monitor 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 Branch Circuit Monitor continues to ping unavailable sensors, and moves out of the *unavailable* state after detecting the sensor for two consecutive scans.

Connected sensors always show *unavailable* if they are NOT under management.

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 Environmental Sensors Guide or Online Help for information on setting the normal state or dip switch, which is accessible on the Raritan website's **PX2 Support Files** page (<https://www.raritan.com/support/product/px2/px2-support-files>).*

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 a 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 Environmental Sensors Guide or Online Help for information on setting the normal state or dip switch, which is accessible on the Raritan website's **PX2 Support Files page** (<https://www.raritan.com/support/product/px2/px2-support-files>).*

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 ($=$).

Unmanaging Environmental Sensors

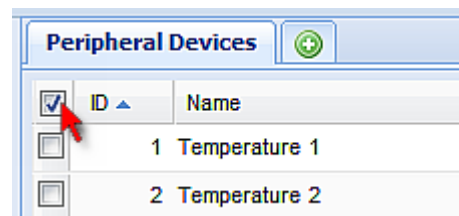
When it is unnecessary to monitor a particular environmental factor, you can unmanage or release the corresponding environmental sensor so that the Branch Circuit Monitor device stops retrieving the sensor's reading and/or state. This procedure also applies if you want to unmanage an actuator.

► **To release a managed sensor or actuator:**

1. If the BCM folder is not expanded, expand it to show all components and component groups. See **Expanding the Tree** (on page 85).

*Note: The BCM folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the Branch Circuit Monitor** (on page 103).*

2. Click Peripheral Devices in the Explorer pane, and the Peripheral Devices page opens in the right pane.
3. Select the checkbox of the desired sensor or actuator on the Peripheral Devices page. To release multiple ones, select multiple checkboxes.
 - To select all those listed on the Peripheral Devices page, simply select the checkbox in the header row.



4. 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.

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 Branch Circuit Monitor automatically brings newly-connected environmental sensors and actuators under management after detecting them.

When this feature is disabled, the Branch Circuit Monitor 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 BCM folder.
2. The folder is named "my BCM" by default. The name can be customized. See **Naming the Branch Circuit Monitor** (on page 103)
3. Click Setup in the Settings section. The Pdu Setup dialog appears.
4. Deselect the Peripheral Device Auto Management checkbox.
5. 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. See **Expanding the Tree** (on page 85).
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 Explorer pane, and the Peripheral Devices page opens in the right 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.

- Click "Switch on" or "Switch off" to turn on or off the selected actuators.

Asset Management

Configure the asset management settings only when an asset sensor is physically connected to the Branch Circuit Monitor device.

*Note: To set up an asset management system, see **Connecting the Asset Management Sensor** (on page 51).*

Configuring the Asset Sensor

The EMX cannot detect how many rack units (tag ports) a connected to asset management sensor supports, so you must provide this information manually.

When you add an asset management sensor, you name it. Additionally, you can provide a description to identify each asset sensor.

The customized name is followed by the label in parentheses.

Note: In this context, the label refers to the port number where the asset sensor is connected. In Branch Circuit Monitor, a Feature port is identified with a combination of the name "Asset Strip" and the port number.

► To configure an asset sensor:

- Connect the asset sensor to the EMX if it is not already.
- Click on the Feature Ports folder in the navigation tree to expand it.
- Click the desired asset sensor. 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.

- Click Setup in the Settings section. The Setup of Asset Strip dialog appears.
- Enter a name of the asset sensor.
- In the "Number of Rack Units" field, type the total number of rack units supported by the AMS. Default is 48.
- 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.
- 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.
9. 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.
 10. 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 Branch Circuit Monitor 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.
11. To change the LED color denoting the absence of a connected 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.

12. Click OK.

Setup of Asset Sensor 4 (4)

Name: Asset Sensor 4

Number of Rack Units: 48

Numbering Mode: Bottom-Up

Numbering Offset: 1

Orientation: Top Connector

Color with connected Tag: ■ FF0000

Color without connected Tag: ■ FF00FF

OK Cancel

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. You can configure or change the color settings for all LEDs on the connected asset sensor(s) by following the procedure below.

This feature is accessible only by users with Administrative Privileges.

► To configure all LED colors:

1. Connect the asset sensor to the Branch Circuit Monitor if it is not already.
2. Click on the Feature Ports folder in the navigation tree to expand it.
3. Click the desired asset sensor. 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. Click Setup on the asset sensor page. The setup dialog for that asset sensor appears.
5. To change the LED color denoting the absence of a connected 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** (see "**Changing a Specific Rack Unit's LED Color Settings**" on page 246).*

Changing a Specific Rack Unit's LED Color Settings

In the Branch Circuit Monitor 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. Click on the Feature Ports folder in the navigation tree to expand it.
3. Click the desired asset sensor. 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 Branch Circuit Monitor 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			

- 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 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:**

- Connect the asset sensor to the Branch Circuit Monitor if it is not already.
- Click on the Feature Ports folder in the navigation tree to expand it.
- Click the desired asset sensor. 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. Click Extended Device Info, where the asset sensor data is displayed.
5. Click Close to quit the dialog.

Webcam Management

With a Logitech® webcam connected to the Branch Circuit Monitor device, you can visually monitor the environment around the Branch Circuit Monitor 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 Branch Circuit Monitor, see **Connecting a Logitech Webcam** (on page 61).

You can manually store snapshots taken from the webcam onto the Branch Circuit Monitor or a remote server. See **Saving Snapshots** (on page 255) or **Configuring Webcam Storage** (on page 257).

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 253).

Events that trigger emails containing snapshots from a webcam can be created. See **Creating Actions** (on page 181).

Configuring Webcams


Before you can configure a webcam, it must be connected to the Branch Circuit Monitor. See **Connecting a Logitech Webcam** (on page 61).

► 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 Branch Circuit Monitor 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.

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 249).
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 Branch Circuit Monitor 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 Branch Circuit Monitor interface, and up to two (2) remote sessions. See **Sending Snapshots or Videos in an Email or Instant Message** (on page 253).*

► 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 Branch Circuit Monitor 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 219).*




2. By default the Branch Circuit Monitor 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 Branch Circuit Monitor web interface.

- To change any image settings, click Setup . See **Configuring Webcams** (on page 249) or **Adjusting Image Properties** (on page 250).
 - To save the snapshot being displayed, click the "Store Snapshot to Webcam Storage" icon . See **Saving Snapshots** (on page 255).
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.

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 Branch Circuit Monitor. 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 219).*

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 Branch Circuit Monitor 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 158).

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.

Snapshot Storage

Once a snapshot is taken using the Store Snapshot to Webcam Storage feature, it is stored locally on the Branch Circuit Monitor by default. Up to ten (10) images can be stored on the Branch Circuit Monitor 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 Branch Circuit Monitor deletes all webcam snapshots that are saved on the device.

Saving Snapshots

If it is intended to keep the snapshot being displayed on the webcam, you can manually save it onto the Branch Circuit Monitor. A snapshot is saved as a JPEG file and stored on the Snapshots page.

Warning: The snapshots stored on the Branch Circuit Monitor are cleared when rebooting the Branch Circuit Monitor. 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 Branch Circuit Monitor, see **Configuring Webcam Storage** (on page 257).*

Managing the Snapshots Saved to Branch Circuit Monitor

A maximum of 10 saved snapshots can be stored and displayed on the Snapshots page of the Branch Circuit Monitor.

See **Saving Snapshots** (on page 255) for instructions on storing snapshots on the Branch Circuit Monitor.

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 257).*

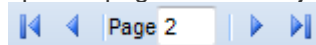
► To view the saved snapshots:


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 249).

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.

► **To change the sorting or displayed columns of the list:**

- You can resort the snapshot list or hide any displayed column in the Storage section. For details, see **Changing the View of a List** (on page 92).

Configuring Webcam Storage

Once a snapshot is taken using the Store Snapshot to Webcam Storage feature, it is stored locally on the Branch Circuit Monitor by default. Up to ten (10) images can be stored on the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor, 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.

Firmware Upgrade

You may upgrade your Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor shows three digits: 'FuP' or 'FUP.'
 - No users can successfully log in to the Branch Circuit Monitor.
 - 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 265) in the online help.*

Viewing Firmware Update History

The firmware upgrade history, if available, is permanently stored on the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor firmware file is required in the recovery procedure.



Viewing the Communication Log

The Branch Circuit Monitor allows you to inspect all communications that occurred between the Branch Circuit Monitor device and its graphical user interface (GUI). The information is usually useful for a technical support engineer only and you may not need to view it.


This feature is accessible only by users with Administrative Privileges.

► **To view the communication log:**

1. Choose Maintenance > View Communication Log. The Communication Log dialog appears.
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.

3. To save the communication log on your computer, click .
4. To clear all records in the communication log, click Clear Communication Log. Click Yes on the confirmation message.

Network Diagnostics

The Branch Circuit Monitor 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 403).*

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 Branch Circuit Monitor 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.

Backup and Restore of Branch Circuit Monitor Device Settings

Different from the Bulk Configuration file, the backup file contains device-specific data like network settings. To back up or restore Branch Circuit Monitor device settings, you should perform the Backup/Restore feature.

All Branch Circuit Monitor information is captured in the XML backup file except for the device logs and TLS certificate.

*Note: To perform the bulk configuration among multiple Branch Circuit Monitor devices, perform the Bulk Configuration feature instead. See **Bulk Configuration** (on page 32).*

► **To download a backup Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor device resets and the Login page re-appears, indicating that the restore is complete.

Note: On startup, the Branch Circuit Monitor 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.

Tip: You can also back up and restore a configuration file using a Secure Copy (SCP) command. See Backup and Restore via SCP.

Accessing the Help

The Help menu provides:

- Current firmware and software packages information
- A link to the Branch Circuit Monitor Online Help

Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 6

Using SNMP

This SNMP section helps you set up the Branch Circuit Monitor for use with an SNMP manager. The Branch Circuit Monitor 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	266
Configuring Users for Encrypted SNMP v3	267
Configuring SNMP Notifications	268
SNMP Gets and Sets	273

Enabling SNMP

By default, SNMP v1/v2c is enabled on the Branch Circuit Monitor so the Branch Circuit Monitor 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.

The image shows the 'SNMP Settings' dialog box with the 'General' tab selected. It contains three main sections: 'SNMP v1 / v2c Settings', 'SNMP v3 Settings', and 'MIB-II System Group'. In the first section, 'SNMP v1 / v2c' is checked, 'Read Community String' is 'public', and 'Write Community String' is empty. In the second section, 'SNMP v3' is unchecked. The third section has empty fields for 'sysContact:', 'sysName:', and 'sysLocation:'. At the bottom, there is a 'Download MIB' button and 'OK' and 'Cancel' buttons.

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 Branch Circuit Monitor via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** (on page 267).*

4. Enter the MIB-II system group information, if applicable:
 - a. sysContact - the contact person in charge of the system being contacted
 - 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 Branch Circuit Monitor is used by the SNMP manager.

*Important: You must download the SNMP MIB for your Branch Circuit Monitor 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 273).*

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 Branch Circuit Monitor.

► 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 142).
5. Click OK. The user is now set up for encrypted SNMP v3 communication.

Configuring SNMP Notifications

The Branch Circuit Monitor automatically keeps an internal log of events that occur. See **Event Rules and Actions** (on page 180). These events can also be used to send SNMP v2c or v3 notifications to a third-party destination.

The Branch Circuit Monitor 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 (5) resends in three (3) 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 Branch Circuit Monitor release. This ensures your SNMP manager has the correct MIB for the release you are using. See **Downloading SNMP MIB** (on page 273).*

SNMPv2c Notifications

► To configure the Branch Circuit Monitor 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 main sections: 'SNMP v1 / v2c Settings', 'SNMP v3 Settings', and 'MIB-II System Group'. In the 'SNMP v1 / v2c Settings' section, the 'enable' checkbox is checked, the 'Read Community String' is 'public', and the 'Write Community String' is empty. In the 'SNMP v3 Settings' section, the 'enable' checkbox is unchecked. In the 'MIB-II System Group' section, the 'sysContact', 'sysName', and 'sysLocation' fields are empty. At the bottom, there is a 'Download MIB' button with a dropdown arrow, and 'OK' and 'Cancel' buttons.

2. Enter the MIB-II system group information, if applicable:
 - a. sysContact - the contact person in charge of the system being contacted
 - b. sysName - the name assigned to the system
 - c. sysLocation - the location of the system
3. Select the MIB to be downloaded. The SNMP MIB for your Branch Circuit Monitor is used by the SNMP manager.

*Important: You must download the SNMP MIB for your Branch Circuit Monitor 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 273).*

4. Click OK.
5. On the Notifications tab, select the Enable checkbox to enable the SNMP notification feature.
6. From the Notification Type drop-down, select the type of SNMP notification.

7. 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.
8. 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.
9. In the Port fields, enter the port number used to access the device(s).
10. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the Branch Circuit Monitor and all SNMP management stations.
11. Click OK.

SNMPv3 Notifications

► To configure the Branch Circuit Monitor 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 main sections: 'SNMP v1 / v2c Settings', 'SNMP v3 Settings', and 'MIB-II System Group'. In the 'SNMP v1 / v2c Settings' section, 'SNMP v1 / v2c:' is checked (enable), 'Read Community String:' is 'public', and 'Write Community String:' is empty. In the 'SNMP v3 Settings' section, 'SNMP v3:' is unchecked. In the 'MIB-II System Group' section, 'sysContact:', 'sysName:', and 'sysLocation:' are all empty text boxes. At the bottom, there is a 'Download MIB' button with a dropdown arrow, and 'OK' and 'Cancel' buttons.

2. Enter the MIB-II system group information, if applicable:
 - a. sysContact - the contact person in charge of the system being contacted
 - b. sysName - the name assigned to the system
 - c. sysLocation - the location of the system
3. Select the MIB to be downloaded. The SNMP MIB for your Branch Circuit Monitor is used by the SNMP manager.

*Important: You must download the SNMP MIB for your Branch Circuit Monitor 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 273).*

4. Click OK.
5. On the Notifications tab, select the Enable checkbox to enable the SNMP notification feature.
6. From the Notification Type drop-down, select the type of SNMP notification.
7. For SNMP TRAPs, the engine ID is prepopulated.

8. 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.
9. 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 traps, the Branch Circuit Monitor is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the Branch Circuit Monitor, 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 Branch Circuit Monitor device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The Branch Circuit Monitor 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 Branch Circuit Monitor MIB.

The Branch Circuit Monitor MIB

The SNMP MIB file is required for using your Branch Circuit Monitor device with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Downloading SNMP MIB

The SNMP MIB file for the Branch Circuit Monitor can be easily downloaded from the web interface. There are two ways to download the SNMP MIB file.

Note: You can ignore the Asset Management- or Asset Strip-related feature because the Branch Circuit Monitor does not support the asset management function.

► 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 Branch Circuit Monitor power 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. The Device Information dialog appears.
2. Click the "download" link in the PDU-MIB field to download the desired SNMP MIB file.
 - PDU2-MIB: The SNMP MIB file for Branch Circuit Monitor power management.

