



# BCM2 Power Meter User Guide

Copyright © 2025 Raritan  
BCM\_G2\_UG\_C1\_4.3.0  
January 2025  
Release 4.3.0

# Contents

<b>Safety Information</b>	<b>8</b>
<b>Installation and Initial Configuration</b>	<b>10</b>
Product Models	10
Hardware Installation	10
BCM2 Series Hardware Installation	10
PM Series Hardware Installation: PMC-1000, PMC-1001, PMM-1000, PMB-1960, PMMC-1000	19
Login and Configuration	33
Configuring Power Meters and Branch Circuit Monitors	34
Using the BCM2's Display	38
Automatic and Manual Modes	39
Control Buttons	39
Power Meters	40
Peripherals	43
<b>Using the Web Interface</b>	<b>48</b>
Supported Web Browsers and Mobile Devices	48
Login, Logout and Password Change	48
Login and Logout	48
Changing Your Password	49
Logout	50
Introduction to the Web Interface	50
Menu	52
Quick Access to a Specific Page	54
Sorting a List	54
Viewing the Dashboard	54
Dashboard - Power Meters	55
Dashboard - Alerted Sensors	56
Dashboard - Alarms	57
Dashboard - Power Meter History	58
PMC Power Metering Controller	59
Power Meters	61
Viewing the Power Meter Data	61
Power Meter Management	63
Enable Modbus Access	63
Viewing the Panel Data	64
Panel Mains Circuit Management	67

Panel Branch Circuits Operations. . . . .	67
Setting Power Thresholds. . . . .	68
Export Readings as CSV. . . . .	74
Peripherals. . . . .	76
Yellow- or Red-Highlighted Sensors. . . . .	80
Managed vs Unmanaged Sensors/Actuators. . . . .	81
Sensor/Actuator States. . . . .	82
Finding the Sensor's Serial Number. . . . .	84
Identifying the Sensor Position and Channel. . . . .	84
Automatic Management of Sensors. . . . .	85
Managing One Sensor or Actuator. . . . .	85
Individual Sensor/Actuator Pages. . . . .	87
Z Coordinate Format. . . . .	92
Serial Access With Dominion Serial Access Module. . . . .	93
DSAM Connection. . . . .	94
DSAM LED Operation. . . . .	94
View DSAM Serial Ports . . . . .	95
Configure DSAM Serial Ports. . . . .	95
Connect to DSAM Serial Targets in the Web Interface. . . . .	97
DSAM CLI Commands. . . . .	98
Connect to DSAM Serial Targets via SSH. . . . .	99
Asset Strips. . . . .	100
Asset Strip Automatic Firmware Upgrade. . . . .	108
External Beeper. . . . .	108
Power CIM. . . . .	109
User Management. . . . .	109
Creating Users. . . . .	109
Editing or Deleting Users. . . . .	113
Creating Roles. . . . .	114
Editing or Deleting Roles. . . . .	116
Permissions. . . . .	117
Setting Your Preferred Measurement Units. . . . .	117
Setting Default Measurement Units. . . . .	118
Device Settings. . . . .	118
Network Settings. . . . .	119
Configuring Network Services. . . . .	142
Configuring Security Settings. . . . .	151
Setting the Date and Time. . . . .	171
Door Access. . . . .	173
Event Rules and Actions. . . . .	175
Setting Data Logging. . . . .	227
Configuring Data Push Settings. . . . .	229

Monitoring Server Accessibility . . . . .	234
Front Panel Settings . . . . .	240
Configuring the Serial Port . . . . .	241
Lua Scripts . . . . .	243
Miscellaneous . . . . .	247
Using Prometheus and Grafana . . . . .	248
Requirements for Prometheus and Grafana . . . . .	248
Collected Data . . . . .	249
Maintenance . . . . .	249
Device Information . . . . .	249
Viewing Connected Users . . . . .	250
Viewing, Pausing, Resuming or Clearing the Local Event Log . . . . .	252
Updating the Firmware . . . . .	253
Viewing Firmware Update History . . . . .	255
Bulk Configuration . . . . .	255
Backup and Restore of Device Settings . . . . .	260
Network Diagnostics . . . . .	261
Downloading Diagnostic Information . . . . .	261
Hardware Issue Detection . . . . .	262
Rebooting . . . . .	263
Resetting All Settings to Factory Defaults . . . . .	264
Webcam Management . . . . .	265
Configuring Webcams and Viewing Live Images . . . . .	266
Sending Links to Snapshots or Videos . . . . .	268
Viewing, Downloading, Deleting Locally-Saved Snapshots . . . . .	269
Changing Storage Settings . . . . .	270
SmartLock . . . . .	273
Door Status and Control . . . . .	276
Card Readers . . . . .	278
<b>Using SNMP</b> . . . . .	<b>280</b>
Enabling and Configuring SNMP . . . . .	280
SNMPv3 Notifications . . . . .	280
SNMPv2c Notifications . . . . .	282
Downloading SNMP MIB . . . . .	283
SNMP Gets and Sets . . . . .	284
The MIB File . . . . .	284
SNMP Sets and Thresholds . . . . .	285
Configuring NTP Server Settings . . . . .	285
Retrieving Energy Usage . . . . .	286
<b>Using the Command Line Interface</b> . . . . .	<b>287</b>
Logging in to CLI . . . . .	287

With HyperTerminal. . . . .	287
With SSH or Telnet. . . . .	288
With an Analog Modem. . . . .	289
Different CLI Modes and Prompts. . . . .	289
Closing a Local Connection. . . . .	290
Logging out of CLI. . . . .	290
Tips for Using the CLI. . . . .	290
The ? Command for Showing Available Commands. . . . .	290
Querying Available Parameters for a Command. . . . .	291
Retrieving Previous Commands. . . . .	291
Automatically Completing a Command. . . . .	292
Multi-Command Syntax. . . . .	292
Showing Information. . . . .	294
Actuator Information. . . . .	294
Asset Strip Settings. . . . .	295
Authentication Settings. . . . .	295
Blade Slot. . . . .	297
Command History. . . . .	297
Device Configuration. . . . .	297
Date and Time Settings. . . . .	298
Default Measurement Units. . . . .	298
Event Log. . . . .	298
Environmental Sensor Information. . . . .	300
Environmental Sensor Default Thresholds. . . . .	301
Existing Roles. . . . .	302
Existing User Profiles. . . . .	302
Front Panel Permissions. . . . .	303
Network Configuration. . . . .	303
Network Connections Diagnostic Log. . . . .	307
Peripheral Devices Settings. . . . .	307
Environmental Sensor Package Information. . . . .	307
Reliability Data. . . . .	308
Reliability Error Log. . . . .	308
Rack Unit Settings of an Asset Strip. . . . .	309
Reliability Hardware Failures. . . . .	309
Security Settings. . . . .	310
Server Reachability Information. . . . .	310
Serial Port Settings. . . . .	311
Clearing Information. . . . .	311
Clearing Event Log. . . . .	311
Clearing Diagnostic Log for Network Connections. . . . .	311
Configuring the Device and Network. . . . .	312

Device Configuration Commands. . . . .	312
Network Configuration Commands. . . . .	314
Time Configuration Commands. . . . .	343
Security Configuration Commands. . . . .	347
User Configuration Commands. . . . .	365
Role Configuration Commands. . . . .	374
Authentication Commands. . . . .	378
Environmental Sensor Configuration Commands. . . . .	392
Configuring Environmental Sensors' Default Thresholds. . . . .	395
Commands for Environmental Sensors. . . . .	397
Actuator Configuration Commands. . . . .	399
Server Reachability Configuration Commands. . . . .	400
Peripheral Devices Configuration Commands. . . . .	403
Asset Management Commands. . . . .	404
Serial Port Configuration Commands. . . . .	405
Actuator Control Operations. . . . .	407
Unblocking a User. . . . .	408
Resetting the BCM2. . . . .	408
Restarting the BCM2. . . . .	408
Resetting to Factory Defaults. . . . .	409
Network Troubleshooting in Diagnostic Mode. . . . .	410
Querying DNS Servers. . . . .	410
Showing Network Connections. . . . .	411
Testing the Network Connectivity. . . . .	411
Tracing the Route. . . . .	412
Example - Ping Command. . . . .	412
<b>Appendices</b>	<b>412</b>
Equipment Setup Worksheet Sample. . . . .	413
Special Configuration and Upgrade Methods. . . . .	417
Configuration or Firmware Upgrade with a USB Drive. . . . .	417
Bulk Configuration or Firmware Upgrade via DHCP (TFTP/HTTPS). . . . .	429
Raw Configuration Upload and Download. . . . .	446
Bulk Configuration, Firmware Upgrade, or Backup/Restore via SCP. . . . .	451
Remote Authentication Examples. . . . .	461
LDAP Configuration Illustration. . . . .	461
RADIUS Configuration Illustration. . . . .	466
Cisco ISE Xerus TACACS+ Authentication. . . . .	480
Updating the LDAP Schema. . . . .	488
Returning User Group Information. . . . .	488
Setting the Registry to Permit Write Operations to the Schema. . . . .	488
Creating a New Attribute. . . . .	489

Adding Attributes to the Class. . . . .	490
Updating the Schema Cache. . . . .	492
Editing rcusergroup Attributes for User Members. . . . .	492
Additional Xerus Information - Assorted Products. . . . .	494
Reserving IP Addresses in DHCP Servers. . . . .	494
Sensor Threshold Settings. . . . .	496
Default Voltage and Current Thresholds. . . . .	503
Altitude Correction Factors. . . . .	504
Unbalanced Current Calculation. . . . .	505
Ways to Probe Existing User Profiles. . . . .	506
Role of a DNS Server. . . . .	506
Installing the USB-to-Serial Driver (Optional). . . . .	506
Device-Specific Settings. . . . .	507
TLS Certificate Chain. . . . .	508
Xerus Product Integration. . . . .	514
Connecting a PDU to a Dominion KVM or Serial Device. . . . .	514
Power IQ Configuration. . . . .	516
Connecting a Modbus RTU Device or Bus. . . . .	516
dcTrack. . . . .	517
Third Party Licenses. . . . .	519
Licenses - Angular. . . . .	519
Licenses - Bind9. . . . .	528
Licenses - Clish. . . . .	534
Licenses - Dropbear. . . . .	539
Licenses - FreeType. . . . .	541
Licenses - IW. . . . .	543
Licenses - JSON-C. . . . .	543
Licenses - LIBTIRPC. . . . .	544
Licenses - LIBXML2. . . . .	544
Licenses - Mbus. . . . .	544
Licenses - Net-SNMP. . . . .	545
Licenses - Open LDAP. . . . .	550
Licenses - OpenSSL. . . . .	552
Licenses - Wireless-RegDB. . . . .	553
Licenses - WPA Supplicant and Hostapd. . . . .	554

# Safety Information

---

---

## DANGER!

---

---

### HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

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

## NOTICE

---

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

## CAUTION

---

### RISK OF EQUIPMENT DAMAGE

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

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

Installation category: CAT II or CAT III

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

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



This symbol indicates an electrical shock hazard exists.





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

# Installation and Initial Configuration

- This equipment must only be installed and serviced by qualified electrical personnel.
- Read, understand and follow the instructions before installing this product.
- See [Safety Information](#) (on page 8).

## In This Chapter

Product Models. . . . .	10
Hardware Installation. . . . .	10
Login and Configuration. . . . .	33
Using the BCM2's Display. . . . .	38

### Product Models

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

### Hardware Installation

BCM2 supports two hardware options. Select your hardware version for installation instructions:

- [BCM2 Series Hardware Installation](#) (on page 10)
- [PM Series Hardware Installation: PMC-1000, PMC-1001, PMM-1000, PMB-1960, PMMC-1000](#) (on page 19)

## BCM2 Series Hardware Installation

### Safety Information

---

---

**DANGER!**

---

---

#### HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

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

---

**NOTICE**

---

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

---

## CAUTION

---

### RISK OF EQUIPMENT DAMAGE

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

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

Provide overcurrent protection and disconnecting device for supply conductors with approved current limiting devices suitable for protecting the wiring.

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



This symbol indicates an electrical shock hazard exists.



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

## Equipment Maintenance and Service

**WARNING!** This equipment must only be installed by qualified electrical personnel. This product contains no user serviceable parts. Do not open, alter or disassemble this product. All repairs and servicing must be performed by Raritan authorized service personnel. Failure to comply with this warning may result in electric shock, personal injury and death.

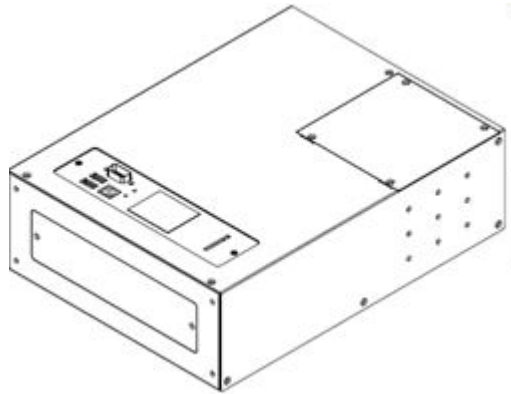
### Legrand

270 Davidson, Somerset, NJ 08873 USA

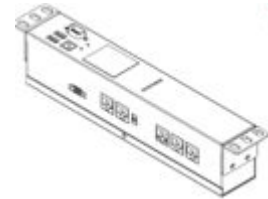
## Product Overview

Raritan's BCM2 hardware is a branch circuit monitor that supports the Xerus technology platform.

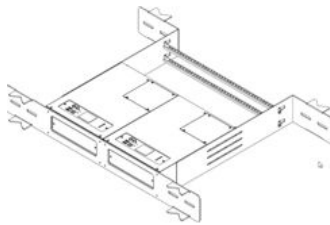
- 96 channel branch circuit monitor. *BCM2\_96xx (with built-in controller)*
- Models available with or without built-in meter controller, with power line cords or field wiring terminals.
- One meter controller (built-in or external) interconnects one to eight BCM2.
- Built-in controller is top or front mountable.
- External controller rack mounts or attaches to PDU access door.



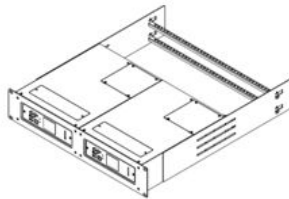
▶ *External meter controller*



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



BCM2\_FLOOR\_MOUNT\_KIT



BCM2\_RACK\_MOUNT\_KIT



BCM2\_WALL\_MOUNT\_KIT

## Product Specifications

### Voltage Measurement Inputs:

Input Range* for BCM2-9610	90-120VLN, 156-208VLL
Input Range* for BCM2-9610Y	90-277VLN, 156-480VLL
Input Range* for BCM2-9611	220-240VLN, 380-415VLL

Measurement Category CAT III, Pollution Level 2

Frequency 47-63 Hz

Input Impedance 10M $\Omega$

\*Ratings for models with field wiring terminals.  
For models with factory installed line-cords,  
rating is limited by plug and ratings are labeled  
on back on unit.

**Current Measurement Inputs:**

Input Range 0-333mV

Input Impedance 10k $\Omega$

CT Type Voltage Output = 333mV at rated  
current

CT Rated Current 1-1200A

**Meter Measurement Accuracy:**

Active Power & Energy 0.5%: IEC 62053 Class .5, EN  
50470-3 Class C

Reactive Power & Energy 2%

RMS Voltage & Current 0.2%

Frequency 0.1%

Sample Rate 64x AC frequency (phase locked)

Measurement Update Rate 3 seconds: IEC 61000-4-30 Class S

**Power Requirements:**

Voltage 90-240V

Current 0.2A

Overvoltage Category CAT III, Pollution Level 2

Frequency 50-60 Hz

**Environmental:**

Operating Temperature	0-60°C
Operating Humidity	5-85%RH
Operating Elevation	0-3000m

**Conformance:**

Safety	UL/EN 61010-1
EMC/EMI	EN61326-1, FCC Part 15 Class A

## BCM2 Rear Panel Connectors and Controls

**A** Voltage measurement input. Model dependent: line cord or conduit knockout

**B** Meter power input. Not present on line cord models.

**C** Meter Bus connectors. Daisy chains multiple meters to common controller.

**D** Meter Bus Terminator Switch. Electrically terminates meter bus.

**E** Meter ID switches. Assigns each meter a unique ID number.

**F** Eight branch circuit CT connectors (CT1 through CT8).

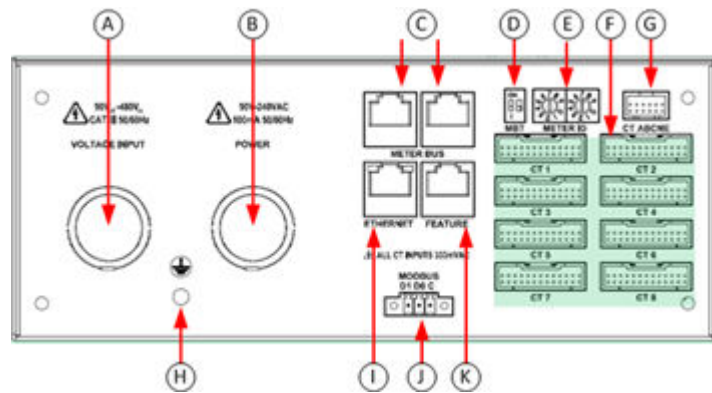
**G** Panel mains CT connector.

**H** Ground connection point (optionally grounds meter to rack).

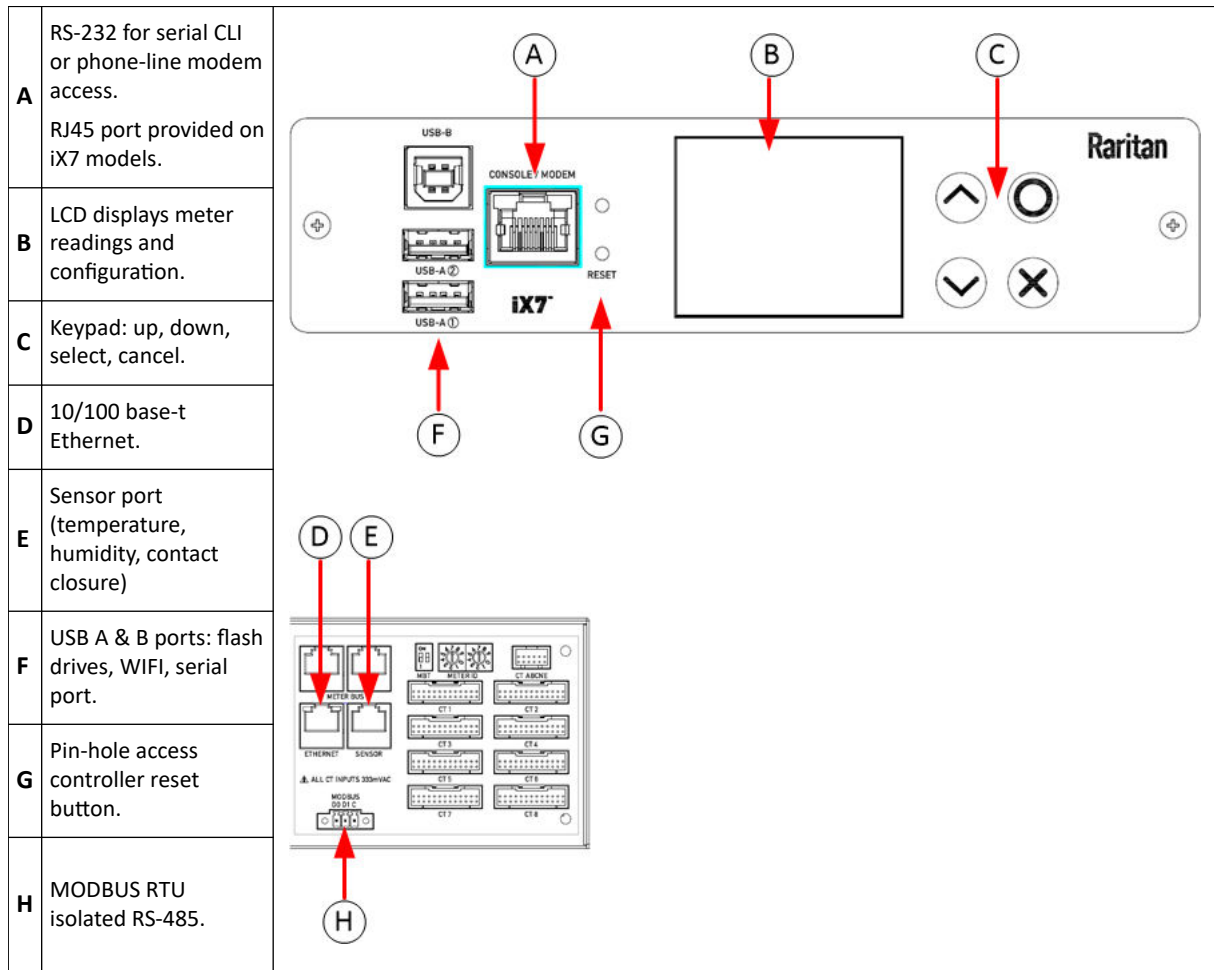
**I** 10/100 base-t Ethernet jack. (Models with built-in meter controller.)