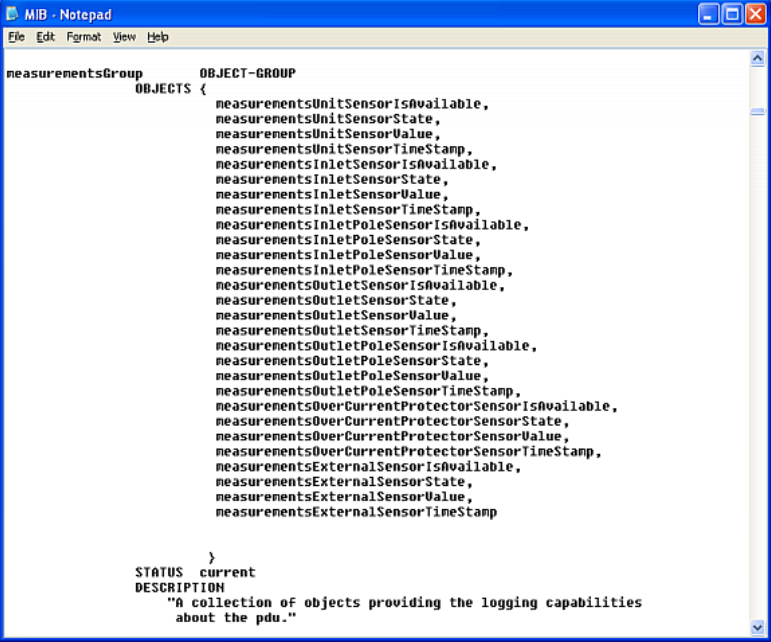
The "USB Console INF file" link lets you download the USB-to-serial driver that may be required only when the Branch Circuit Monitor is connected to a computer via an USB cable for configuration. See ***Installing the USB-to-Serial Driver (Optional)*** (on page 24) for details.

3. Click Save to save the file onto your computer.

Layout

Opening the MIB reveals the custom objects that describe the Branch Circuit Monitor 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.



```
measurementsGroup      OBJECT-GROUP
                        OBJECTS {
                            measurementsUnitSensorIsAvailable,
                            measurementsUnitSensorState,
                            measurementsUnitSensorValue,
                            measurementsUnitSensorTimeStamp,
                            measurementsInletSensorIsAvailable,
                            measurementsInletSensorState,
                            measurementsInletSensorValue,
                            measurementsInletSensorTimeStamp,
                            measurementsInletPoleSensorIsAvailable,
                            measurementsInletPoleSensorState,
                            measurementsInletPoleSensorValue,
                            measurementsInletPoleSensorTimeStamp,
                            measurementsOutletSensorIsAvailable,
                            measurementsOutletSensorState,
                            measurementsOutletSensorValue,
                            measurementsOutletSensorTimeStamp,
                            measurementsOutletPoleSensorIsAvailable,
                            measurementsOutletPoleSensorState,
                            measurementsOutletPoleSensorValue,
                            measurementsOutletPoleSensorTimeStamp,
                            measurementsOverCurrentProtectorSensorIsAvailable,
                            measurementsOverCurrentProtectorSensorState,
                            measurementsOverCurrentProtectorSensorValue,
                            measurementsOverCurrentProtectorSensorTimeStamp,
                            measurementsExternalSensorIsAvailable,
                            measurementsExternalSensorState,
                            measurementsExternalSensorValue,
                            measurementsExternalSensorTimeStamp
                        }
STATUS current
DESCRIPTION
    "A collection of objects providing the logging capabilities
    about the pdu."
```

For example, the measurementsGroup group contains objects for sensor readings of Branch Circuit Monitor as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor value". pduRatedCurrent, part of the configGroup group, describes the device's current rating.

Note that the MIB file uses the following terms to refer to the device or its components:

- pdu, px or unit: The Branch Circuit Monitor device
- inlet: Mains channels
- outlet: Branch circuit channels

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 Branch Circuit Monitor to generate a warning and send an SNMP notification when certain parameters are exceeded. See **Setting Power Thresholds** (on page 136) 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 7 Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer a Branch Circuit Monitor device.

In This Chapter

About the Interface	277
Logging in to CLI	277
Help Command.....	281
Querying Available Parameters for a Command.....	282
Showing Information.....	282
Clearing Information	308
Configuring the Branch Circuit Monitor Device and Network	308
Configuring Environmental Sensors' Default Thresholds	381
Environmental Sensor Configuration Commands	383
Environmental Sensor Threshold Configuration Commands	388
Actuator Configuration Commands	391
USB-Cascading Configuration Commands	392
Asset Management Commands	393
Actuator Control Operations	399
Unblocking a User	401
Resetting the Branch Circuit Monitor.....	401
Network Troubleshooting.....	403
Retrieving Previous Commands.....	406
Automatically Completing a Command	406
Logging out of CLI	407

About the Interface

The Branch Circuit Monitor 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 Branch Circuit Monitor device
- Display the Branch Circuit Monitor and network information, such as the device name, firmware version, IP address, and so on
- Configure the Branch Circuit Monitor 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 111).*

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.

► To log in using HyperTerminal:

1. Connect your computer to the Branch Circuit Monitor 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 Branch Circuit Monitor. 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 280) in the online help 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 Branch Circuit Monitor.

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 111) in the online help.
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 280) in the online help 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 Branch Circuit Monitor.

With an Analog Modem

The Branch Circuit Monitor 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 Branch Circuit Monitor via the modem:

1. Make sure the Branch Circuit Monitor has an analog modem connected. See **Connecting an Analog Modem** (on page 62).
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 Branch Circuit Monitor. See **Configuring the Serial Port** (on page 123).
4. Type the following AT command to make a connection with the Branch Circuit Monitor.

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 Branch Circuit Monitor:

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 Branch Circuit Monitor.

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 Branch Circuit Monitor device, the **>** prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the Branch Circuit Monitor 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 Branch Circuit Monitor device and network configurations. See **Entering Configuration Mode** (on page 309).
- 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 403).

Closing a Local Connection

Close the window or terminal emulation program when you finish accessing a Branch Circuit Monitor device over the local connection.

When accessing or upgrading multiple Branch Circuit Monitor 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 282).*

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 Branch Circuit Monitor 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 280).*

Device Configuration

This command shows the Branch Circuit Monitor's configuration, such as the device name, firmware version and model type.

```
# show bcm
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show bcm details
```

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. <i>Tip: You can also type the command without adding this option "all" to get the same data.</i>
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 Branch Circuit Monitor is a slave device connected to the LAN via the master Branch Circuit Monitor device, the `show network mode` command displays `wired(USB)` instead of `wired`.

Wireless Configuration

This command only shows the wireless configuration of the Branch Circuit Monitor 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.
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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor. See **Existing User Profiles** (on page 299) for the preferred measurement units for a specific user.*

Branch Circuit Information

This command syntax shows the branch circuit information.

```
#          show branches <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#          show branches <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all branch circuits.
	<i>Tip: You can also type the command without adding this option "all" to get the same data.</i>

Option	Description
A specific branch circuit number	<p>Displays the information for the specified branch circuit only.</p> <ul style="list-style-type: none"> <n> is the index number of the selected branch circuit channel. <p>This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the chassis of the Branch Circuit Monitor.</p> <p>See Identifying Branch Circuit Channel Numbers (on page 73).</p>

Displayed information:

- Without the parameter "details," only the branch circuit name is displayed.
- With the parameter "details," more branch circuit information is displayed in addition to the name, such as the RMS current, voltage and active energy.

Important: Measurements of the branch circuit CTs may be incorrect if you have not properly configured your branch circuit CTs using the web interface. See *Configuring the Branch Circuit Channels* (on page 130).

Mains Information

This command syntax shows the mains information.

```
#          show mains
```

To show detailed information, add the parameter "details" to the end of the command.

```
#          show mains details
```

Displayed information:

- Without the parameter "details," only the mains' name and current values are displayed.
- With the parameter "details," more mains information is displayed in addition to the current values, such as the voltage, active power and active energy.

Important: Measurements of the mains CTs may be incorrect if you have not properly configured your mains CTs using the web interface. See

*Configuring the Mains Channels (on page 129).***Branch Circuit Threshold Information**

This command syntax shows the specified branch circuit sensor's threshold-related information.

```
#          show sensor branch <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#          show sensor branch <n> <sensor type> details
```

Variables:

- <n> is the index number of the selected branch circuit channel.
This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the chassis of the Branch Circuit Monitor. See **Identifying Branch Circuit Channel Numbers** (on page 73).
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the sensor reading, state, threshold, deassertion hysteresis and assertion delay settings of the specified branch circuit sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

Branch Circuit Pole Threshold Information

This command is applicable to a three-phase branch circuit only. See **Configuring the Branch Circuit Channels** (on page 130) for how to configure a 3-phase branch circuit.

This command syntax shows the specified branch circuit pole sensor's threshold-related information.

```
#          show sensor branchpole <n> <p> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#          show sensor branchpole <n> <p> <sensor type> details
```

Variables:

- <n> is the index number of the selected branch circuit channel.
This index number is available on the Branch Circuits page of the web interface and likely to be different from the channel number labeled on the chassis of the Branch Circuit Monitor. See **Identifying Branch Circuit Channel Numbers** (on page 73).
- <p> is the label of the branch circuit pole whose sensors you want to query.

Pole	Label <p>	Current sensor	Voltage sensor
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Displayed information:

- Without the parameter "details," only the sensor reading, state, threshold, deassertion hysteresis and assertion delay settings of the specified branch circuit pole sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

Mains Threshold Information

This command syntax shows the specified mains sensor's threshold-related information.

```
#          show sensor mains <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#          show sensor mains <sensor type> details
```

Variables:

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion delay settings of the specified mains sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

Mains Pole Threshold Information

This command syntax shows the specified mains pole sensor's threshold-related information.

```
# show sensor mainspole <p> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show sensor mainspole <p> <sensor type> details
```

Variables:

- <p> is the label of the mains pole whose sensors you want to query.

Pole	Label <p>	Current sensor	Voltage sensor
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified mains pole sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor.

```
#          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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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.
sensor	Internal or external sensor events, such as state changes of any sensors.

Event type	Description
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.

Note: You can ignore the powerLogic event type in the CLI because the Branch Circuit Monitor does not support it.

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 Branch Circuit Monitor.

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 280).*

Clearing Information

You can use the clear commands to remove unnecessary data from the Branch Circuit Monitor.

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 280).*

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 Branch Circuit Monitor Device and Network

To configure the Branch Circuit Monitor 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 280).*

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 309).

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 280).

Device Configuration Commands

A device configuration command begins with *emd*. You can use the device configuration commands to change the settings that apply to the whole Branch Circuit Monitor device.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Changing the Device Name

This command changes the Branch Circuit Monitor device's name.

```
config:#    emd name "<name>"
```

Variables:

- *<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 Z Coordinate Format for Environmental Sensors

This command enables or disables the use of rack units for specifying the height (Z coordinate) of environmental sensors.

```
config:#    emd externalSensorsZCoordinateFormat <option>
```

Variables:

- *<option>* is one of the options: *rackUnits* or *freeForm*.

Option	Description
rackUnits	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.
freeForm	Any alphanumeric string can be used for specifying the Z coordinate.

Note: After determining the format for the Z coordinate, you can set a value for it. See **Setting the Z Coordinate** (on page 386).

Enabling or Disabling Data Logging

This command enables or disables the data logging feature.

```
config:#    emd dataRetrieval <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the data logging feature.
disable	Disables the data logging feature.

For more information, see **Setting Data Logging** (on page 125).

Setting the Data Logging Measurements Per Entry

This command defines the number of measurements accumulated per log entry.

```
config:#    emd measurementsPerLogEntry <number>
```

Variables:

- <number> is an integer between 1 and 600. The default is 60 samples per log entry.

For more information, see **Setting Data Logging** (on page 125).

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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor device.

An IP protocol configuration command begins with *network ip*.

Enabling IPv4 or IPv6

This command determines which IP protocol is enabled on the Branch Circuit Monitor.

```
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 Branch Circuit Monitor.

```
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 Branch Circuit Monitor 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 318).

► **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 Branch Circuit Monitor only supports Protected Extensible Authentication Protocol (PEAP) as the outer authentication.
- The value of <inner_auth> is *MSCHAPv2* because Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 309).

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
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwYydgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkw/YDTL2ftgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMEFQxCzAJBgNVBAYTAiVTMTYwNAYDVQK
Ey1OYXRpb25hbCBZBZJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVROBAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVROKBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+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."

```

MIICjTCCAfIgAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTElMAk
GA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxM
zQ5MDUrMDgwMBcROTwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEwxdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwr
gJBALrAwYdgmzNP/ts0Uyf6BpmiJYktU/w4NG67ULa4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlyDTL2ftGvfw0CAQOjgaswgag
wZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTA1VTMTYwNAYDVQ
QKEy1OYXRpb25hbCBZBZJvbmF1dG1jcyBhbmQgU3BhY2UgQWRta
W5pc3RyYXRpb24xDALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0w
C4AJODMyOTcwODEwMBGGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLGgiTkCKp0F5EWIrVDwh54NNevkCQRZ
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 Branch Circuit Monitor device.

```
config:#    network ipv4 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your Branch Circuit Monitor 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 322).

```
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 322).

```
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 Branch Circuit Monitor supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor device.

```
config:#    network ipv6 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your Branch Circuit Monitor 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 326).

```
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 326).

```
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 Branch Circuit Monitor supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the Branch Circuit Monitor 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 Branch Circuit Monitor 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.

Option	Description
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 369).

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 117) 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.

Mode	Description
false	Customized NTP server settings do NOT override the DHCP-specified NTP servers.

Setting the Time Zone

In addition to the web interface, the CLI also provides a list of time zones for you to configure the date and time for your Branch Circuit Monitor device.

```
config:#    time zone
```

After a list of time zones is displayed, you can either type the index number of the desired time zone or simply press Enter to cancel this setting.

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 Branch Circuit Monitor and then shows the result. For instructions on specifying NTP servers via CLI, see **Setting NTP Parameters** (on page 337).

To perform this command successfully, you must:

- Own the "Change Date/Time Settings" permission.
- Customize NTP servers. See **Setting NTP Parameters** (on page 337).
- Make the customized NTP servers override the DHCP-assigned ones. See **Overriding DHCP-Assigned NTP Servers** (on page 337).

This command is available either in the administrator/user mode or in the configuration mode. See **Different CLI Modes and Prompts** (on page 280).

▶ **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 Branch Circuit Monitor 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.

Option	Description
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 377).*

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.
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 Branch Circuit Monitor. Do either of the following, or you cannot successfully log in to the Branch Circuit Monitor:

- 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 309).*

Example

```

Welcome to Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 377).

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 Branch Circuit Monitor 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 377).

► **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 377).

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 minLength <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 maxLength <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.
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 377).*

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 Branch Circuit Monitor 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 377).*

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, Branch Circuit Monitor 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 377).

► 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 Branch Circuit Monitor 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 377).

► **Enable or disable the SNMP v3 access to Branch Circuit Monitor 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.

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 377).

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 Branch Circuit Monitor user interfaces for all users via CLI, see **Setting Up User Preferences (Units of Measure)** (see "Setting Default Measurement Units" on page 370, on page 369).*

► 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.

Setting Up User Preferences (Units of Measure)

Change user preferences:

```
config:# user modify admin preferredTemperatureUnit C or
F
```

```
config:# user modify admin preferredLengthUnit meter or
feet
```

```
config:# user modify admin preferredPressureUnit pascal
or psi
```

Change default preferences:

```
config:# user defaultPreferences preferredPressureUnit
pascal or 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 377).

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 Branch Circuit Monitor user interfaces for a specific user via CLI, see **Changing Measurement Units** (on page 367).

► **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.
- <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

Privilege	Description
acknowledgeAlarms	Acknowledge Alarms
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration
changeAuthSettings	Change Authentication Settings
changeEmdConfiguration	Change EMD Configuration
changeExternalSensorsConfiguration	Change Peripheral Device Configuration
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
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)

Privilege	Description
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 Images and Configuration

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.
- <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.
- <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>
```

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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 external* 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.

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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 377).

► **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 Branch Circuit Monitor 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 Branch Circuit Monitor 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
```

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 377).

- **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	%

Sensor types	Measurement units
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 391).

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 Branch Circuit Monitor 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 391).*

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 Branch Circuit Monitor 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.

Type	Description
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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 for Environmental Sensors** (on page 310).*

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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 377).

► 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 Branch Circuit Monitor 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.

<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.

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 377).

► **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 Branch Circuit Monitor 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 for Environmental Sensors** (on page 310).*

- <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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor device. Usually you do not need to perform this command unless your asset sensors do NOT come with the tilt sensor, causing the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor 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 395) and Setting LED Colors for Disconnected Tags (on page 396). 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 398) and Setting an LED Mode for a Rack Unit (on page 398) 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 Branch Circuit Monitor 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 395) and **Setting LED Colors for Disconnected Tags** (on page 396).*

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 Branch Circuit Monitor 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 280).

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 Branch Circuit Monitor 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 Branch Circuit Monitor 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
```

Unblocking a User

If any user is blocked from accessing the Branch Circuit Monitor, 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 277).
2. When the Username prompt appears, type `unlock` and press Enter.

Username: `unlock`

3. When the "Username to unlock" prompt appears, type the name of the blocked user and press Enter.

Username to unlock:

4. A message appears, indicating that the specified user was unblocked successfully.

Resetting the Branch Circuit Monitor

You can reset the Branch Circuit Monitor device to factory defaults or simply restart it using the CLI commands.

Restarting the Device

This command restarts the Branch Circuit Monitor device. It is not a factory default reset.

► **To restart the Branch Circuit Monitor device:**

1. Ensure you have entered administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the Branch Circuit Monitor 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 Branch Circuit Monitor device to factory defaults.

► **To reset Branch Circuit Monitor settings after login, use either command:**