**J** MODBUS RTU isolated RS485. (Models with built-in meter controller.)

**K** Sensor port. (Models with built-in meter controller.)



## Meter Controller Connectors and Controls



## Voltage Measurement and Power Wiring

BCM2-96xx series products are available with factory installed line cords (PLUGGABLE EQUIPMENT) or conduit knockouts and field wiring terminals (PERMANENTLY CONNECTED EQUIPMENT).

This section describes how to wire models with conduit knockouts and field wiring terminals. Models with factory installed line cords are not end user wired and must not be opened or modified.

There are two conduit knockouts on the rear panel – one for voltage inputs (voltages that are measured), the other for power (power to run the product). In most cases, only voltage inputs are wired because power can be derived from the voltage inputs (see jumpers in figure).

Product power is taken from the voltage inputs using two jumpers. A separate circuit can be used for power which insures BCM2 continues to operate when voltages inputs fail. A separate power circuit MUST be used if the voltage inputs exceed power rating (90-240VAC). When using a separate circuit, remove factory jumpers and wire circuit to the power L1 and L2 terminals.

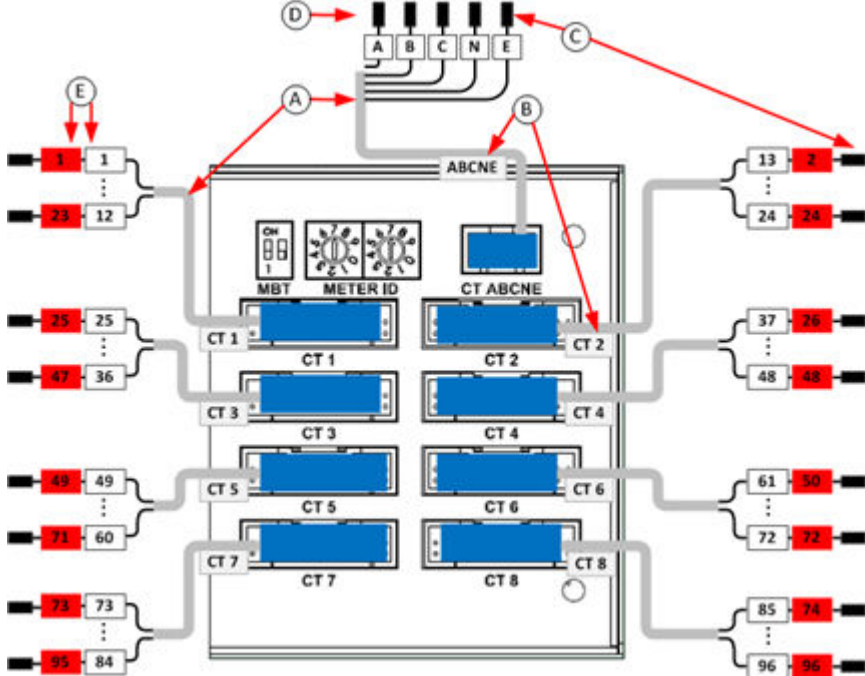

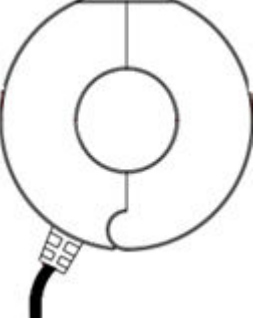
<p><b>A</b> Terminals accept 14-18 AWG solid or stranded wire. Use ring terminals on stranded wire. Use wire rated 75°C or higher.</p>	
<p><b>B</b> Jumpers power unit from voltage inputs. Move or remove as necessary.</p>	
<p><b>C</b> Connect ground wires to stud.</p>	
<p><b>D</b> Verify circuit voltages match product ratings.</p>	
<p><b>E</b> ½ and ¾ conduit fitting knockouts</p>	

Panel Voltage	Voltage Inputs				Power		CT ABCNE					
	A	B	C	N	L1	L2	A	B	C	N	E	
1-phase 120V, 230V	X			X	A	N	X				O	O
1-phase 208V	X	X		O	A	B	X				O	O
Split-phase 120/240	X	X		X	A	B	X	X			O	O
3-phase 4-wire	X	X	X		A	B	X	X	X		O	O
3-phase 5-wire	X	X	X	X	A	N	X	X	X		O	O

Note: X: Selection, Blank: Non-selection, O: Option

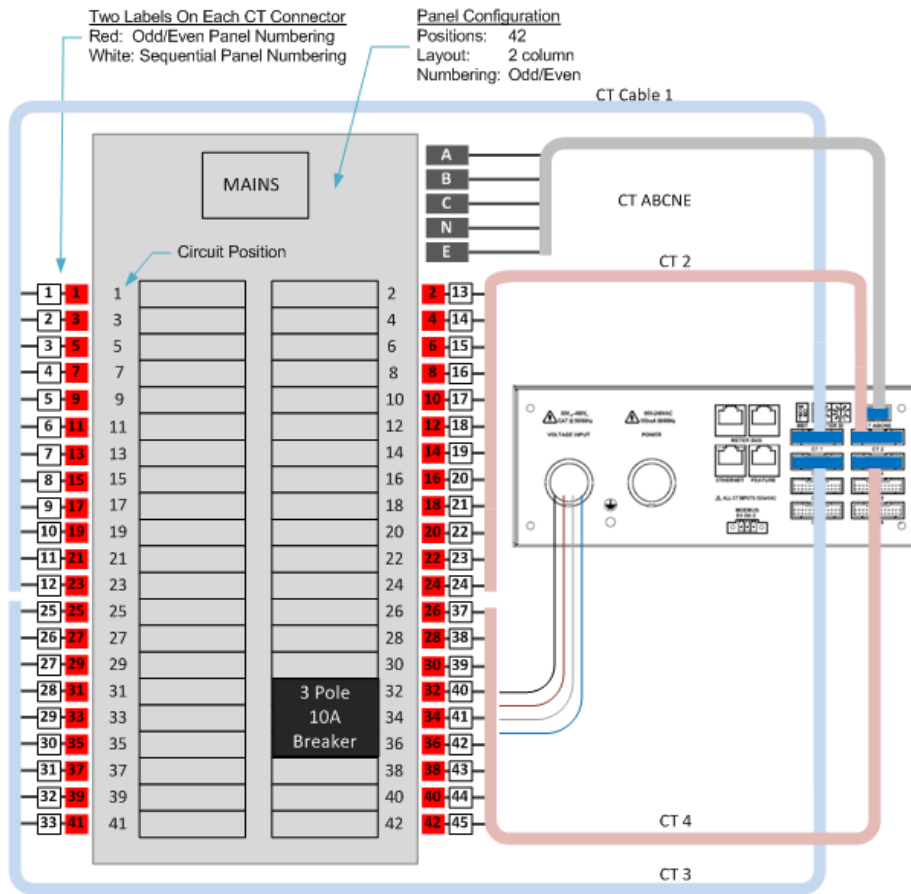


## Current Transformer (CT) Wiring

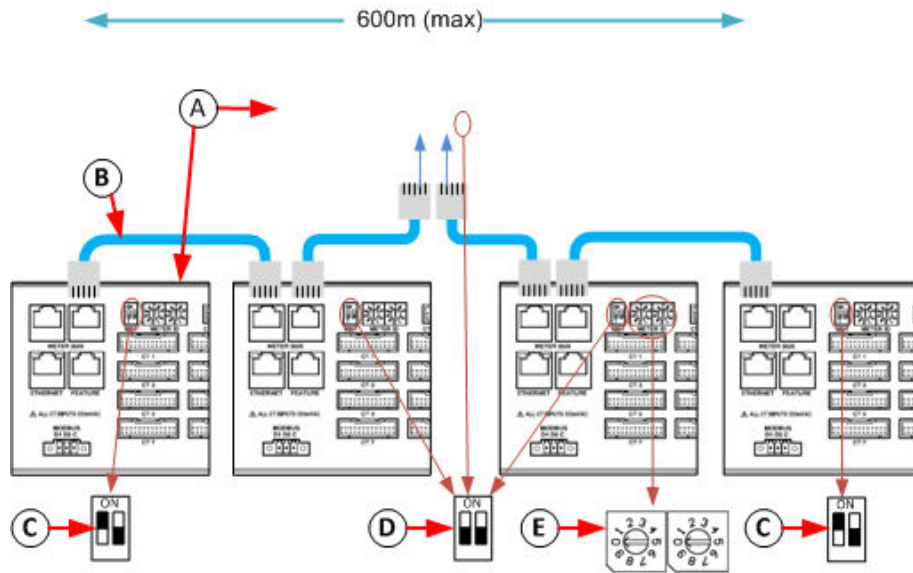
<b>A</b>	Multi-conductor CT cable. Available lengths: 3m, 10m.	
<b>B</b>	Connect labeled end into matching labeled rear panel connector	
<b>C</b>	CT plugs into 2-pin locking connector (Molex 43640-0201)	
<b>D</b>	Main Circuit: 3 phase lines (A,B,C), Neutral (N), Earth (E).	
<b>E</b>	Branch Circuits have two labels: Red labels for odd/even numbered panels. White labels for sequentially numbered panels.	
 <ul style="list-style-type: none"> <li>• All CTs 333mV output. DO NOT use current output CT.</li> <li>• CT can be connected to live circuit in either direction. Meter auto corrects polarity.</li> <li>• CT must be completely closed and tab locked to ensure proper energy metering.</li> </ul> 		

Branch Circuit	Description	Current Transformers	
		How Many	Connect To
Line-Neutral (LN)	120V/230V circuit wired to 1-pole circuit breaker	1	phase line
Line-Line (LL)	208/240/400V circuit wired to 2-pole circuit breaker	1	either phase line
Line-Line-Neutral (LLN)	120V+208/240V circuit wired to 2-pole circuit breaker	2	each phase line
Three-Phase (LLL, LLLN)	3-phase circuit wired to 3-pole circuit breaker	3	each phase line

# Panel Wiring Example



## Controller Wiring to Meters



<b>A</b>	Daisy chain:
	<ul style="list-style-type: none"> <li>• Meter with built-in controller + 1 to 7 controller-less meters</li> <li>or</li> <li>• external controller + 1 to 8 controller-less meters.</li> </ul>
	<b>B</b> All cables shielded Cat-5, each cable: 100m max. length.
	<b>C</b> Switch MBT (terminator) ON for devices at ends of daisy chain.
	<b>D</b> Switch MBT OFF for devices in middle of daisy chain.
<b>E</b> Assign each meter unique ID: valid values 01 through 08	

## PM Series Hardware Installation: PMC-1000, PMC-1001, PMM-1000, PMB-1960, PMMC-1000

### Safety Information

---



---

DANGER!