```
#      reset factorydefaults  
  
-- OR --  
  
#      reset factorydefaults /y
```

► **To reset Branch Circuit Monitor settings before login:**

```
Username:  factorydefaults
```

See **Using the CLI Command** (on page 444) for details.

Network Troubleshooting

The Branch Circuit Monitor 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 280).

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.
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 Branch Circuit Monitor 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 Specifications

In This Chapter

Branch Circuit Monitor Specifications.....	408
Raritan CT Specifications	408
Power Measurement Accuracy	412
Maximum Ambient Operating Temperature	413
RADIUS Configuration Illustration	414
Serial RS-232 Port Pinouts.....	440
Sensor RJ-12 Port Pinouts	440
Feature RJ-45 Port Pinouts	440

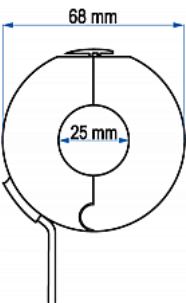
Branch Circuit Monitor Specifications

Model	Maximum circuits (lines)	Input power	Frequency	Update rate
BCM-2400	24 circuits, including 21 branch circuits rated up to 30A and 1 three-phase mains rated up to 250A (or higher, depending on the mains CT used)	Three-phase Wye-connected, 190-415VAC, 20A (North America) or 16A (Europe)	50/60 Hz	1 second

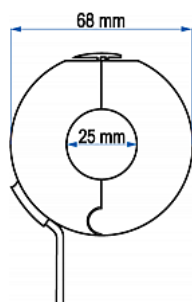
Raritan CT Specifications

Raritan provides different mains and branch circuit CTs that are rated differently.

Mains CT Rated at 200A



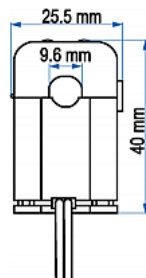
CT electric specifications	
Rated primary current (RMS) 50/60Hz	1-200A
Maximum current (continuous)	360A
Turns ratio	Np:Ns=1:3000
Secondary output at rated current	333mV (resistor inside the CT)
D.C. resistance maximum at 20 degrees Celsius	120 ohm
Accuracy	1%
Phase error at rated current range	<= 1 degree
Operating temperature	-40 to 85 degrees Celsius
Storage temperature	-45 to 90 degrees Celsius
Dielectric withstanding voltage (Hi-pot)	2500V/1mA/1min
Impulse withstand voltage	5KV peak
Insulation resistance	DC500V/100M ohm min

Mains CT Rated at 250A


CT electric specifications	
Rated primary current (RMS) 50/60Hz	5-250A
Maximum current (continuous)	360A
Turns ratio	Np:Ns=1:3750

CT electric specifications	
Secondary output at rated current	333mV (resistor inside the CT)
D.C. resistance maximum at 20 degrees Celsius	95 ohm
Accuracy	0.5%
Phase error at rated current range	≤ 1.5 degrees
Operating temperature	-40 to 85 degrees Celsius
Storage temperature	-45 to 90 degrees Celsius
Dielectric withstanding voltage (Hi-pot)	2500V/1mA/1min
Impulse withstand voltage	5KV peak
Insulation resistance	DC500V/100M ohm min

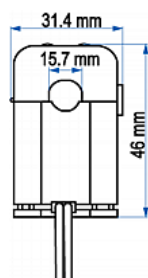
Branch Circuit CTs Rated at 60A



CT electric specifications	
Rated primary current 50/60Hz	1-60A
Maximum current (continuous)	120A
Turns ratio	$N_p:N_s=1:2000$
Current ratio	30A/15mA
D.C. resistance maximum at 20 degrees Celsius	250 ohm
Accuracy @RL ≤ 10 ohm	2%
Operating temperature	-40 to 65 degrees Celsius

CT electric specifications

Storage temperature	-45 to 85 degrees Celsius
Dielectric withstanding voltage (Hi-pot)	2500V/1mA/1min
Impulse withstand voltage	5KV peak
Insulation resistance	DC500V/100M ohm min

Branch Circuit CTs Rated at 60A**CT electric specifications**

Rated primary current 50/60Hz	0.6-100A
Maximum current (continuous)	200A
Turns ratio	$N_p:N_s=1:4000$
Current ratio	100A/25mA
D.C. resistance maximum at 20 degrees Celsius	540 ohm
Accuracy @RL <= 10 ohm	1%
Operating temperature	-40 to 65 degrees Celsius
Storage temperature	-45 to 85 degrees Celsius
Dielectric withstanding voltage (Hi-pot)	2500V/1mA/1min
Insulation resistance	DC500V/100M ohm min

Power Measurement Accuracy

The measurement accuracy of the Branch Circuit Monitor varies based on the Raritan CTs you are using.

Mains Accuracy

The following accuracy data applies only to Raritan's mains CTs and therefore the mains channels on the Branch Circuit Monitor when using Raritan's mains CTs.

Item	Mains CT's measurement accuracy	Mains circuits' measurement accuracy
RMS voltage (V)		2%
RMS current (A)	CTs rated at 200A - 1% CTs rated at 250A - 0.5%	CTs rated at 200A - 2% CTs rated at 250A - 1.5%
Active power (W)		CTs rated at 200A - 2% CTs rated at 250A - 1.5%
Apparent power (VA)		CTs rated at 200A - 2% CTs rated at 250A - 1.5%
Active energy (Wh)		CTs rated at 200A - 2% CTs rated at 250A - 1.5%

Branch Circuit Accuracy

The following accuracy data applies only to Raritan's branch circuit CTs and therefore the branch circuit channels on the Branch Circuit Monitor.

Item	Branch circuit CT's measurement accuracy	Branch circuits' measurement accuracy
RMS voltage (V)		2%
RMS current (A)	CTs rated at 60A - 2% CTs rated at 100A - 1%	CTs rated at 60A - 3% CTs rated at 100A - 2%
Active power (Watts)		CTs rated at 60A - 3% CTs rated at 100A - 2%
Apparent power (VA)		CTs rated at 60A - 3% CTs rated at 100A - 2%
Active energy (Watts-hour)		CTs rated at 60A - 3% CTs rated at 100A - 2%

Maximum Ambient Operating Temperature

The maximum ambient operating temperature (TMA) for all Branch Circuit Monitor models are the same.

Note: At the time of writing, there are only two Branch Circuit Monitor models available -- BCM-2400 and BCM-2401.

Specification	Measure
Max Ambient Temperature	60 degrees Celsius

Appendix B

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 Branch Circuit Monitor device. See **Adding RADIUS Server Settings** (on page 176).
- 2. Configure roles on the Branch Circuit Monitor device. See **Creating a Role** (on page 147).
- 3. Configure your RADIUS server. See **Microsoft Network Policy Server** (on page 414) or **Non-Windows RADIUS Server** (on page 438).

In This Chapter

Microsoft Network Policy Server	414
Non-Windows RADIUS Server	438

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 Branch Circuit Monitor 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 435).

Step A: Add Your Branch Circuit Monitor as a RADIUS Client

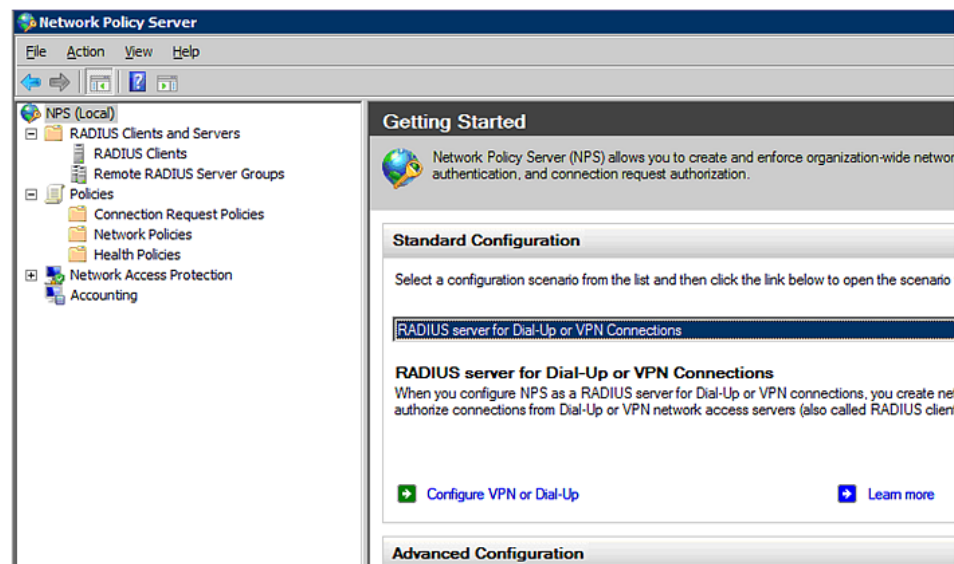
The RADIUS implementation on a Branch Circuit Monitor follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

In this illustration, we assume:

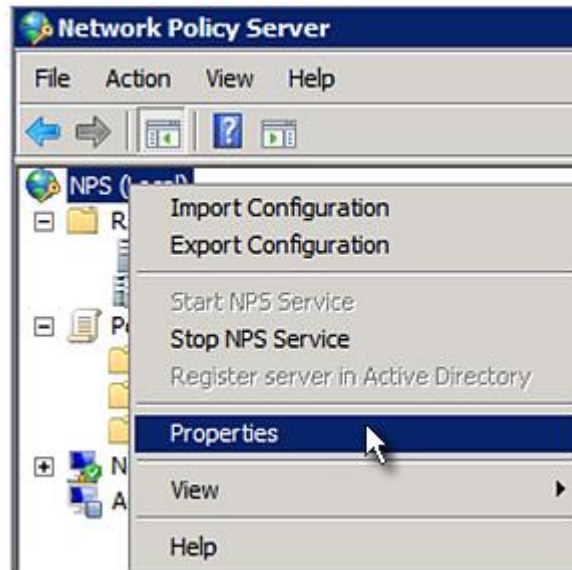
- IP address of your Branch Circuit Monitor: 192.168.56.29
- RADIUS authentication port specified for Branch Circuit Monitor: 1812
- RADIUS accounting port specified for Branch Circuit Monitor: 1813

► **To add your Branch Circuit Monitor to the RADIUS NPS:**

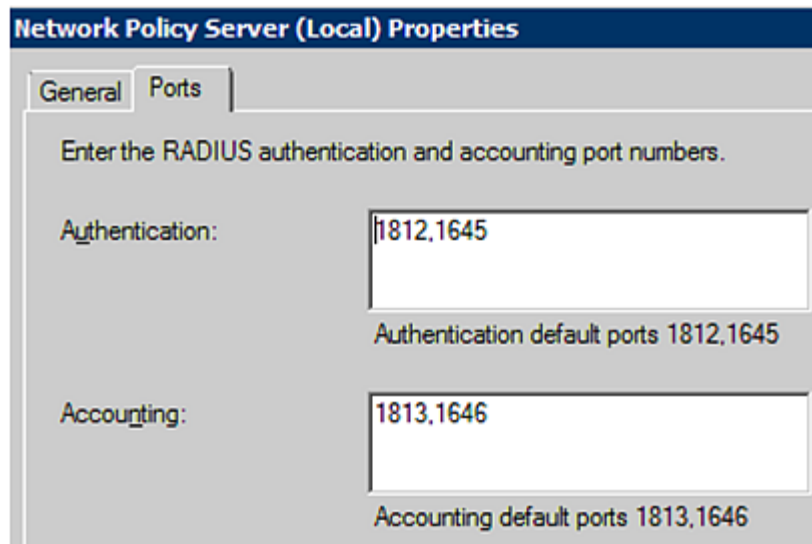
1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.



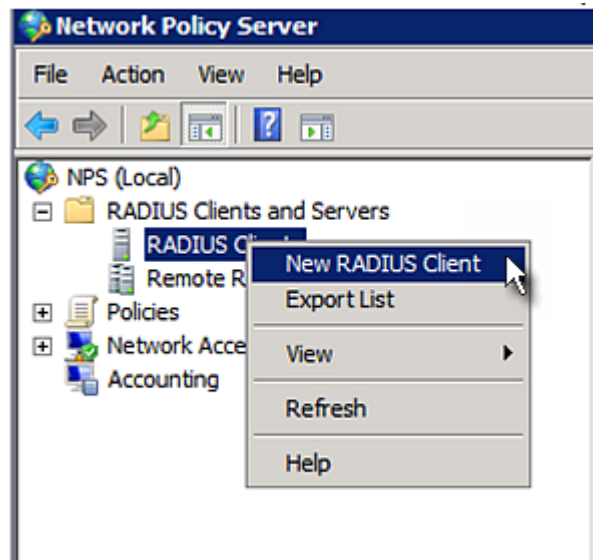
2. Right-click NPS (Local), and select Properties.



Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your Branch Circuit Monitor. 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 Branch Circuit Monitor to NPS:
 - a. Verify the "Enable this RADIUS client" checkbox is selected.
 - b. Type a name for identifying your Branch Circuit Monitor 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 Branch Circuit Monitor.

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 Branch Circuit Monitor

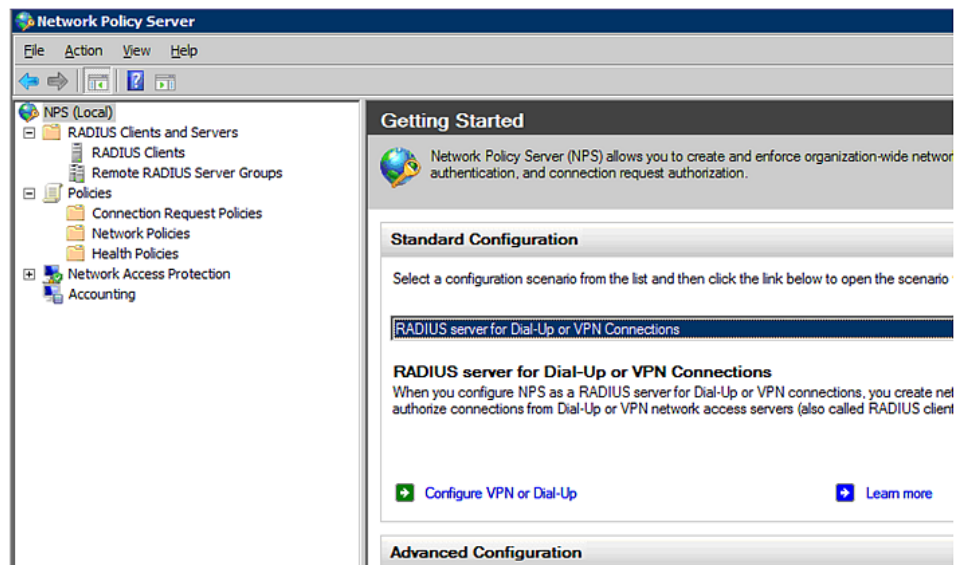
- b. Connection request forwarding method
- c. Authentication method(s)
- d. Standard RADIUS attributes

In the following illustration, we assume:

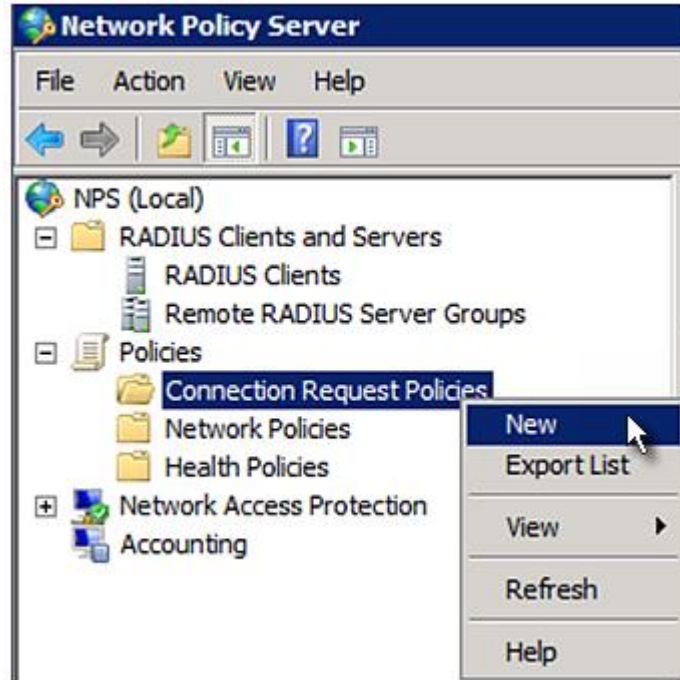
- *Local* NPS server is used
- IP address of your Branch Circuit Monitor: *192.168.56.29*
- RADIUS protocol selected on your Branch Circuit Monitor: *CHAP*
- Existing role of your Branch Circuit Monitor: *Admin*

► **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.

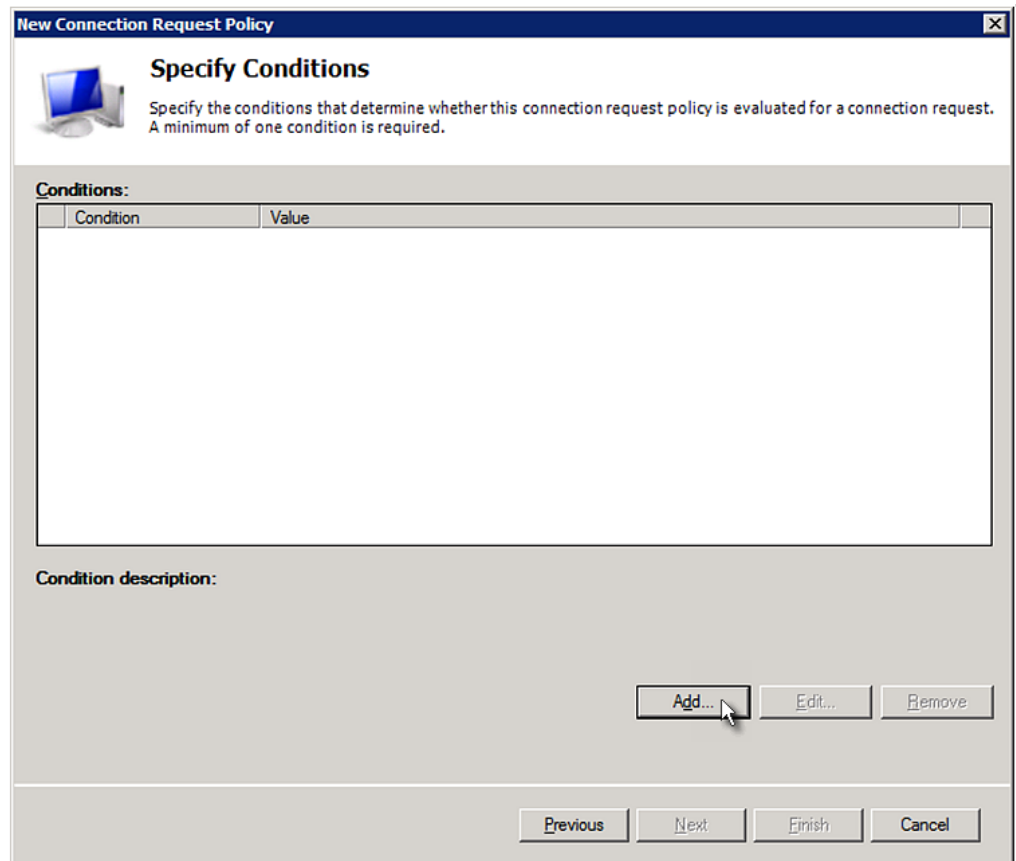
Policy name:

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:**

☐ **Vendor specific:**

4. Click Next to show the "Specify Conditions" screen. Click Add.



New Connection Request Policy

Specify Conditions

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

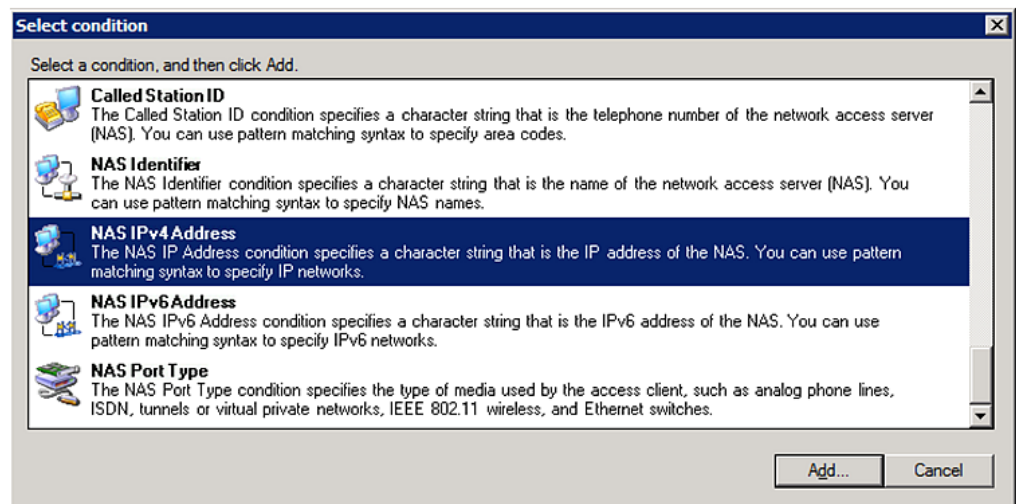
Condition	Value
-----------	-------

Condition description:

Buttons: Add..., Edit..., Remove

Buttons: Previous, Next, Finish, Cancel

5. The "Select condition" dialog appears. Click Add.



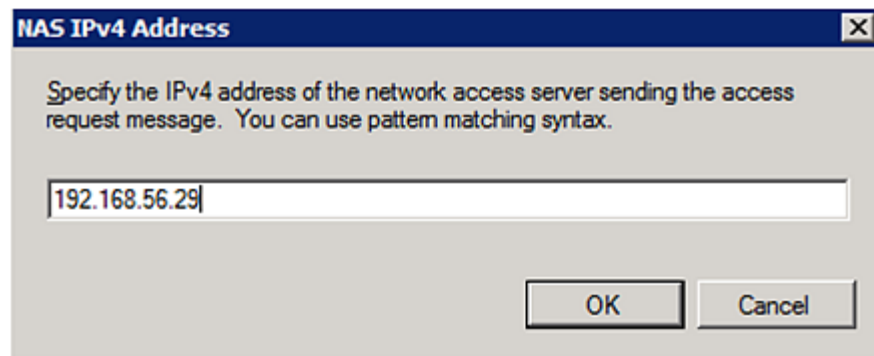
Select condition

Select a condition, and then click Add.

- Called Station ID**
The Called Station ID condition specifies a character string that is the telephone number of the network access server (NAS). You can use pattern matching syntax to specify area codes.
- NAS Identifier**
The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.
- NAS IPv4 Address**
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.
- NAS IPv6 Address**
The NAS IPv6 Address condition specifies a character string that is the IPv6 address of the NAS. You can use pattern matching syntax to specify IPv6 networks.
- NAS Port Type**
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

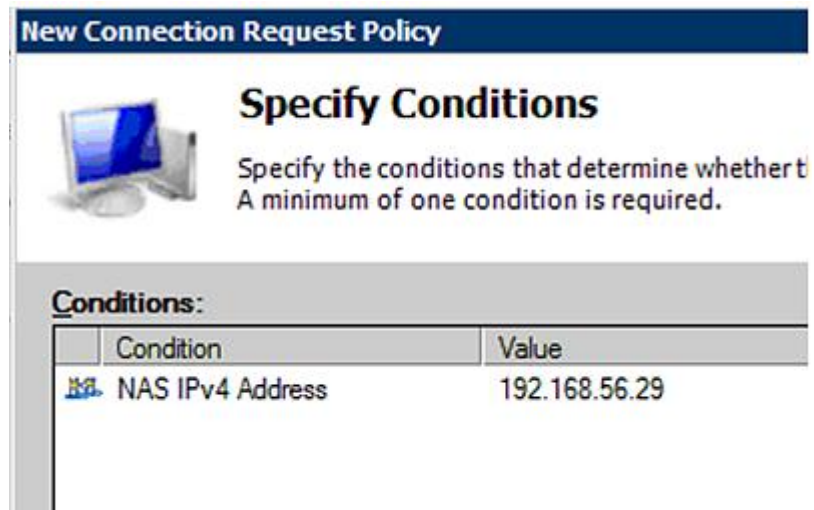
Buttons: Add..., Cancel

6. The NAS IPv4 Address dialog appears. Type the Branch Circuit Monitor IP address -- 192.168.56.29, and click OK.




The dialog box is titled "NAS IPv4 Address" and contains the instruction: "Specify the IPv4 address of the network access server sending the access request message. You can use pattern matching syntax." Below this is a text input field containing "192.168.56.29". At the bottom right are "OK" and "Cancel" buttons.

7. Click Next in the New Connection Request Policy dialog.



The dialog box is titled "New Connection Request Policy" and features a "Specify Conditions" section with a computer icon. The text reads: "Specify the conditions that determine whether t A minimum of one condition is required." Below this is a table with the heading "Conditions:".

Condition	Value
 NAS IPv4 Address	192.168.56.29

8. 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.

The screenshot shows a Windows-style dialog box titled "New Connection Request Policy". Inside, there's a sub-header "Specify Connection Request Forwarding" with a small icon of a computer. Below this, a text box explains: "The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group." A note states: "If the policy conditions match the connection request, these settings are applied." The "Settings:" section is divided into two panes. The left pane is titled "Forwarding Connection Request". The right pane contains the instruction: "Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication." There are three radio button options: 1. "Authenticate requests on this server" (which is selected). 2. "Forward requests to the following remote RADIUS server group for authentication:" followed by a dropdown menu showing "<not configured>" and a "New..." button. 3. "Accept users without validating credentials". At the bottom of the dialog are four buttons: "Previous", "Next", "Finish", and "Cancel".

9. When the system prompts you to select the authentication method, select the following two options:
 - Override network policy authentication settings
 - CHAP -- the Branch Circuit Monitor uses "CHAP" in this example

Note: If your Branch Circuit Monitor 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 do not select 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 they are listed.

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.

New Connection Request Policy

Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

Configure the settings for this network policy.
If conditions match the connection request and the policy grants access, settings are applied.

Settings:

Specify a Realm Name

Attribute

RADIUS Attributes

Standard

☒ Vendor Specific

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
------	-------

Add... Edit... Remove

Previous Next Finish Cancel

11. Select Filter-Id from the list of attributes and click Add.

Add Standard RADIUS Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:
All

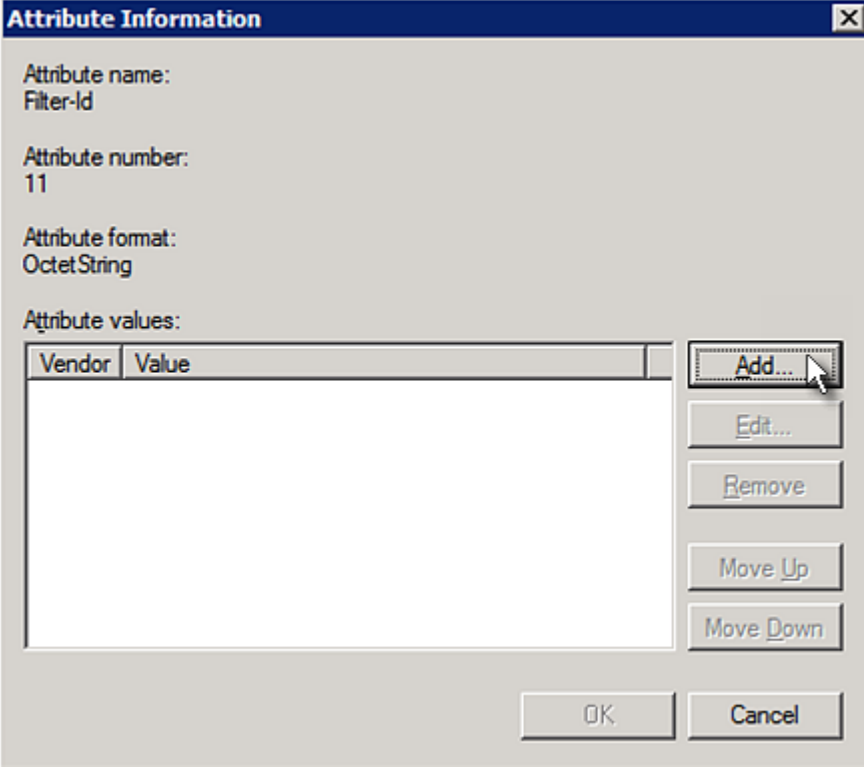
Attributes:

Name
Acct-Interim-Interval
Callback-Id
Callback-Number
Class
Filter-Id
Framed-AppleTalk-Link
Framed-AppleTalk-Network

Description:
Specifies the name of filter list for the user requesting authentication.

Add... Close

12. In the Attribute Information dialog, click Add.



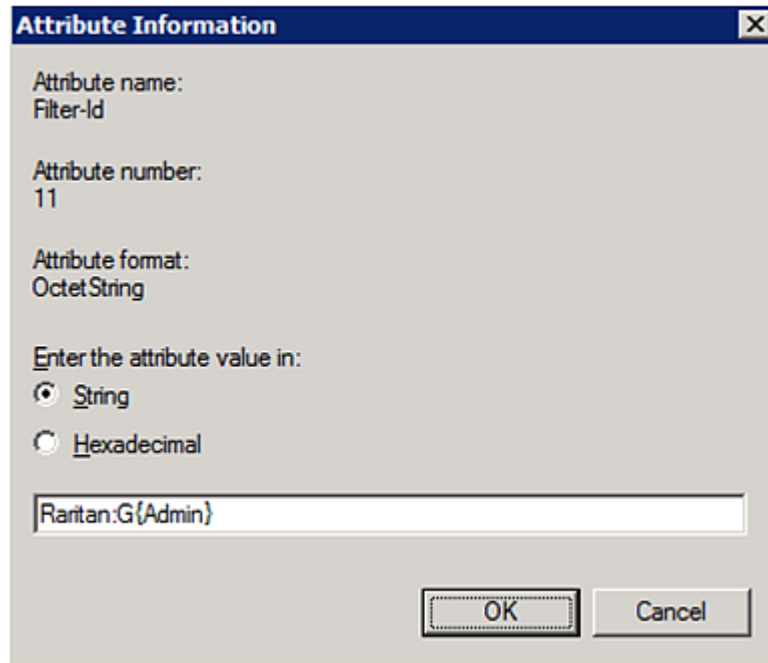
The image shows a Windows-style dialog box titled "Attribute Information". It contains the following fields and controls:

- Attribute name:** Filter-Id
- Attribute number:** 11
- Attribute format:** OctetString
- Attribute values:** A table with two columns: "Vendor" and "Value". The table is currently empty.
- Buttons:** "Add...", "Edit...", "Remove", "Move Up", "Move Down", "OK", and "Cancel".

A mouse cursor is pointing at the "Add..." button.

13. Select String, type *Raritan:G{Admin}* in the text box, and then click OK.

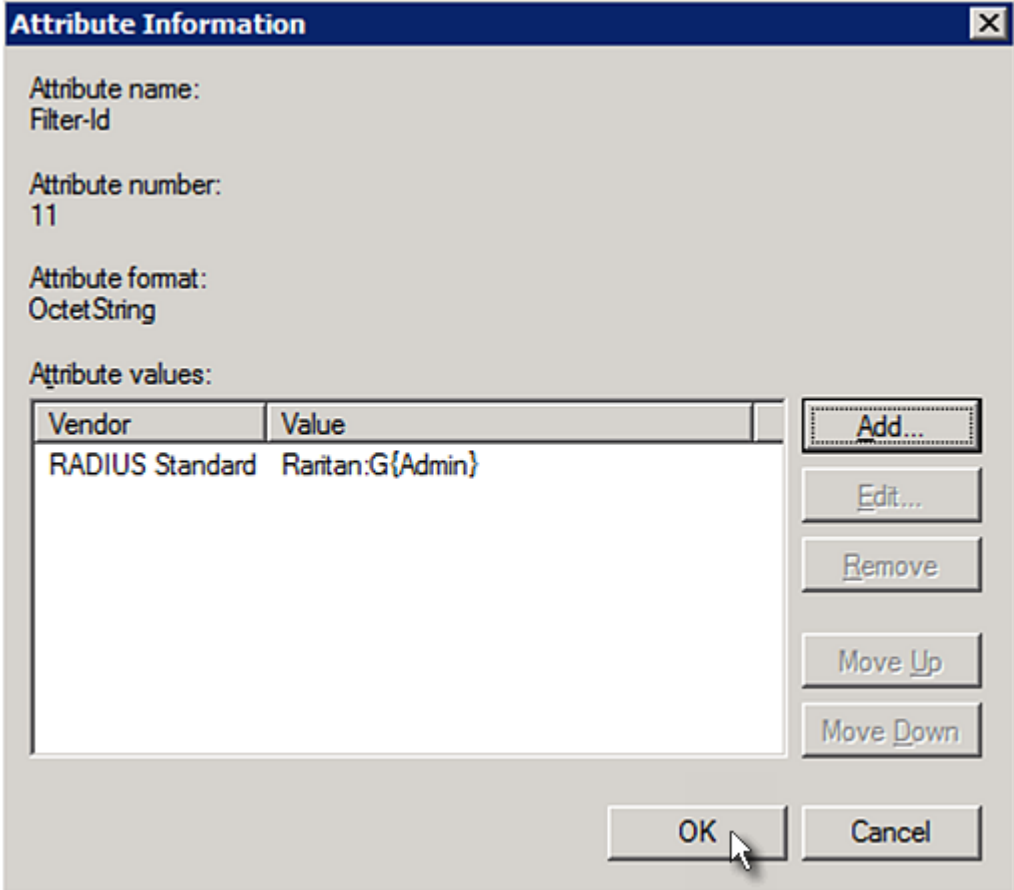
Admin inside the curved brackets {} is the existing role on the Branch Circuit Monitor. It is recommended to use the Admin role to test this configuration. The role name is case sensitive.



The image shows a Windows-style dialog box titled "Attribute Information". It contains the following fields and controls:

- Attribute name:** Filter-Id
- Attribute number:** 11
- Attribute format:** OctetString
- Enter the attribute value in:**
 - ☒ String
 - ☐ Hexadecimal
- Text input field:** Raritan:G{Admin}
- Buttons:** OK and Cancel

14. The new attribute is added. Click OK.



The dialog box is titled "Attribute Information" and contains the following fields and controls:

- Attribute name:** Filter-Id
- Attribute number:** 11
- Attribute format:** OctetString
- Attribute values:** A table with two columns: Vendor and Value.

Vendor	Value
RADIUS Standard	Raritan:G{Admin}

Buttons on the right side of the table:


- Add...
- Edit...
- Remove
- Move Up
- Move Down

Buttons at the bottom right:

- OK
- Cancel

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.

New Connection Request Policy

Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

KXII Policy

Policy conditions:

Condition	Value
NAS IPv4 Address	192.168.56.29

Policy settings:

Condition	Value
Authentication Provider	Local Computer
Override Authentication	Enabled
Authentication Method	Encryption authentication (CHAP)
Filter-Id	Raritan:G\Admin

To close this wizard, click Finish.

Step C: Configure a Vendor-Specific Attribute

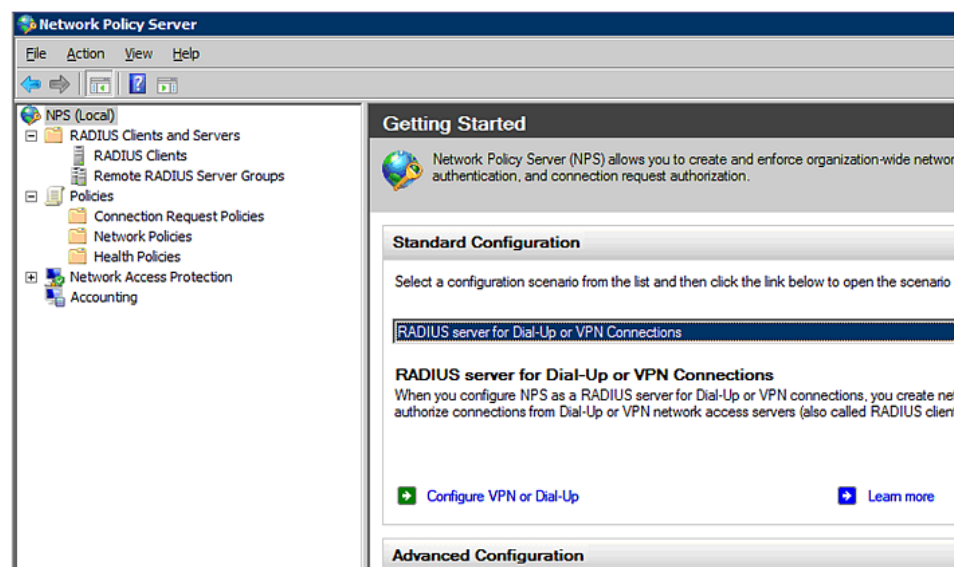
You must specify a vendor-specific attribute (VSA) for Raritan on Windows 2008 NPS. Raritan's vendor code is **13742**.

In the following illustration, we assume:

- There are three roles available on your Branch Circuit Monitor: *Admin*, *User*, and *SystemTester*.

► To configure VSA:

1. Open the NPS console, and expand the Policies folder.

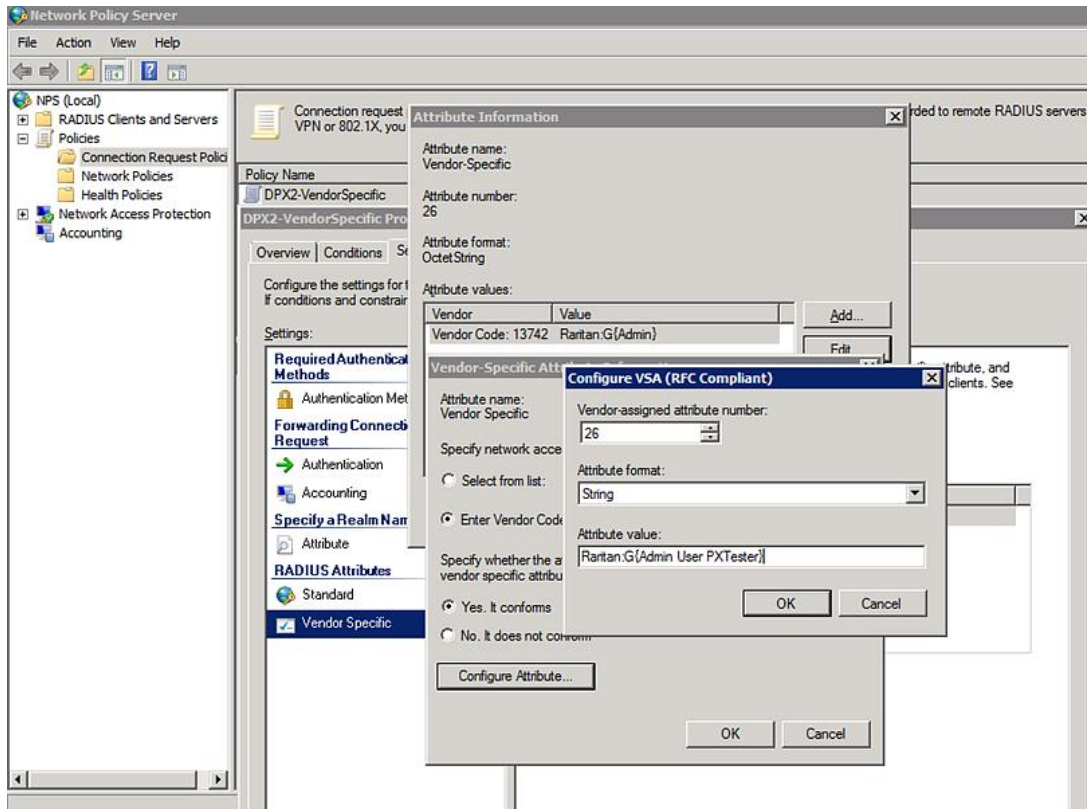


2. Select Connection Request Policies and double-click the policy where you want to add a custom VSA. The policy's properties dialog appears.
3. Click the Settings tab.
4. Select Vendor Specific, and click Add. The Add Vendor Specific Attribute dialog appears.
5. Select Custom in the Vendor field, and 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.

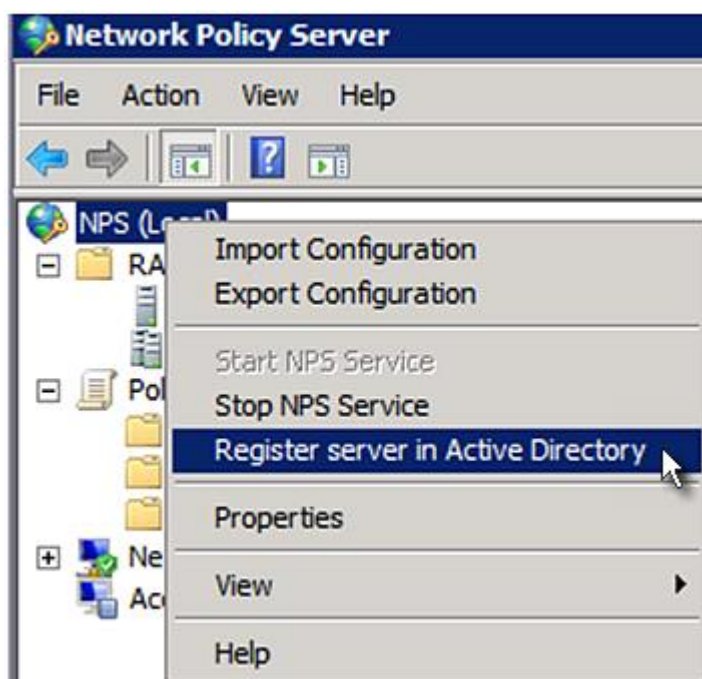
If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

- Store password using reversible encryption

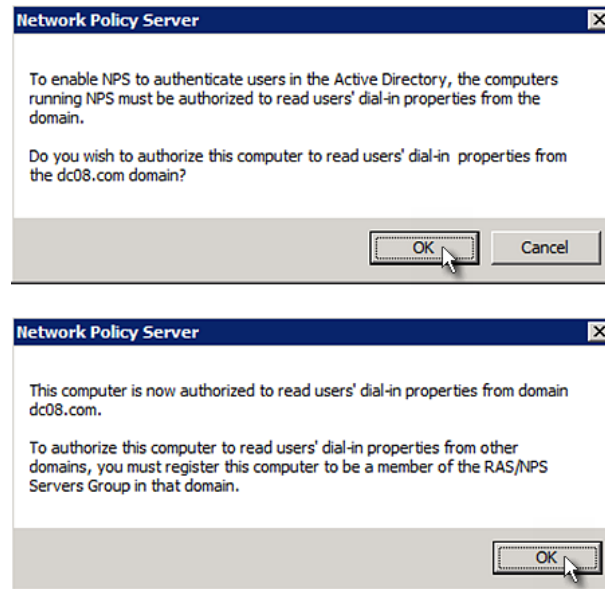
Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.

► **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 Branch Circuit Monitor 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 'Remote control Terminal Services Profile COM+' dialog box with the 'Dial-in' tab selected. The 'Network Access Permission' section has three radio buttons: 'Allow access' (selected), 'Deny access', and 'Control access through NPS Network Policy'. Below this is a checkbox for 'Verify Caller-ID:' which is unchecked. The 'Callback Options' section has three radio buttons: 'No Callback' (selected), 'Set by Caller (Routing and Remote Access Service only)', and 'Always Callback to:' (unchecked). Below this is a checkbox for 'Assign Static IP Addresses' which is unchecked, and a button labeled 'Static IP Addresses...'. The 'Apply Static Routes' section is also unchecked, with a button labeled 'Static Routes...'. At the bottom are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

► **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.

- Click the Account tab and select the "Store password using reversible encryption" checkbox.

The screenshot shows the Windows XP User Accounts control panel window with the 'Account' tab selected. The window has a title bar and a menu bar with 'Member Of', 'Dial-in', 'Environment', and 'Sessions'. Below the menu bar are tabs for 'Remote control', 'Terminal Services Profile', and 'COM+'. The main content area is divided into sections: 'User logon name:' with a text box and a dropdown; 'User logon name (pre-Windows 2000):' with two text boxes containing 'DC08\' and 'Administrator'; 'Logon Hours...' and 'Log On To...' buttons; an 'Unlock account' checkbox; 'Account options:' with a list of checkboxes including 'Store password using reversible encryption' which is checked; and 'Account expires' with radio buttons for 'Never' (selected) and 'End of:' followed by a date dropdown showing 'Saturday, May 23, 2009'. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

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 439).

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:

ATTRIBUTE Raritan-Vendor-Specific 26 Raritan:G{Admin User SystemTester}

Serial RS-232 Port Pinouts

RS-232 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DCD	Input	Data
2	RxD	Input	Receive data (data in)
3	TxD	Output	Transmit data
4	DTR	Output	Data terminal ready
5	GND	—	Signal ground
6	DSR	Input	Data set ready
7	RTS	Output	Request to send
8	CTS	Input	Clear to send
9	RI	Input	Ring indicator

Sensor RJ-12 Port Pinouts

RJ-12 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	+12V	—	Power (500mA, fuse protected)
2	GND	—	Signal Ground
3	—	—	—
4	—	—	—
5	GND	—	Signal Ground
6	1-wire		Used for Feature Port

Feature RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DTR	Output	Reserved
2	GND	—	Signal Ground
3	+5V	—	Power for CIM (200mA, fuse protected) Warning: Pin 3 is only intended for use with Raritan devices.
4	TxD	Output	Transmit Data (Data out)
5	RxD	Input	Receive Data (Data in)
6	+12V	—	Warning: Pin 6 is only intended for use with Raritan devices. Do NOT connect.
7	GND	—	Signal Ground
8	DCD	Input	Reserved

Appendix C Circuit Monitoring Worksheet

Branch Circuit Monitor Model _____

Branch Circuit Monitor Serial Number _____

Electrical Panel _____

1 (CT number)	(Circuit name)	2 (CT number)	(Circuit name)
3 (CT number)	(Circuit name)	4 (CT number)	(Circuit name)
5 (CT number)	(Circuit name)	6 (CT number)	(Circuit name)
7 (CT number)	(Circuit name)	8 (CT number)	(Circuit name)
9 (CT number)	(Circuit name)	10 (CT number)	(Circuit name)
11 (CT number)	(Circuit name)	12 (CT number)	(Circuit name)
13 (CT number)	(Circuit name)	14 (CT number)	(Circuit name)
15 (CT number)	(Circuit name)	16 (CT number)	(Circuit name)
17 (CT number)	(Circuit name)	18 (CT number)	(Circuit name)
19 (CT number)	(Circuit name)	20 (CT number)	(Circuit name)
21 (CT number)	(Circuit name)		

Appendix D Resetting to Factory Defaults

You can use either the reset button or the command line interface (CLI) to reset the Branch Circuit Monitor.

Important: Exercise caution before resetting the Branch Circuit Monitor 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.....	443
Using the CLI Command	444

Using the Reset Button

► **To reset to factory defaults using the reset button:**

1. Connect a computer to the Branch Circuit Monitor device. See **Connecting the Branch Circuit Monitor to a Computer** (on page 23).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the Branch Circuit Monitor. For information on the serial port configuration, see Step 2 of **Initial Network Configuration** (see "**Initial Network Configuration via CLI**" on page 26).
3. Press (and release) the Reset button of the Branch Circuit Monitor 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 Branch Circuit Monitor 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 Branch Circuit Monitor to factory defaults. For information on CLI, see **Using the Command Line Interface** (on page 276).

► **To reset to factory defaults after logging in to the CLI:**

1. Connect to the Branch Circuit Monitor device. See **Logging in to CLI** (on page 277) or **Connecting the Branch Circuit Monitor to a Computer** (on page 23).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the Branch Circuit Monitor. For information on the serial port configuration, see Step 2 of **Initial Network Configuration via CLI** (on page 26).
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 Branch Circuit Monitor provides an easier way to reset the product to factory defaults in the CLI prior to login.

1. Connect to the Branch Circuit Monitor 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 E 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 groups intended for the Branch Circuit Monitor
- b. Create user groups for the Branch Circuit Monitor on the AD server
- c. Configure LDAP authentication on the Branch Circuit Monitor device
- d. Configure roles on the Branch Circuit Monitor 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	445
Step B. Configure User Groups on the AD Server	446
Step C. Configure LDAP Authentication on the Branch Circuit Monitor Device	447
Step D. Configure Roles on the Branch Circuit Monitor	450

Step A. Determine User Accounts and Groups

Determine the user accounts and groups that are authenticated for accessing the Branch Circuit Monitor. In this example, we will create two user groups with different permissions. Each 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 for the Branch Circuit Monitor on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups for the Branch Circuit Monitor 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 Branch Circuit Monitor Device

You must enable and set up LDAP authentication properly on the Branch Circuit Monitor device to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See **Modifying Network Settings** (on page 107) and **Role of a DNS Server** (on page 110).
- 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 Branch Circuit Monitor 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.
- LDAP over SSL - Have the checkbox deselected since the TLS encryption is not applied in this example.
- Port - Ensure the field is set to 389.
- SSL Port and Server 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

☐ LDAP over SSL

Port: 389

SSL Port: 636

☐ Use only trusted LDAP Server Certificates

Server Certificate: not set Show... Remove...

select new certificate... Browse...

☐ 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

Test Connection

OK Cancel

- Click OK. The LDAP server is saved.
- Click OK. The LDAP authentication is activated.

Note: If the Branch Circuit Monitor 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 Branch Circuit Monitor and the LDAP server to use the same NTP server(s).

Step D. Configure Roles on the Branch Circuit Monitor