---



---

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

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

---

**NOTICE**

---

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

---

**CAUTION**

---

**RISK OF EQUIPMENT DAMAGE**

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

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

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

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



This symbol indicates an electrical shock hazard exists.



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

## Equipment Maintenance and Service

WARNING! This equipment must only be installed by qualified electrical personnel. This product contains no user serviceable parts. Do not open, alter or disassemble this product. All repairs and servicing must be performed by Raritan authorized service personnel. Failure to comply with this warning may result in electric shock, personal injury and death.

### Legrand

270 Davidson, Somerset, NJ 08873 USA

## Product Overview - PM Series Power Meters

Raritan PM series power meters is a modular power metering solution that is a flexible alternative to the all-in-one BCM2 hardware. All solutions support Xerus technology platform.

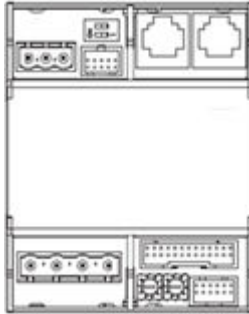
The PM series includes controllers, power meters, and branch circuit monitor modules.

In each configuration, you must have exactly one controller component. In the PM series, there are 2 controller options:

1. PMC is a controller-only module.
2. PMMC is a controller with 1 built-in power meter.

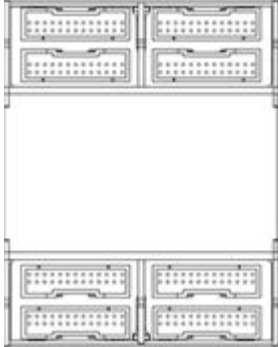
**PMM:** a 3-phase power meter with neutral and earth current monitoring.

**PMM**



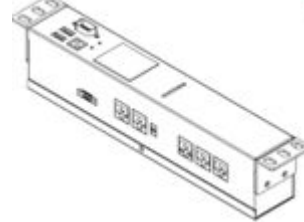
**PMB:** a 96 channel branch circuit monitor that plugs into PMM. A PMM+PMB monitors a panel board mains and branch circuit.

**PMB**



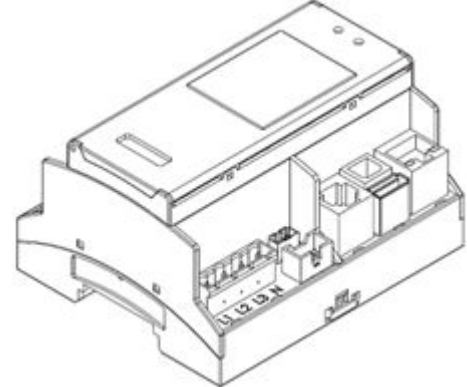
**PMC:** power meter controller. One PMC controls up to 70 PMM or 8 PMM+PMB.

**PMC**



Interconnection uses standard shielded CAT-5 cable. All modules receive redundant power and continue to function as long as one or more PMM remain powered.

**PMMC**



**PMMC:** PMM with a built-in power meter controller. Control up to 69 additional PMM or 8 PMM + PMB.

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

CTs are available in various ratings and contain built-in burden resistors so they can be snapped onto live wires without damage.

CT orientation is not critical because meter auto-corrects polarity for any CT installed backwards.

CT connections are made close to branch circuits using multi-conductor wiring harnesses with individual CT wire-pairs labeled and terminated with a keyed connector.

## Product Specification

### Voltage Measurement Inputs:

Input Range*	90-277VLN, 156-480VLL
Measurement Category	CAT III, Pollution Level 2
Frequency	47-63 Hz
Input Impedance	10M $\Omega$

\*Ratings for models with field wiring terminals. For models with factory installed line-cords, rating is limited by plug and ratings are labeled on back on unit.

### Current Measurement Inputs:

Input Range	0-333mV
Input Impedance	10k $\Omega$
CT Type	Voltage Output = 333mV at rated current
CT Rated Current	1-1200A

### Meter Measurement Accuracy:

Active Power & Energy	0.5%: IEC 62053 Class .5, EN 50470-3 Class C
Reactive Power & Energy	2%
RMS Voltage & Current	0.2%
Frequency	0.1%
Sample Rate	64x AC frequency (phase locked)
Measurement Update Rate	3 seconds: IEC 61000-4-30 Class S

### Power Requirements:

Voltage	90-240V
Current	0.2A
Overvoltage Category	CAT III, Pollution Level 2

Frequency 50-60 Hz

**Mechanical:**

Terminal Block Screw Torque 0.37 ft-lb (0.5Nm) to 0.44 ft-lb (0.6Nm)

Terminal Block Wire Size 14-24AWG (.5-1.6mm)

Terminal Wire Temperature Rating > 75 degree C

DIN Rail T35 (35mm)

**Environmental:**

Operating Temperature 0-60°C

Operating Humidity 5-85%RH

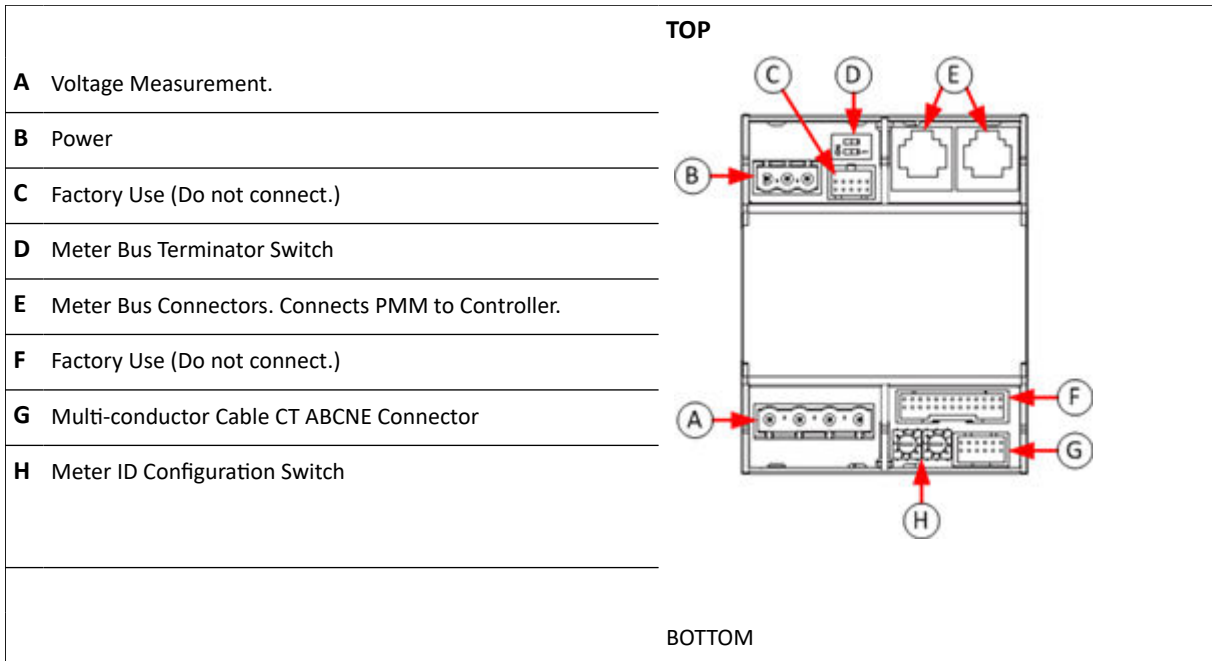
Operating Elevation 0-3000m

**Conformance:**

Safety UL/EN 61010-1

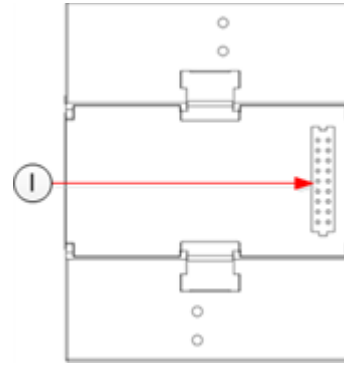
EMC/EMI EN61326-1, FCC Part 15 Class A

### Power Meter (PMM) Connectors and Controls





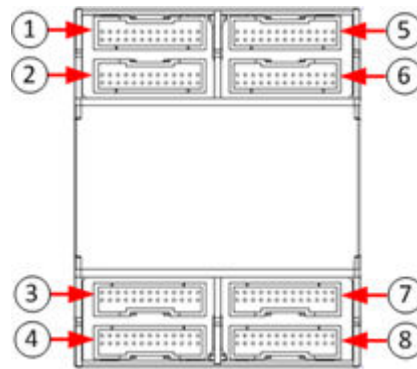
**I** Expansion Port. Connects PMM to PMB



## Power Meter Branch Monitor (PMB) Connectors

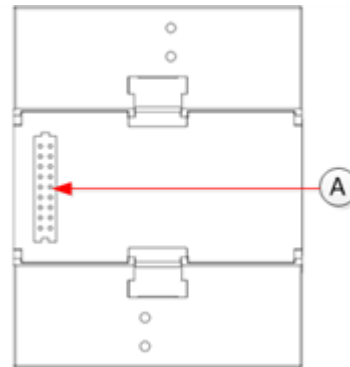
- 1** Multi-conductor cable CT 1 connector.
- 2** Multi-conductor cable CT 2 connector.
- 3** Multi-conductor cable CT 3 connector.
- 4** Multi-conductor cable CT 4 connector.
- 5** Multi-conductor cable CT 5 connector.
- 6** Multi-conductor cable CT 6 connector.
- 7** Multi-conductor cable CT 7 connector.
- 8** Multi-conductor cable CT 8 connector.