A role on the Branch Circuit Monitor determines the system permissions. You must create the roles whose names are identical to the user groups created for the Branch Circuit Monitor on the AD server or authorization will fail. Therefore, we will create the roles named *BCM_User* and *BCM_Admin* on the Branch Circuit Monitor.

In this illustration, we assume:

- Users assigned to the *BCM_User* role can only access the Branch Circuit Monitor and view settings.
- Users assigned to the *BCM_Admin* role can both access and configure the Branch Circuit Monitor because they have the Administrator permissions.

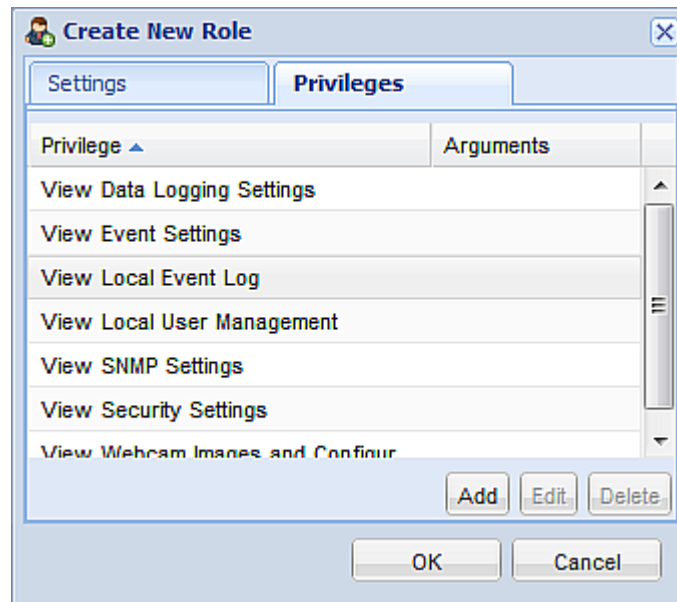
► **To create the BCM_User role with appropriate permissions assigned:**

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

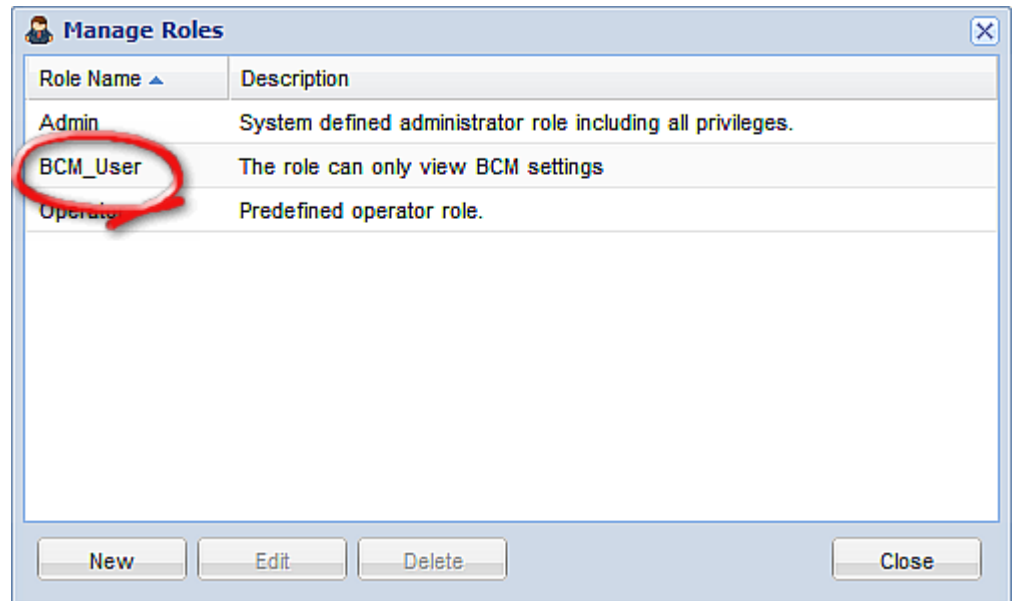
Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

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. In this example, we type "The role can only view BCM settings" to describe the role.
5. Click the Privileges tab to select all View XXX permissions (where XXX is the name of the setting). A View XXX permission lets users view the XXX 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.

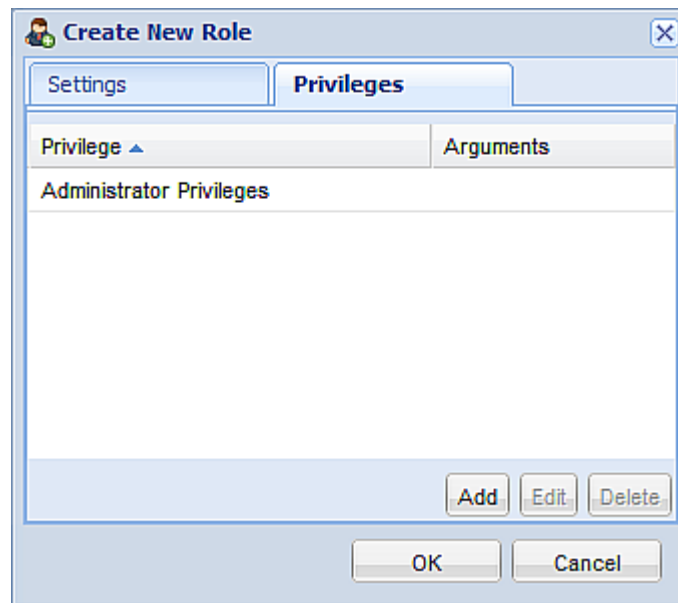


7. Keep the Manage Roles dialog opened to continue creating the BCM_Admin role.

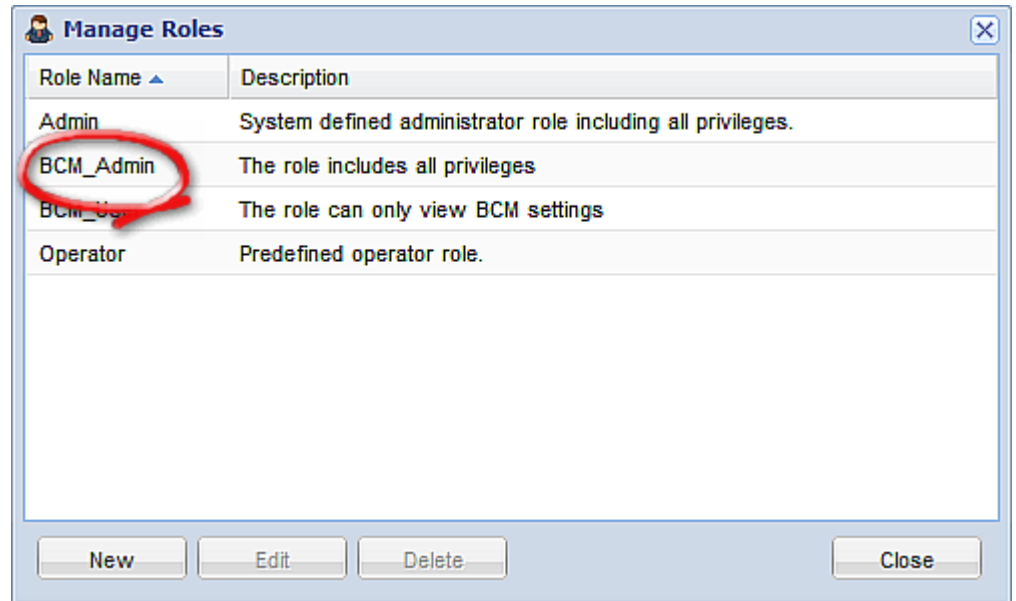
► **To create the BCM_Admin role with full permissions assigned:**

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 Branch Circuit Monitor 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 F Integration

The Branch Circuit Monitor device can work with certain Raritan products to provide diverse power solutions.

In This Chapter

Power IQ.....	454
Dominion KX II.....	457
RF Code Energy Monitoring Solution.....	460

Power IQ

You can use Raritan's Power IQ to collect the power measurement data of all Raritan Branch Circuit Monitor devices and remotely manage or monitor them.

In Power IQ, a Raritan Branch Circuit Monitor should be treated like a PDU and its branch circuit channels should be treated like a PDU's outlets.

Raritan'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, see either of the following available on Raritan's website:

- Power IQ User Guide: Available on the **Support page** (<http://www.raritan.com/support/>).
- Power IQ Online Help: Available on the **Product Online Help page** (<http://www.raritan.com/support/online-help/>).
- 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 on the **PX2 web page** (<http://www.raritan.com/support/product/px2/>) of the Raritan website.

Adding PDUs to Power IQ Management

Once Power IQ is configured, add Raritan PX or other PDUs to its management. Power IQ can then gather data from these PDUs. If you're adding a PDU that uses a custom dynamic plugin, see Adding PDUs with Custom Dynamic Plugins.

You can also add PDUs to Power IQ by uploading a CSV file containing the information. See Adding PDUs in Bulk with CSV Files in the Power IQ User Guide.

► To add PDUs to Power IQ management:

1. In the PDUs tab, click Add.
2. Enter the IP address of the PDU.
3. If the PDU is in a daisy-chained configuration or console server configuration, enter the PDU's position number in the chain or serial port number in the Proxy Index field. For example, this field is mandatory for a *slave* Raritan PDU in the port forwarding configuration. See Adding Raritan PDUs in the Port Forwarding Configuration.

You can also specify branch circuit monitors using the Proxy Index field. See Adding Veris Branch Circuit Monitors with Acquisuite.

Note: If the PDU is not in this type of configuration, leave the Proxy Index field blank.

4. Enter an asset tag number or other asset management code in the External Key field. **Optional.**
5. Enter data in Custom Field 1 and Custom Field 2. **Optional.** The labels may have been changed in Power IQ to identify these fields.
6. If the PDU is a Raritan PX, enter a valid Username and Password for the PDU in the PDU Administrative Credentials section. Re-enter the password in the Password Confirm field.
7. Select the SNMP Version.
 - For SNMP version 1/2c PDUs, enter an SNMP Community String that has at least READ permissions to this PDU. This enables polling the PDU for data. Enter an SNMP community string that has both READ and WRITE permissions to the PDU to enable power control, outlet naming, sensor naming, and buffered data retrieval.
 - For SNMP version 3 PDUs, enter the Username and select an Authorization Level. The authorization levels are:

- noAuthNoPriv - No Authentication Passkey, No Encoding Passkey
 - authNoPriv - Authentication Passkey, No Encoding Passkey
 - authPriv - Authentication Passkey, Encoding Passkey
- a. Depending on the Authorization Level selected, you must enter additional credentials for Authorization and Privacy.
 - b. Authorization Protocol: Select MD5 or SHA.
 - c. Enter the PDU's Authorization Passkey, then re-enter the passkey in the Authorization Passkey Confirm field.
 - d. Privacy Protocol: Select DES or AES.
 - e. Enter the PDU's Privacy Passkey, then re-enter the passkey in the Privacy Passkey Confirm field.

Note: You must enable the SNMP agent on all PDUs added to Power IQ.

8. Select "Validate and wait for discovery to complete before proceeding" to check credentials and view the discovery process status as you add this PDU. **Optional.** See Validating PDU Credentials in the Power IQ User Guide.
9. Click Add.

Note: PDU discovery is complete once the PDU model type is determined. SNMP fields such as contact or location values are not determined until this device is polled for the first time.

Once added, the PDU appears in the PDU list. Power IQ begins polling the PDU for sensor data. You can configure how often Power IQ polls PDU. See Configuring Polling Intervals in the Power IQ User Guide.

Dominion KX II

The Branch Circuit Monitor can be connected to the Raritan's Dominion KX II device (a digital KVM switch) to provide one additional alternative of remote monitoring.

The KX II allows you to connect Branch Circuit Monitor devices to KX II ports. The Branch Circuit Monitor configuration is done from the KX II Port Configuration page.

Note that this integration requires the following firmware versions:

- Dominion KX II -- 2.4 or later
- Branch Circuit Monitor -- 2.2.15 or later

Dominion KX II integration requires D2CIM-PWR and straight CAT5 cable.

For more information on Dominion KX II, see either of the following:

- Dominion KX II User Guide: Available on the Raritan website's **Support page** (<http://www.raritan.com/support/>).
- Dominion KX II Online Help: Available on the **Product Online Help page** (<http://www.raritan.com/support/online-help/>).

Connecting to KX II

The Branch Circuit Monitor is connected to the KX II using the D2CIM-PWR CIM.

► To connect the KX II:

1. Connect the male RJ-45 of the D2CIM-PWR to the female RJ-45 connector labeled "FEATURE" of the Branch Circuit Monitor.
2. Connect the female RJ-45 connector of the D2CIM-PWR to any of the available female system port connectors on the KX II using a straight through Cat5 cable.
3. Connect the Branch Circuit Monitor to an AC power source.
4. Power on the device.

Naming the Branch Circuit Monitor in the KX II

The Branch Circuit Monitor can be named in the Branch Circuit Monitor as well as in KX II.

Once a Branch Circuit Monitor is connected to the KX II, it will appear on the Port Configuration page. Click on the power port name on that page to access it. The Type and the Name fields are prepopulated.

Note: The (CIM) Type cannot be changed.

The following information is displayed for each branch circuit channel on the Branch Circuit Monitor: [Outlet] Number, Name, and Port Association.

Use this page to name the Branch Circuit Monitor and its branch circuit channels. Names can be up to 32 alphanumeric characters and can include special characters.

► **To name the Branch Circuit Monitor and branch circuit channels:**

Note: Raritan's CommandCenter Secure Gateway can be used to manage the KX II, and it does not recognize names containing spaces in KX II.

1. Enter the Name of the Branch Circuit Monitor (if needed).
2. Change the [Outlet] Name if desired. (Outlet names default to the branch circuit channel #.)

Home > Device Settings > Port Configuration > Port

Port 17

Type:

PowerStrip

Name:

PowerStrip-PCR8

Outlets

Number	Name	Port Association
1	Dominion-Port1(1)	Dominion- Port7
2	Outlet 2	
3	Outlet 3	
4	Outlet 4	
5	Outlet 5	
6	Outlet 6	
7	Outlet 7	
8	Outlet 8	

OK

Cancel

RF Code Energy Monitoring Solution

With the RF Code active RFID hardware and management software and Raritan's Branch Circuit Monitor combined, a wire-free energy monitoring solution that provides a picture of power utilization is offered.

This combined solution does not require any additional IP address configuration or association. All you need to do is plug an RF Code R170 PDU sensor tag into the SENSOR port of the Branch Circuit Monitor device.

The RF Code R170 PDU sensor tag collects the power data generated by Raritan Branch Circuit Monitor and sends the data to the RF Code Sensor Manager software, which not only manages the power data but also make computations about the power usage from the collected data.

You can use the RF Code Sensor Manager to manage the power data using:

- Live table views
- Map views
- Interactive graphing and reporting
- Scheduled graphing and reporting
- Alerting and thresholding

Appendix G Additional Branch Circuit Monitor Information

In This Chapter

Altitude Correction Factors	461
Raritan Training Website	462
Truncated Data in the Web Interface	462
Reserving IP Addresses in Windows DHCP Servers.....	463
Ways to Probe Existing User Profiles.....	463

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
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

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 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.

Truncated Data in the Web Interface

Some fields of the Branch Circuit Monitor 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 Branch Circuit Monitor uses its serial number as the client identifier in the DHCP request. Therefore, to successfully reserve an IP address for the Branch Circuit Monitor in a Windows® DHCP server, use the Branch Circuit Monitor device's serial number as the unique ID instead of the MAC address.

Convert the serial number into ASCII codes for the IP address reservation entry. For example, if the Branch Circuit Monitor device's serial number is PEG1A00003, use the serial number's ASCII codes "50 45 47 31 41 30 30 30 30 33" as the unique ID.

Ways to Probe Existing User Profiles

This section indicates available ways to query existing user accounts on the Branch Circuit Monitor.

- 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.

Index

A

- A Note about Enabling Thresholds • 277
- A Note about Infinite Loop • 217
- A Note about Untriggered Rules • 220
- About the Interface • 279
- Access Security Control • 152
- Accessing the Help • 265
- Action Group • 183, 185
- Actuator Configuration Commands • xiii, 385, 386, 393
- Actuator Control Operations • xiii, 401
- Actuator Information • 297
- Add Page Icon • 88, 92
- Adding a Firewall Rule • 343
- Adding a Monitored Device • 380
- Adding a Role-Based Access Control Rule • 357
- Adding Authentication Servers • 175
- Adding IT Devices for Ping Monitoring • 222
- Adding LDAP Server Settings • 175
- Adding PDUs to Power IQ Management • 457
- Adding RADIUS Server Settings • 178, 416
- Additional Branch Circuit Monitor Information • 463
- Adjusting Image Properties • 252, 254
- Adjusting the Pane • 90
- AD-Related Configuration • 416, 437
- Alarm • 184, 185
- Alarms List • 99
- Alerted Sensors • 98
- All Privileges • 375
- Altitude Correction Factors • 127, 463
- Asset Management • 245
- Asset Management Commands • 395
- Asset Sensor Management • 395
- Asset Sensor Settings • 303
- Automatically Completing a Command • 408

B

- Backup and Restore of Branch Circuit Monitor Device Settings • 32, 264
- Before You Begin • 8
- Blade Extension Strip Settings • 304
- Branch Circuit Accuracy • 414
- Branch Circuit Channels • 69
- Branch Circuit CTs Rated at 60A • 412, 413

- Branch Circuit Information • 74, 288
- Branch Circuit Monitor Specifications • 410
- Branch Circuit Pole Threshold Information • 291
- Branch Circuit Threshold Information • 290
- Browser-Defined Shortcut Menu • 97
- Browsing through the Online Help • 265
- Bulk Configuration • 32, 264
- Bulk Configuration for Branch Circuit Thresholds • 140, 141

C

- Cascading the Branch Circuit Monitor via USB • 4, 37, 70, 78, 80, 102, 108
- Certificate Signing Request • 168
- Changing a Specific Rack Unit's LED Color Settings • 248
- Changing a User's Password • 363
- Changing Default Thresholds • 237
- Changing HTTP(S) Settings • 114, 153
- Changing Measurement Units • 369, 372
- Changing Modbus/TCP Settings • 119
- Changing SSH Settings • 115, 147
- Changing Telnet Settings • 116
- Changing the Column • 95
- Changing the Default Policy • 153, 154, 163, 164
- Changing the Device Name • 312
- Changing the LAN Duplex Mode • 330
- Changing the LAN Interface Speed • 330
- Changing the Modbus Configuration • 336
- Changing the Modbus Port • 337
- Changing the Role List View • 152
- Changing the Role(s) • 369
- Changing the Sensor Description • 388
- Changing the Sensor Name • 386
- Changing the Sorting • 96, 221
- Changing the SSH Configuration • 333
- Changing the SSH Port • 333
- Changing the Telnet Configuration • 332
- Changing the Telnet Port • 333
- Changing the User List View • 149
- Changing the View of a List • 95, 100, 149, 152, 225, 259
- Changing Your Own Password • 372
- Changing Your Password • 85
- Channel Convention • 12, 18, 20, 21, 68, 69, 134

- Channel or CT Configuration • 131
 - Channels • 68
 - Checking Server Monitoring States • 224
 - Checking the AC Electrical Panel • 9
 - Checking the Accessibility of NTP Servers • 341
 - Checking the Internal Beeper State • xiii, 130
 - Circuit Monitoring Worksheet • 9, 15, 444
 - Clearing Event Entries • 226
 - Clearing Event Log • 310
 - Clearing Information • 310
 - Closing a Local Connection • 282
 - Collapsing the Tree • 90
 - Combining Asset Sensors • 53
 - Command History • 308
 - Components of an Event Rule • 182
 - Configuring Environmental Sensors • 227, 233, 237, 238
 - Configuring Environmental Sensors' Default Thresholds • xiii, 383
 - Configuring IP Protocol Settings • 314
 - Configuring IPv4 Parameters • 321
 - Configuring IPv6 Parameters • 325
 - Configuring SMTP Settings • 129, 189, 190
 - Configuring SNMP Notifications • 118, 215, 216, 270
 - Configuring the Asset Sensor • 245
 - Configuring the Branch Circuit Channels • 15, 35, 74, 76, 133, 135, 137, 289, 291
 - Configuring the Branch Circuit Monitor • 22, 110
 - Configuring the Branch Circuit Monitor Device and Network • 310
 - Configuring the Cascading Mode • 38, 394
 - Configuring the Feature Port • 124
 - Configuring the Firewall • 153
 - Configuring the Mains Channels • 15, 76, 98, 132, 137, 290
 - Configuring the Serial Port • 65, 126, 281
 - Configuring the SNMP Settings • 117, 145
 - Configuring Users for Encrypted SNMP v3 • 118, 268, 269
 - Configuring Webcam Storage • 199, 251, 257, 258, 259
 - Configuring Webcams • 251, 252, 254, 258
 - Connect a DPX Using an Optional Sensor Hub • 43
 - Connecting a DPX2 Sensor Package to DX • 51, 52
 - Connecting a GSM Modem • xiii, 64
 - Connecting a Logitech Webcam • 63, 88, 89, 251
 - Connecting an Analog Modem • xiii, 65, 281
 - Connecting an Electrical Conduit • 10
 - Connecting an External Beeper • xiii, 65
 - Connecting an RF Code PDU Sensor Tag • 66
 - Connecting Asset Sensors to the Branch Circuit Monitor • 55, 59
 - Connecting Blade Extension Strips • 56
 - Connecting Branch Circuit CTs • 14, 19, 69
 - Connecting Composite Asset Sensors to BCM • 59
 - Connecting Composite Asset Sensors Using an X Cable • 60
 - Connecting Environmental Sensor Packages • 40, 62, 227
 - Connecting External Equipment (Optional) • 40
 - Connecting Mains CTs • 14, 17, 69
 - Connecting the Asset Management Sensor • 53, 245
 - Connecting the Branch Circuit Monitor to a Computer • 23, 445, 446
 - Connecting the Branch Circuit Monitor to Your Network • 25, 107, 108
 - Connecting to KX II • 459
 - Connection Ports • 3, 69
 - Control Buttons • 73
 - Controlling Actuators • 244
 - Copying the Branch Circuit Monitor Configuration • 34
 - Creating a Certificate Signing Request • 168
 - Creating a Role • 147, 150, 374, 416
 - Creating a Self-Signed Certificate • 170
 - Creating a User Profile • 83, 115, 144, 148, 149, 150, 151, 269, 362
 - Creating Actions • 64, 99, 183, 206, 219, 251
 - Creating an Event Rule • 65, 183
 - Creating Firewall Rules • 153, 155
 - Creating Role-Based Access Control Rules • 163, 164
 - Creating Rules • 200
 - CT Dimensions • 16
 - CT Terminals and Buttons • 69
- ## D
- Daisy-Chain Limitations of Composite Asset Sensors • 60, 62
 - Data Pane • 93
 - Date and Time Settings • 287

- Default Log Messages • 207
 - Default Measurement Units • 288
 - Deleting a Firewall Rule • 346
 - Deleting a Monitored Device • 381
 - Deleting a Role • 152, 378
 - Deleting a Role-Based Access Control Rule • 360
 - Deleting a User Profile • 148, 371
 - Deleting an Event Rule or Action • 220
 - Deleting Authentication Server Settings • 180
 - Deleting Firewall Rules • 158
 - Deleting Ping Monitoring Settings • 224
 - Deleting Role-Based Access Control Rules • 167
 - Describing the Sensor or Actuator's Location • 233, 236
 - Determining the SSH Authentication Method • 334
 - Determining the Time Setup Method • 338
 - Device Configuration • 285
 - Device Configuration Commands • 312
 - Device Management • 100
 - Diagnostic Commands • 405
 - Dictionary File • 440
 - Different CLI Modes and Prompts • 280, 281, 282, 284, 310, 311, 341, 401, 405
 - Disabling External Authentication • 180
 - Disabling the Automatic Management Function • 244
 - Displaying the Asset Sensor Information • 250
 - Displaying the Device Information • 101
 - Dominion KX II • 459
 - Downloading Diagnostic Information • 264
 - Downloading Key and Certificate Files • 172
 - Downloading SNMP MIB • 118, 269, 270, 271, 273, 275
 - DPX Sensor Packages • xiii, 41
 - DPX2 Sensor Packages • xiii, 46
 - DX Sensor Packages • xiii, 49
- E**
- EAP CA Certificate Example • 318, 320
 - Editing Authentication Server Settings • 180
 - Editing Firewall Rules • 157
 - Editing Ping Monitoring Settings • 223
 - Editing Role-Based Access Control Rules • 166
 - Email and SMS Message Placeholders • 190, 191, 196, 197, 212
 - Enabling and Editing the Security Banner • 162
 - Enabling Data Logging • 128
 - Enabling External and Local Authentication Services • 181
 - Enabling IPv4 or IPv6 • 315
 - Enabling Login Limitations • 160, 256
 - Enabling or Disabling a User Profile • 365
 - Enabling or Disabling Data Logging • 313
 - Enabling or Disabling Modbus • 336
 - Enabling or Disabling SNMP v1/v2c • 334
 - Enabling or Disabling SNMP v3 • 335
 - Enabling or Disabling SSH • 333
 - Enabling or Disabling Strong Passwords • 353
 - Enabling or Disabling Telnet • 332
 - Enabling or Disabling the Read-Only Mode • 337
 - Enabling or Disabling the Restricted Service Agreement • 347
 - Enabling or Disabling the Service Advertisement • 337
 - Enabling Password Aging • 161
 - Enabling Service Advertisement • 120, 337
 - Enabling SNMP • 128, 268
 - Enabling Strong Passwords • 161
 - Enabling the Feature • 163
 - Enabling the Firewall • 153
 - Enabling User Blocking • 159
 - Entering Configuration Mode • 282, 311, 320
 - Entering Diagnostic Mode • 282, 405
 - Environmental Sensor Configuration Commands • xiii, 385
 - Environmental Sensor Default Thresholds • 299
 - Environmental Sensor Information • xiii, 77, 294
 - Environmental Sensor Package Information • 296
 - Environmental Sensor Threshold Configuration Commands • xiii, 390
 - Environmental Sensor Threshold Information • 298
 - Environmental Sensors and Actuators • 227
 - Event Log • 305
 - Event Rules and Actions • 117, 129, 139, 182, 222, 270
 - Example • 349
 - When Hysteresis is Useful • 143
 - When to Disable Hysteresis • 143
 - Example - Actuator Naming • 394
 - Example - Default Upper Thresholds for Temperature • 385
 - Example - Ping Command • 408
 - Example - Server Settings Changed • 383

Example - Turning On a Specific Actuator • 403
 Example 1 • 217
 Example 1 - Asset Sensor LED Colors for Disconnected Tags • 401
 Example 1 - Basic Security Information • 309
 Example 1 - Combination of IP, Subnet Mask and Gateway Parameters • 379
 Example 1 - Creating a User Profile • 373
 Example 1 - Environmental Sensor Naming • 390
 Example 1 - IPv4 Firewall Control Configuration • 360
 Example 1 - Networking Mode • 338
 Example 1 - Time Setup Method • 340
 Example 1 - Upper Critical Threshold for a Temperature Sensor • 392
 Example 2 • 217
 Example 2 - Adding an IPv4 Firewall Rule • 361
 Example 2 - Combination of SSID and PSK Parameters • 379
 Example 2 - Enabling Both IP Protocols • 338
 Example 2 - In-Depth Security Information • 309
 Example 2 - Modifying a User's Roles • 374
 Example 2 - Primary NTP Server • 341
 Example 2 - Rack Unit Naming • 401
 Example 2 - Sensor Threshold Selection • 390
 Example 3 - Default Measurement Units • 374
 Example 3 - User Blocking • 361
 Example 3 - Wireless Authentication Method • 338
 Example 4 - Adding an IPv4 Role-based Access Control Rule • 361
 Example 4 - Static IPv4 Configuration • 338
 Examples • 308, 338, 340, 360, 373, 389, 401
 Existing Roles • 302
 Existing User Profiles • 288, 301
 Expanding a Blade Extension Strip • 249
 Expanding the Tree • 88, 135, 136, 137, 138, 139, 140, 141, 228, 231, 233, 239, 243, 244
 Explorer Pane • 87
 External Beeper • 184, 187

F

Feature RJ-45 Port Pinouts • 442
 Firewall Control • 341
 Firmware Upgrade • 34, 260
 Forcing a Password Change • 365

Forcing HTTPS Encryption • 153, 168
 Format of the • 441
 Full Disaster Recovery • 261

G

Gathering the External Authentication Information • 173
 Gathering the LDAP Information • 174
 Gathering the RADIUS Information • 174

H

Help Command • 283
 History Buffer Length • 308
 How to Use the Calendar • 122

I

Identifying Branch Circuit Channel Numbers • 74, 75, 289, 290, 291
 Identifying Cascaded Devices • 39, 101, 102
 Identifying Environmental Sensors • 227, 228, 232
 Identifying Sensor or Actuator Channels • 231
 Idle Timeout • 352
 Initial Network Configuration via CLI • 26, 91, 445, 446
 Installation and Configuration • 8
 Installing a CA-Signed Certificate • 170
 Installing Existing Key and Certificate Files • 172
 Installing the USB-to-Serial Driver (Optional) • 23, 24, 276
 Integration • 456
 Internal Beeper • 198
 Introduction • 1
 Introduction to the Web Interface • 86
 IP Address • 22, 79
 IP Configuration • 285

L

LAN Interface Settings • 286
 Layout • 276
 LCD Display • 71
 LCD Display Panel • 71
 LDAP Configuration Illustration • 178, 447
 Line Cord • 67
 Listing TCP Connections • 263
 Log an Event Message • 184, 188