**TOP**



**A** Expansion port. Connects PMB to PMM or PMMC.

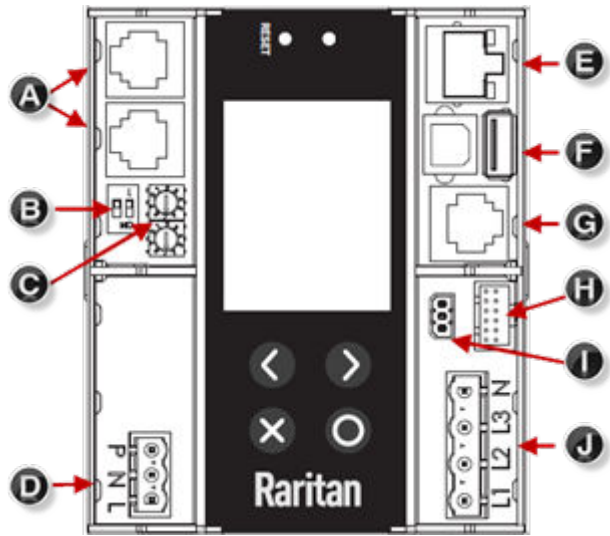
**BOTTOM**



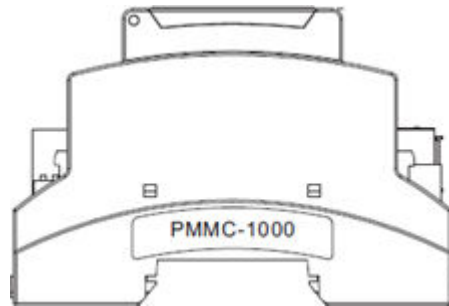
## Power Meter with Controller (PMMC)

**TOP**

- A** Meter Bus Connectors
  - B** Meter Bus Terminator Switch
  - C** Meter ID Configuration Switch
  - D** Power
  - E** Ethernet
  - F** USB-A and USB-B
  - G** Sensor Port
  - H** Multi-conductor Cable CT ABCNE Connector
  - I** Modbus
  - J** Voltage Measurement
- Expansion Port is on bottom side of unit. Connects PMMC to PMB.

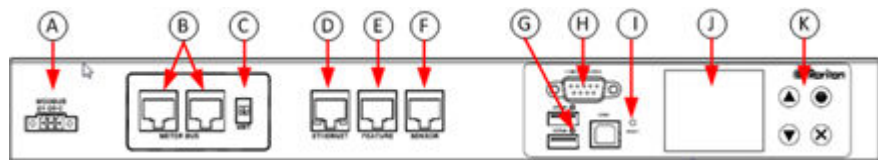


**END**



## Power Meter Controller (PMC) iX6/iX7

- A** MODBUS RTU isolated RS-485
- B** Meter bus connector (to PMM)
- C** Meter bus terminator switch
- D** 10/100 base-t Ethernet.
- E** Feature port (Raritan asset strip)
- F** Sensor port (temperature, humidity, etc.)
- G** USB A & B (flash drives, WIFI, serial port)
- H** RS-232 (terminal CLI, modem)
- I** Pin-hole access reset button
- J** LCD (meter readings, settings, configuration)
- K** Keypad



---

Note: iX7 PMC and BCM2 devices have RJ45 console connectors. iX6 has a DE-9 console connector.

---

## DIN Rail Mounting PMM + PMB

**BOTTOM**

**A**

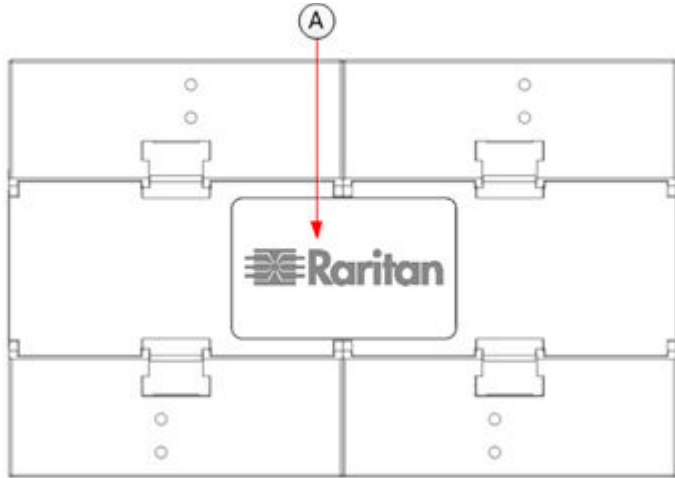


Expansion Connector supplied with PMB.

Do not hot-plug the Expansion Port! PMM and PMB must be disconnected from all power source before plugging Expansion Port.

Snap Expansion Connector to Expansion Ports on bottoms of PMM and PMB or PMMC and PMB.

\*Example shows PMC model.



**TOP**

**B**

35mm DIN rail

**C**

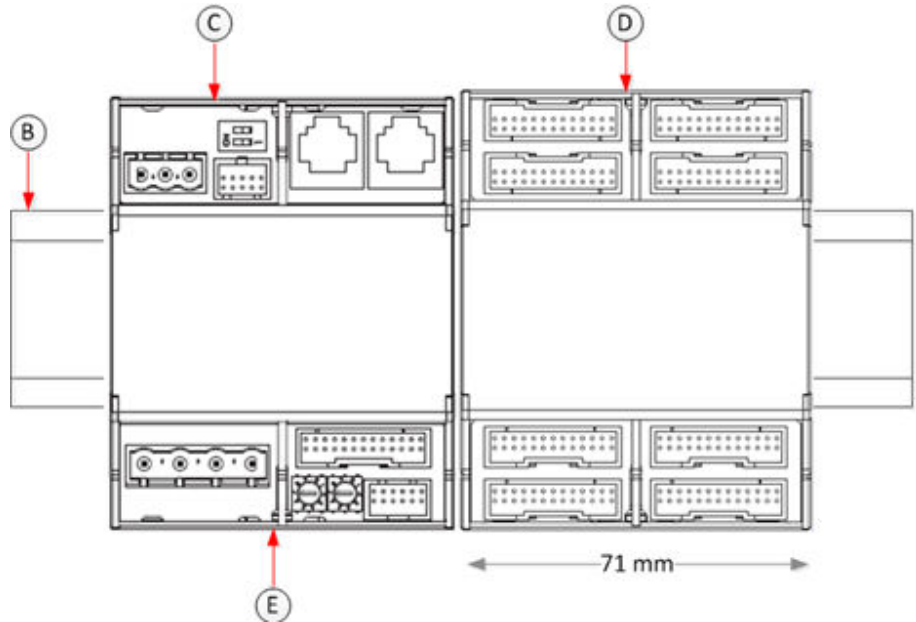
PMM

**D**

PMB

**E**

Modules snap into rail. Pull white tab here to remove.

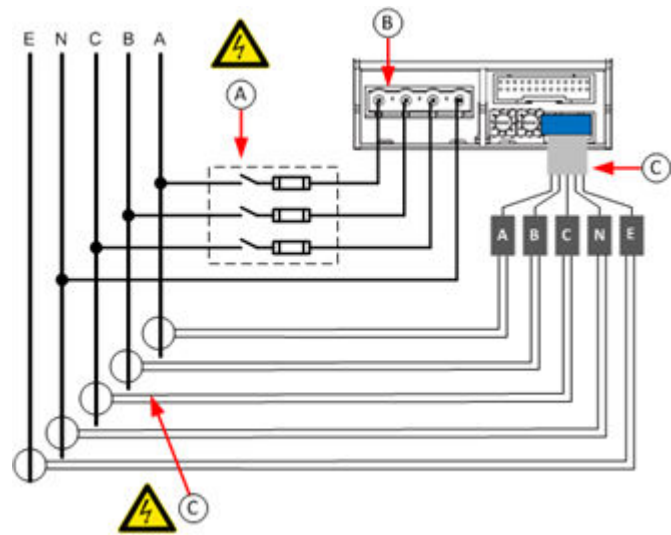


## Voltage and Current Measurement Wiring

**A** Protect phase lines with fused disconnects rated for available short circuit current at connection point.

**B** All wiring: 14-22 AWG, 75°C, solid or stranded. Do not solder tin wire ends.

**C** All CT: 333mV output at rated current. Do not use current output CT. CTs can be connected to live circuits. Connect CT in either direction.

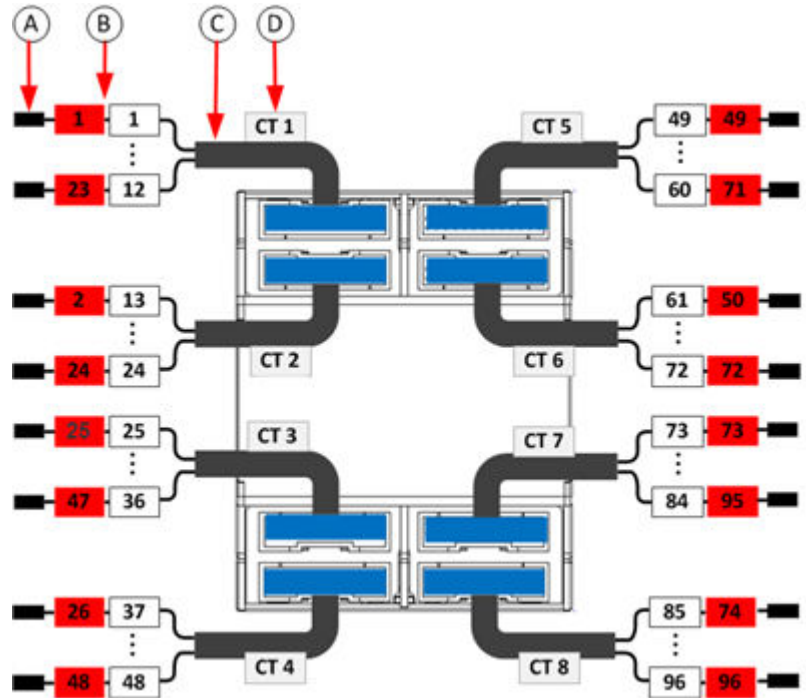
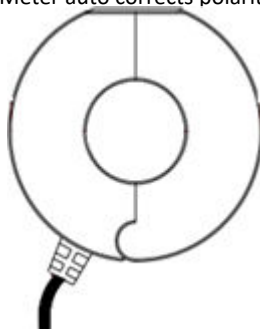


Circuit Type	Circuit Description	Wiring Connections						
		Voltage				CT		
		A	B	C	N	A	B	C
Single-Phase	L-N (120V,230V,240V)	X			X	X		
	L-L (208V, 400V)	X	X			X		
Split-Phase	North American 120/240V Panel, 2L+N circuit	X	X		X	X	X	
Three-Phase	3L, 3-phase without neutral	X	X	X		X	X	X
	3L+N, 3-phase with neutral	X	X	X	X	X	X	X

Note: X: Selection, Blank: Non-selection

## PMB Branch Circuit Wiring

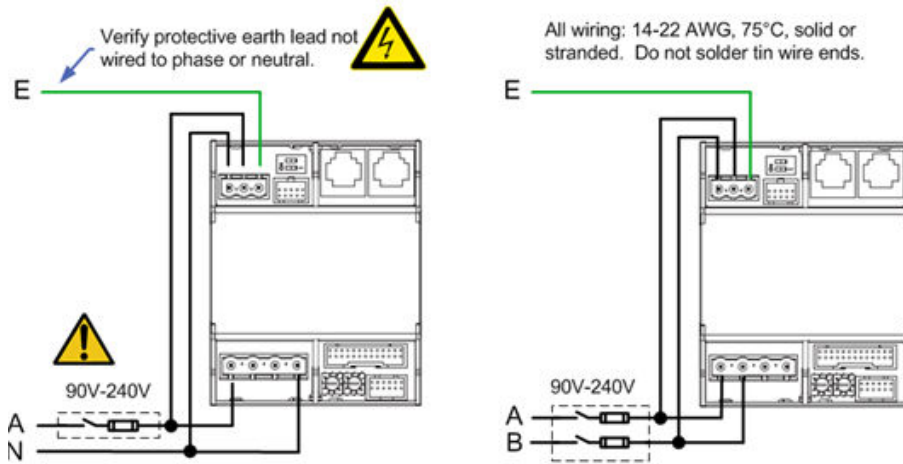
- A** CT plugs into 2-pin locking connector (Molex 43640-0201)
- B** Branch Circuits have two labels: Red labels for odd/even numbered panels. White labels for sequentially numbered panels.
- C** Multi-conductor CT cable. Available lengths: 3m, 10m.
- D** Connect labeled end into matching labeled connector
- All CTs 333mV output. DO NOT use current output CT. CT can be connected to live circuit in either direction. Meter auto corrects polarity.



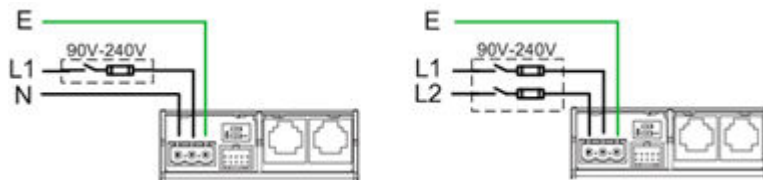
Branch Circuit	Description	Current Transformers	
		How Many	Connect To
Line-Neutral (LN)	120V/230V circuit wired to 1-pole circuit breaker	1	phase line
Line-Line (LL)	208/240/400V circuit wired to 2-pole circuit breaker	1	either phase line
Line-Line-Neutral (LLN)	120V+208/240V circuit wired to 2-pole circuit breaker	2	each phase line
Three-Phase (LLL, LLLN)	3-phase circuit wired to 3-pole circuit breaker	3	each phase line

## PMM Power Wiring

PMM can be powered from the voltage measurement inputs or from an auxiliary AC power source. Powering from the voltage measurement inputs minimizes circuitry, but the meter may stop functioning if the voltage turns off.

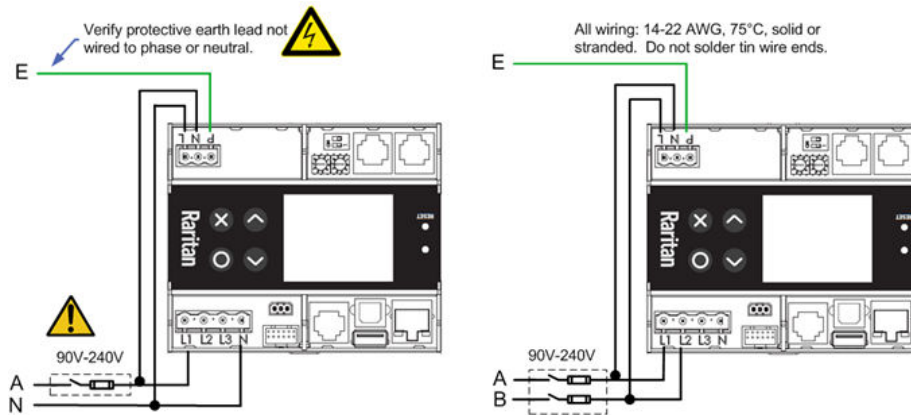


Powering from an auxiliary single phase circuit is required when the voltage measurement circuit exceeds 240V, or when continued operation is required if the voltage measurement inputs turn off.

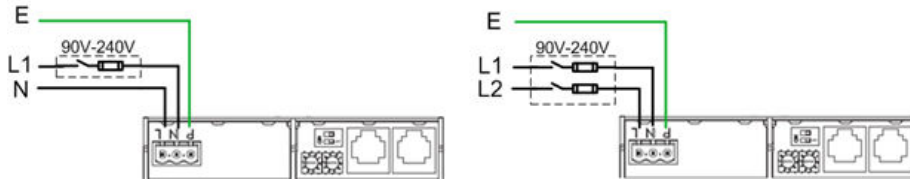


### PMMC Power Wiring

PMMC can be powered from the voltage measurement inputs or from an auxiliary AC power source. Powering from the voltage measurement inputs minimizes circuitry, but the meter may stop functioning if the voltage turns off.



Powering from an auxiliary single phase circuit is required when the voltage measurement circuit exceeds 240V, or when continued operation is required if the voltage measurement inputs turn off.



## Controller Wiring to Meters

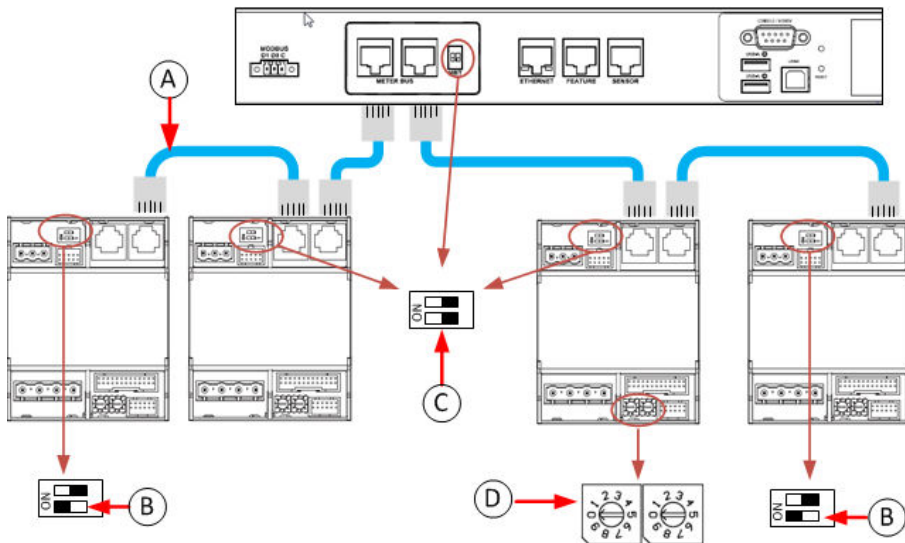
The PMC controller supports up to 70 power meters (PMM) OR eight branch circuit meters (PMM+PMB) using daisy-chain wiring with shielded cat 5 Ethernet cable. The wiring order of the modules and controller is not important.

The PMMC controller supports 69 additional power meters (PMM), OR 7 additional branch circuit meters (PMM+PMB).

---

Note: Diagram shows PMC model. Wiring is the same for PMMC model, except that the first PMM is built into the PMMC.

---



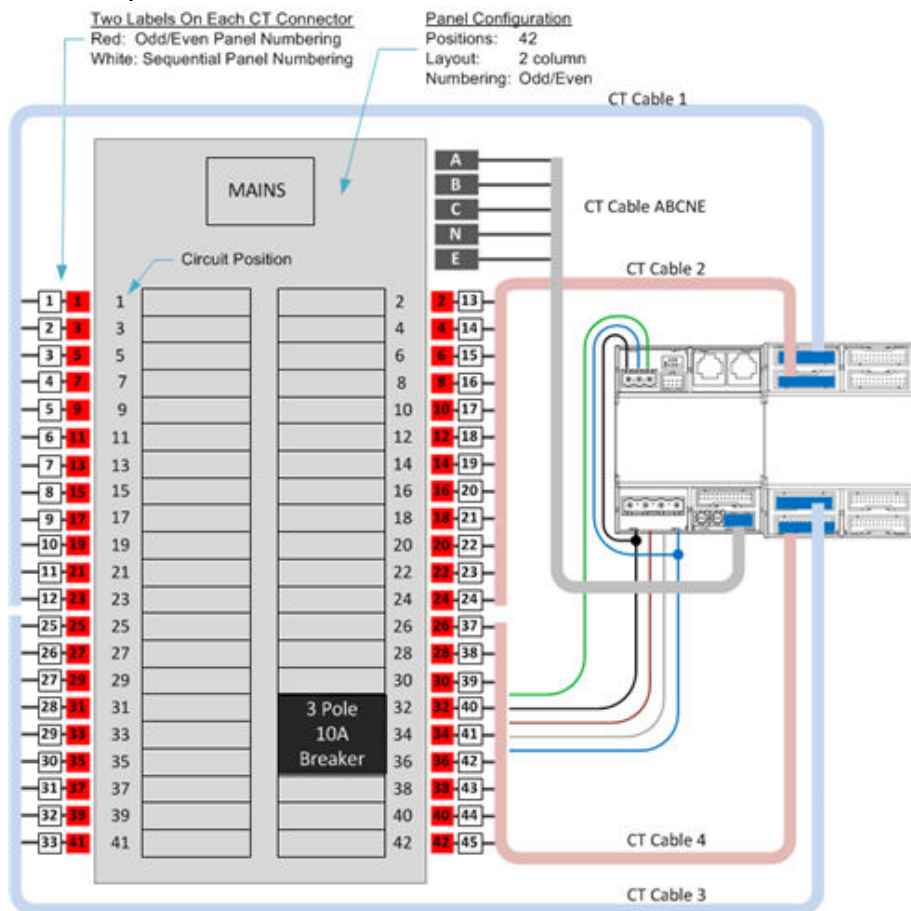
- A** All cables shielded Cat-5, each cable:100m max. length.
- B** Switch MBT (terminator) ON for devices at ends of daisy chain.
- C** Switch MBT OFF for devices in middle of daisy chain.

Assign each meter unique ID:

- D**
  - 01-70: PMM without PMB
  - 01-08: PMM with PMB



## Panel Layout



## Login and Configuration

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

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

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

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

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

## Configuring Power Meters and Branch Circuit Monitors

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

► *To configure with a spreadsheet:*

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

► *To configure with the product web interface:*

Make a network connection to the product. See [Login and Configuration](#) (on page 33). Follow the instructions in this guide, starting with: [Scan Power Meters](#) (on page 34).