 Logging in to CLI • 279, 446

- Logging in to the Web Interface • 83
- Logging out of CLI • 409
- Login • 35, 83
- Login Limitation • 350
- Logout • 85
- Logout Button • 93
- Lowercase Character Requirement • 353

M

- MAC Address • 81
- Mains Accuracy • 414
- Mains Channels • 68
- Mains CT Rated at 200A • 410
- Mains CT Rated at 250A • 411
- Mains Information • 76, 289
- Mains Pole Threshold Information • 293
- Mains Threshold Information • 292
- Managing Environmental Sensors and Actuators • 49, 227, 231
- Managing Event Logging • 225
- Managing Firewall Rules • 343
- Managing Role-Based Access Control Rules • 357
- Managing the Snapshots Saved to Branch Circuit Monitor • 258
- Mapping Channels with Branch Circuits • 35, 136
- Matching the Position • 230
- Matching the Serial Number • 229
- Maximum Ambient Operating Temperature • 9, 415
- Maximum Password History • 355
- Maximum Password Length • 353
- Menus • 87
- Microsoft Network Policy Server • 416
- Minimum Password Length • 353
- Modifying a Firewall Rule • 345
- Modifying a Monitored Device's Settings • 381
- Modifying a Role • 147, 148, 151, 376
- Modifying a Role-Based Access Control Rule • 358
- Modifying a User Profile • 85, 148, 151, 363
- Modifying a User's Personal Data • 364
- Modifying an Action • 118, 219
- Modifying an Event Rule • 218
- Modifying Firewall Control Parameters • 342
- Modifying IPv4 Settings • 111
- Modifying IPv6 Settings • 112
- Modifying Network Interface Settings • 107
- Modifying Network Service Settings • 114, 279, 280

- Modifying Network Settings • 91, 110, 120, 449
- Modifying Role-Based Access Control Parameters • 355
- Modifying SNMPv3 Settings • 366
- Modifying the Network Configuration • 106
- Monitoring a Channel • 138
- Monitoring All Channels • 137
- Monitoring Server Accessibility • 222
- Monitoring the Branch Circuit Channels • 137
- Monitoring the Mains Channels • 136
- More Information • 93
- More Information about AD or RADIUS Configuration • 178
- Mounting the Branch Circuit Monitor • 11, 14
- Multi-Command Syntax • 343, 350, 352, 353, 356, 363, 364, 366, 369, 372, 379, 381, 383, 390, 393

N

- Naming a Rack Unit • 398
- Naming an Asset Sensor • 395
- Naming Branch Circuit Channels • 135
- Naming the Branch Circuit Monitor • 88, 90, 91, 106, 127, 130, 132, 133, 135, 136, 137, 139, 141, 228, 232, 233, 235, 239, 243, 244
- Naming the Branch Circuit Monitor in the KX II • 460
- Naming the Mains Channels • 135
- Network Configuration • 285
- Network Configuration Commands • 313
- Network Diagnostics • 262
- Network Service Settings • 287
- Network Troubleshooting • 262, 405
- Networking Mode • 286
- Non-Windows RADIUS Server • 416, 440
- Numeric Character Requirement • 354

O

- Observing the Safety Guidelines and Instructions • 8
- Operating the LCD Display • 41, 74
- Overriding DHCP-Assigned NTP Servers • 339, 341
- Overriding the IPv4 DHCP-Assigned DNS Server • 323, 324
- Overriding the IPv6 DHCP-Assigned DNS Server • 327, 328
- Overview • 2

P

Package Contents • 7, 8
 Panel Components • 67
 Password Aging • 351
 Password Aging Interval • 351
 Pinging a Host • 263
 Power IQ • 456
 Power Measurement Accuracy • 414
 Printing the Circuit Monitoring Worksheet • 9
 Product Features • 4
 Product Models • 3
 Push Out Sensor Readings • 188

Q

Querying Available Parameters for a Command • 283, 284
 Querying DNS Servers • 406
 Quitting Configuration Mode • 311, 348
 Quitting Diagnostic Mode • 405

R

Rack Unit Configuration • 398
 Rack Unit Settings of an Asset Sensor • 303
 RADIUS Configuration Illustration • 178, 416
 Raritan CT Specifications • 132, 133, 410
 Raritan Current Transformers (Optional) • 16
 Raritan Training Website • 464
 Rebooting the Branch Circuit Monitor Device • 131
 Record Snapshots to Webcam Storage • 184, 199
 Reliability Data • 307
 Reliability Error Log • 308
 Reserving IP Addresses in Windows DHCP Servers • 465
 Reset Button • 81
 Resetting the Branch Circuit Monitor • 403
 Resetting to Factory Defaults • 81, 404, 445
 Resizing a Dialog • 96
 Restarting the Device • 404
 Restricted Service Agreement • 347
 Retrieving Previous Commands • 408
 Retrieving Software Packages Information • 265
 RF Code Energy Monitoring Solution • 66, 462
 Role Configuration Commands • 374
 Role of a DNS Server • 113, 449

Role-Based Access Control • 355

S

Safety Guidelines • iii, 8
 Safety Instructions • iv, 8
 Sample Branch Circuit-Level Event Rule • 216
 Sample Device-Level Event Rule • 215
 Sample Event Rules • 215
 Sample Mains-Level Event Rule • 215
 Saving a Branch Circuit Monitor Configuration • 33
 Saving Snapshots • 251, 254, 257, 258
 Scheduling an Action • 188, 205
 Security Configuration Commands • 341
 Security Settings • 300
 Selecting IPv4 or IPv6 Addresses • 315
 Selecting the Internet Protocol • 110, 111, 112
 Send a Snapshot via Email • 184, 189
 Send an SNMP Notification • 184, 191
 Send Email • 184, 190, 207
 Send Sensor Report • 184, 195
 Send SMS Message • 184, 197
 Sending Snapshots or Videos in an Email or Instant Message • 222, 251, 253, 255
 Sensor RJ-12 Port Pinouts • 442
 Serial Port Configuration Commands • 378
 Serial Port Settings • 302
 Serial RS-232 Port Pinouts • 442
 Server Reachability Configuration Commands • 380
 Server Reachability Information • 306
 Server Reachability Information for a Specific Server • 307
 Setting an LED Color for a Rack Unit • 399, 400
 Setting an LED Mode for a Rack Unit • 399, 400
 Setting Asset Sensor LED Colors • 247
 Setting Data Logging • 128, 313
 Setting Default Measurement Units • 124, 149, 369, 372
 Setting EAP Parameters • 318
 Setting IPv4 Static Routes • 325
 Setting IPv6 Static Routes • 329
 Setting LAN Interface Parameters • 329
 Setting LED Colors for Connected Tags • 397, 399, 400
 Setting LED Colors for Disconnected Tags • 398, 399, 400
 Setting Network Service Parameters • 330

- Setting NTP Parameters • 339, 341
- Setting Power Thresholds • 94, 139, 277
- Setting the Alarmed to Normal Delay for DX-PIR • 389
- Setting the Authentication Method • 316
- Setting the Automatic Daylight Savings Time • 340
- Setting the Branch Circuit Thresholds • 140, 141
- Setting the BSSID • 321
- Setting the Data Logging Measurements Per Entry • 313
- Setting the Date and Time • 121
- Setting the History Buffer Length • 378
- Setting the HTTP Port • 331
- Setting the HTTPS Port • 332
- Setting the IPv4 Address • 322
- Setting the IPv4 Configuration Mode • 322
- Setting the IPv4 Gateway • 323
- Setting the IPv4 Preferred Host Name • 322
- Setting the IPv4 Primary DNS Server • 323
- Setting the IPv4 Secondary DNS Server • 324
- Setting the IPv4 Subnet Mask • 323
- Setting the IPv6 Address • 327
- Setting the IPv6 Configuration Mode • 326
- Setting the IPv6 Gateway • 327
- Setting the IPv6 Preferred Host Name • 326
- Setting the IPv6 Primary DNS Server • 327
- Setting the IPv6 Secondary DNS Server • 328
- Setting the LED Operation Mode • 399
- Setting the Mains Thresholds • 139
- Setting the Networking Mode • 314
- Setting the PSK • 317
- Setting the Serial Port Baud Rate • 378
- Setting the SNMP Configuration • 334
- Setting the SNMP Read Community • 335
- Setting the SNMP Write Community • 335
- Setting the SSID • 316
- Setting the sysContact Value • 335
- Setting the sysLocation Value • 336
- Setting the sysName Value • 336
- Setting the Time Zone • 340
- Setting the X Coordinate • 387
- Setting the Y Coordinate • 387
- Setting the Z Coordinate • 312, 388
- Setting the Z Coordinate Format • 235
- Setting the Z Coordinate Format for Environmental Sensors • 312, 388, 394
- Setting Thresholds for Multiple Sensors • 238
- Setting Up a Power Monitoring System • 14, 35
- Setting Up a TLS Certificate • 152, 167
- Setting Up External Authentication • 113, 152, 173
- Setting Up Role-Based Access Control Rules • 163
- Setting Up Roles • 85, 128, 144, 147, 150
- Setting Up User Login Controls • 159
- Setting Up User Preferences (Units of Measure) • 369, 371
- Setting Up Your Preferred Measurement Units • 124, 127, 148, 149
- Setting Wireless Parameters • 316
- Setup Button • 90
- Showing Information • 284
- Showing Network Connections • 406
- Single Login Limitation • 351
- Snapshot Storage • 257
- SNMP Gets and Sets • 275
- SNMP Sets and Thresholds • 277
- SNMPv2c Notifications • 271
- SNMPv3 Notifications • 273
- Sorting Firewall Rules • 158
- Sorting Role-Based Access Control Rules • 166
- Sorting the Access Order • 179
- Special Character Requirement • 355
- Specifications • 410
- Specifying the Agreement Contents • 348
- Specifying the Asset Sensor Orientation • 397
- Specifying the CC Sensor Type • 386
- Specifying the Device Altitude • 127
- Specifying the Number of Rack Units • 395
- Specifying the Primary NTP Server • 339
- Specifying the Rack Unit Numbering Mode • 396
- Specifying the Rack Unit Numbering Offset • 396
- Specifying the Secondary NTP Server • 339
- Specifying the SSH Public Key • 334, 371
- States of Managed Sensors • 240
- Status Bar • 91
- Step A
 - Add Your Branch Circuit Monitor as a RADIUS Client • 417
- Step A. Determine User Accounts and Groups • 447
- Step B
 - Configure Connection Request Policies • 420
- Step B. Configure User Groups on the AD Server • 448
- Step C

- Configure a Vendor-Specific Attribute • 435
- Step C. Configure LDAP Authentication on the Branch Circuit Monitor Device • 449
- Step D. Configure Roles on the Branch Circuit Monitor • 452
- Strong Passwords • 353
- Supported Maximum DPX Sensor Distances • 45
- Supported Web Browsers • 83
- Supported Wireless LAN Configuration • 26
- Switch Peripheral Actuator • 198
- Switching Off an Actuator • 402
- Switching On an Actuator • 402
- Syslog Message • 184, 193

T

- Testing the Network Connectivity • 407
- Testing the Server Connection • 179
- The Branch Circuit Monitor MIB • 275
- The Yellow- or Red-Highlighted Sensors • 94, 98, 99, 136, 138, 139, 239
- Time Configuration Commands • 338
- Tracing the Network Route • 263
- Tracing the Route • 408
- Truncated Data in the Web Interface • 464

U

- Unblocking a User • 159, 403
- Unmanaging Environmental Sensors • 49, 233, 243
- Unpacking the Product and Components • 8
- Updating the Branch Circuit Monitor Firmware • 37, 260
- Uppercase Character Requirement • 354
- USB Wireless LAN Adapters • 25, 26, 37, 103
- USB-Cascading Configuration Commands • xiii, 394
- USB-Cascading Configuration Information • 300
- User Blocking • 352
- User Configuration Commands • 362
- User Management • 144
- Using Default Thresholds • 389
- Using SNMP • 261, 267
- Using the CLI Command • 404, 446
- Using the Command Line Interface • 114, 236, 278, 446
- Using the Reset Button • 445
- Using the Web Interface • 82

V

- Viewing Connected Users • 221, 253, 255
- Viewing Firmware Update History • 261
- Viewing Sensor Data and Actuator Data • 239
- Viewing the Communication Log • 92, 262
- Viewing the Dashboard • 98
- Viewing the Local Event Log • 129, 175, 193, 225
- Viewing the Wireless LAN Diagnostic Log • 226
- Viewing Webcam Snapshots or Videos • 64, 253

W

- Warning Icon • 93
- Ways to Probe Existing User Profiles • 465
- Webcam Management • 251
- What is Assertion Timeout? • 140, 141, 142, 144, 234
- What is Deassertion Hysteresis? • 139, 140, 141, 142, 220, 234
- What's New in the Branch Circuit Monitor Release 3.1.0 • xiii
- Wired Network Settings • 107
- Wireless Configuration • 286
- Wireless LAN Diagnostic Log • 306
- Wireless Network Settings • 108
- With an Analog Modem • 281
- With HyperTerminal • 279, 403
- With SSH or Telnet • 280

► 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