### Scan Power Meters

1 Click Power Meters.

2 If nothing is configured, scan begins immediately in the Unconfigured Meters section. Click Rescan to refresh the list.

3 Click the power meter or panel in the discovered list to configure it.

Types:

PM: 3-phase

Panel: BCM

ID ▲	Type	Name	Rating	Circuits	A Current	B Current	C Current
1	Panel	Panel Mains 1	250 A	3	0.00 A	0.00 A	0.00 A
9	PM	PMM-1	200 A		0.00 A	0.00 A	0.00 A

ID ▲	Type	BCM Channels
2	Panel	96
3	Panel	96
4	Panel	96
5	Panel	96
6	Panel	96
7	Panel	96
8	Panel	96
10	PM	0
11	PM	0

## Configure Power Meter

1 Enter a name.

Select the circuit type:

- 2
- Single Phase
  - Split Phase
  - 3-phase

3 Enter the mains circuit breaker rating.

Select the checkbox for each CT installed.

4 Enter the CT rating. Ratings are marked on the CT.

5 Click OK.

The configured power meter displays in the dashboard and Power Meters page.

Power Meter 9 (PMM-1)

**Settings**

Name **1** PMM-1

Type **2** 3-Phase

**Modbus**

Enable Modbus Access

Modbus Address

**Main Circuit**

Circuit Rating **3** 200 A

Phase CT  60 A

Neutral CT **4**  200 A

Earth CT  200 A

**5**

## Configure Panel Mains Circuit

1 Enter a name.

Select the circuit type:

- 2
- Single Phase
  - Split Phase
  - 3-phase

Enter the number of circuit positions in the panel.

3 Select the panel layout: one or two columns.

Select the circuit position numbering style: sequential or odd/even.

4 Enter the current rating (circuit breaker rating) of the circuit.

Select the checkbox for each CT installed.

5 Enter the CT rating. Ratings are marked on the CT.

6 Click OK.

## Configure Panel Branch Circuits

In the Power

1 Meters page, click the panel.

The Panel details page opens.

ID ▲	Type	Name	Rating
1	Panel	Panel Mains 1	250 A
9	PM	PMM-1	200 A

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

Panel Branch Circuits										
Pos	Phase	Name	Rating	CT #	V	A	φ	Pos	Phase	Na
1	A							2	A	
3	B							4	B	
5	C							6	C	
7	A							8	A	

- Click Create Circuit.  
**3** The Create Circuit dialog opens.

- 4** Enter a name for the circuit.

- 5** Select the circuit type: One-Phase LN, One-Phase LL, One-Phase LLN, or Three-Phase. Circuit type cannot be changed later.

- 6** Enter the current rating of the circuit in Amps.

- 7** Enter the rating of the CT connected at this circuit position in Amps.

### Create Circuit at Position

Name  **4**

Circuit Type  **5**

Circuit Rating  A **6**

CT Rating  A **7**

Name	Phase	CT # (red label)
1	A <b>8</b>	1 <b>8</b>

**9**

- 8** Click the Phase or CT# to edit the automatic labels.

- 9** Click Create.

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

Panel Branch Circuits						
Pos	Phase	Name	Rating	CT #	V	
1	A	Rack 1	20 A	1	0.0 V	]
3	B			3		
5	C			5		
7	A	Rack 3	20 A	7	0.0 V	]
9	B			9		
11	C			11		

### Using the BCM2's Display

#### Automatic Mode:

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



#### Manual Mode:

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

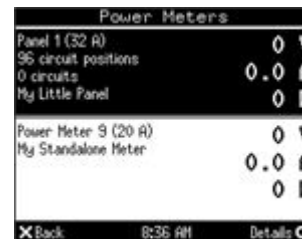
To view the Main Menu, press or .

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

Press or to choose a menu item. Press to select.



#### Power Meters list



## Power Meter details

Power Meter 9		1/5
<b>Name:</b>	My Standalone Meter	
<b>Rating:</b>	20 A	
<b>Phase CT:</b>	60 A	
<b>Neutral CT:</b>	not present	
<b>Earth CT:</b>	not present	
<b>Back</b>		6:37 AM

## Automatic and Manual Modes



After powering on or resetting, the front panel display first shows some dots, then logo and finally enters the automatic mode.

### ► *Automatic mode without alerts available:*

In this mode, the display cycles through information as long as there are no alerts.

### ► *Manual mode:*


To view more information or control outlets, enter manual mode.

Press  or  to enter the manual mode, where the Main Menu is first displayed.

To return to the automatic mode, press  until you return to the main display.

### ► *Alerts:*





- In the automatic mode, when an alert occurs, the display stops cycling through information, and warns you by showing the alerts notice in a yellow or red background.

To enter the manual mode, press .

- In the manual mode, both the top and bottom bars will turn yellow or red to indicate the presence of any alert.

## Control Buttons

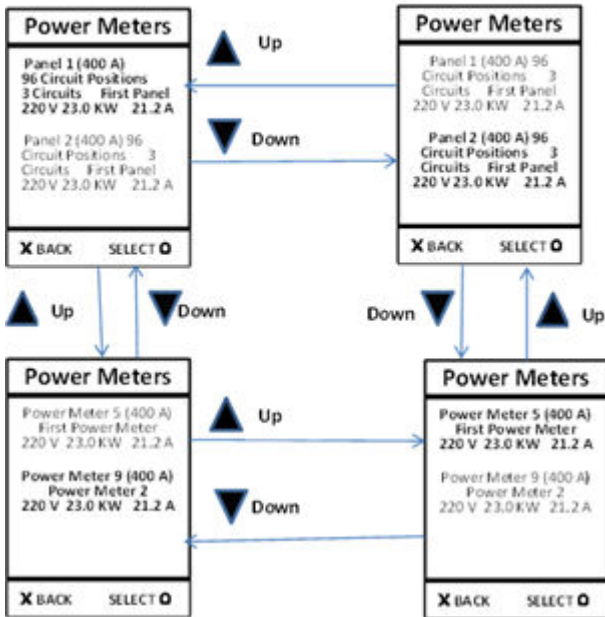
Use the control buttons to navigate to the menu in the manual mode.

Button	Function
	Up
	Down
	OK
	Back -- OR -- Switch between automatic and manual modes

## Power Meters

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

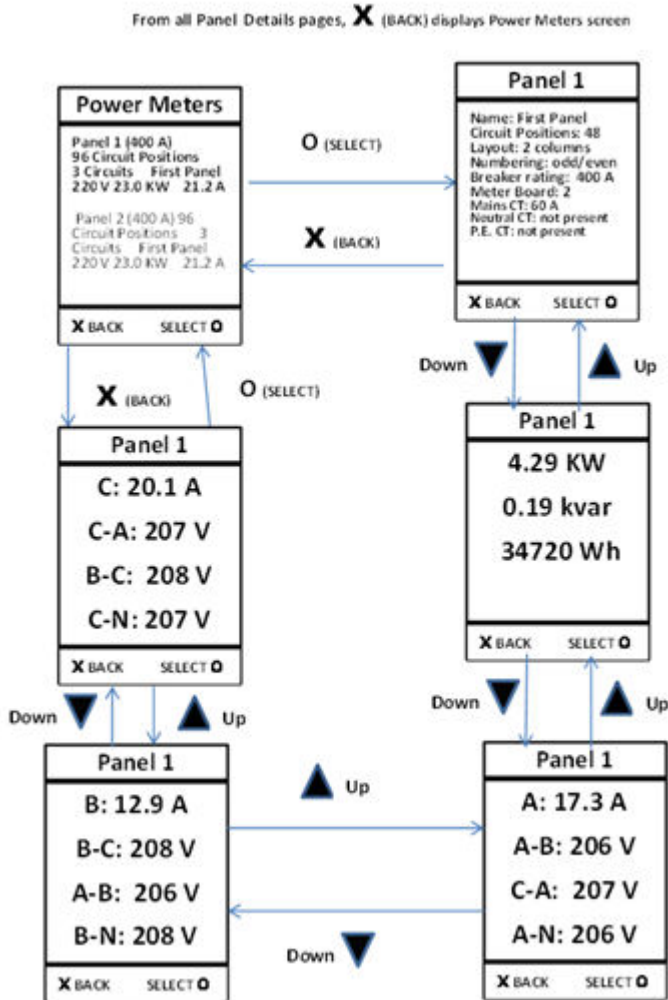
From all Power Meters pages, **X** (BACK) displays the Main Menu





## Panels

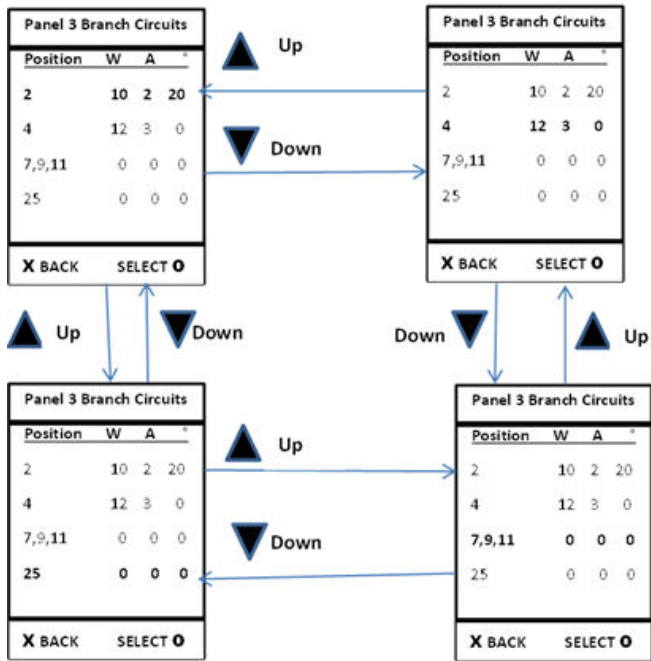
Navigate to a panel from the power meter details and press O (select) to display the panel details and readings.



## Branch Circuits

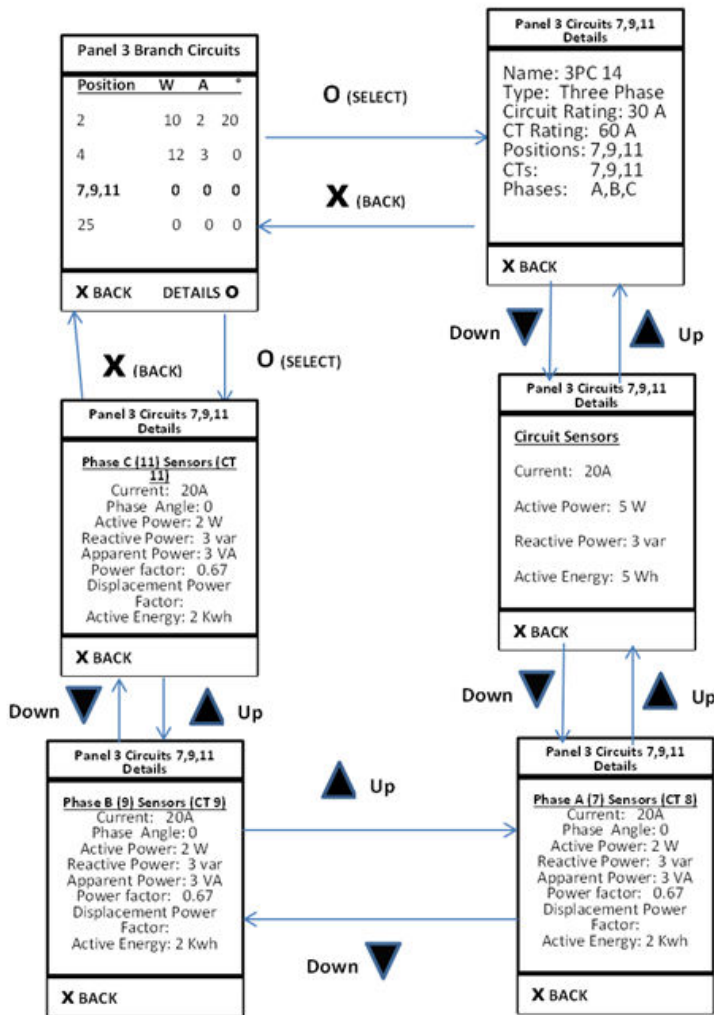
Navigate to a branch circuit from the panel details and press O (select) to display the branch circuit details and readings.

From all Branch Circuits pages, **X** (BACK) displays the Panel Details page



## Branch Circuit Details

From all Branch Details pages, **X** (BACK) displays Panel Branch Circuits screen




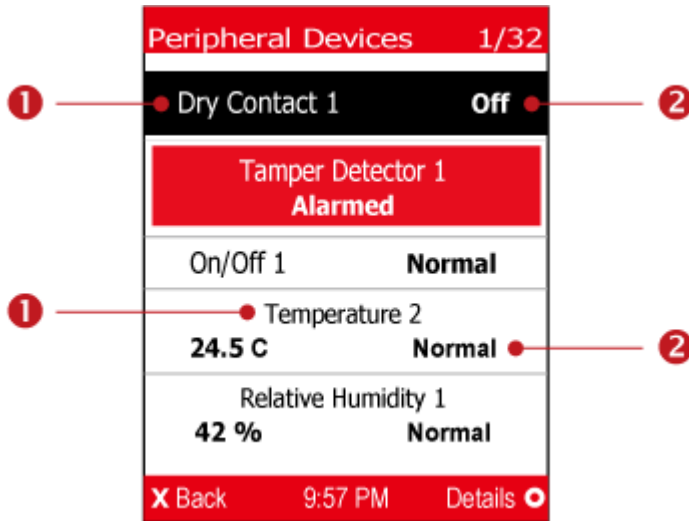
## Peripherals

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

► To show environmental sensor or actuator information:




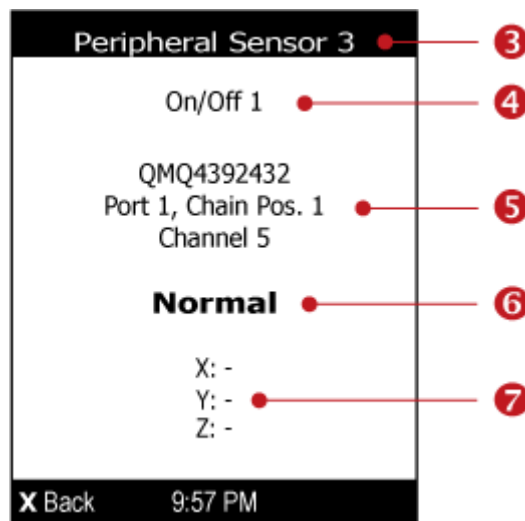
1. Select "Peripherals" in the Main Menu, and press .
  2. The display shows a list of environmental sensors/actuators.
    - When the list exceeds one page, the currently-selected sensor/actuator's ID number and total of managed sensors/actuators are indicated in the top-right corner of the display.
    - If any sensor enters warning, critical, or alarmed state, like 'Tamper Detector 1' shown below, it is highlighted in yellow or red.
- The top and bottom bars also turn yellow or red.



Number	Description
1	Sensor or actuator names.

Number	Description
2	<p>Sensor or actuator states:</p> <ul style="list-style-type: none"> <li>• <i>n/a</i> = unavailable</li> <li>• <i>Normal</i></li> <li>• <i>Alarmed</i></li> <li>• <i>Lower Critical</i> = below lower critical</li> <li>• <i>Lower Warning</i> = below lower warning</li> <li>• <i>Upper Warning</i> = above upper warning</li> <li>• <i>Upper Critical</i> = above upper critical</li> <li>• <i>On</i></li> <li>• <i>Off</i></li> <li>• <i>Open</i></li> <li>• <i>Closed</i></li> </ul> <p>A numeric sensor shows both the reading and state. A state sensor or actuator shows the state only.</p>

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




Number	Description
3	<p>The ID number assigned to this sensor or actuator.</p> <ul style="list-style-type: none"> <li>• A sensor shows "Peripheral Sensor x" (x is the ID number)</li> <li>• An actuator shows "Peripheral Actuator x"</li> </ul>
4	<p>Sensor or actuator name.</p>

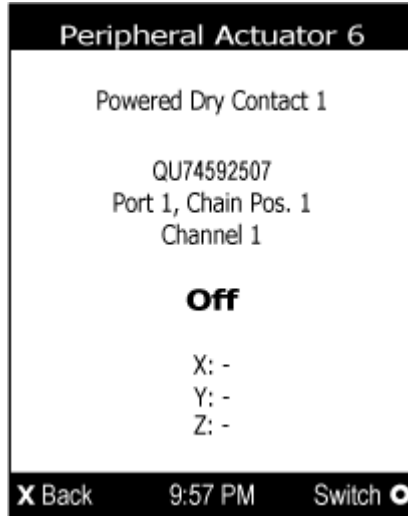
Number	Description
1. <b>5</b>	<p>The following information is listed.</p> <ul style="list-style-type: none"> <li>• Serial number</li> <li>• Chain position, which involves the following information: <ul style="list-style-type: none"> <li>• <i>Port &lt;N&gt;</i>: &lt;N&gt; is the number of the sensor port where this sensor or actuator is connected.</li> <li>• <i>Chain Pos. &lt;n&gt;</i>: &lt;n&gt; is the sensor or actuator's position in a sensor daisy chain.</li> </ul> </li> <li>• If this sensor or actuator is on a sensor package with multiple channels, its channel number is indicated.</li> </ul>
<b>6</b>	<p>Depending on the sensor type, any of the following information is displayed:</p> <ul style="list-style-type: none"> <li>• State of a state sensor: <i>Normal, Alarmed, Open or Closed</i>.</li> <li>• State of an actuator: <i>On or Off</i>.</li> <li>• Reading of a numeric sensor.</li> </ul>
<b>7</b>	X, Y, and Z coordinates which you specify for this sensor or actuator.


► *To switch on or off an actuator:*

By default peripheral actuator control is disabled. You have to enable it in the web interface. See: [Peripherals](#) (on page 76)


1. Select "Peripherals" in the Main Menu, and press  . Select an actuator to switch and press





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



3. Use the arrow buttons to select Yes or No, and then press .
4. Verify that the actuator status shown has been changed.

# Using the Web Interface

This chapter explains how to use the product web interface for administration.

## In This Chapter

Supported Web Browsers and Mobile Devices. . . . .	48
Login, Logout and Password Change. . . . .	48
Introduction to the Web Interface. . . . .	50
Viewing the Dashboard. . . . .	54
PMC Power Metering Controller. . . . .	59
Power Meters. . . . .	61
Peripherals. . . . .	76
Serial Access With Dominion Serial Access Module. . . . .	93
Asset Strips. . . . .	100
External Beeper. . . . .	108
Power CIM. . . . .	109
User Management. . . . .	109
Device Settings. . . . .	118
Using Prometheus and Grafana. . . . .	248
Maintenance. . . . .	249
Webcam Management. . . . .	265
SmartLock. . . . .	273
Card Readers. . . . .	278

### Supported Web Browsers and Mobile Devices

- Firefox® 100 and later
- Safari® (Mac)
- Google® Chrome® 100 and later
- Android 8.1 and later
- iOS 12.5 and later
- Edge (Windows 10, 11 (chrome-based versions))

### Login, Logout and Password Change

The first time you log in, use the factory default user credentials. For details, refer to the Quick Setup Guide accompanying the product. Password change is forced upon first login.

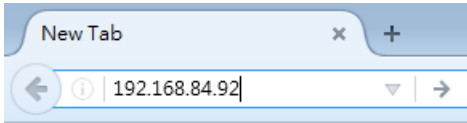
### Login and Logout

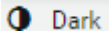
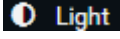
You must enable JavaScript in the web browser for proper operation.



► *To log in to the web interface:*

1. In a supported browser go to the IP address of your BCM2
  - If the link-local addressing has been enabled, you can type *pdu.local* instead of an IP address.



2. If any security alert message appears, accept it.
3. You can set contrast polarity by clicking on Dark and Light icon  or  on bottom left of the login screen.
4. Enter your user name and password, accept any security agreement displayed, and click Login.

---

*Note: To configure the security agreement, go to Device Settings > Security > Service Agreement.*

---

5. The web interface opens.

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

- Click Logout in the top right corner, or close the tab or browser.

## Changing Your Password

You need appropriate permissions to change your password or others' passwords.

► *Password requirements:*

- Case sensitive.
- 4 to 64 characters.

► *Password change required on first login:*

- On *first login*, password change is forced and strong passwords are enabled by default. The new password must be at least 8 characters and contain at least one upper case letter, one lower case letter, and one digit.
- Change the default password and click OK.

► *To change your password via the Change Password command:*

You must have the Change Own Password permission to change your own password.

- Choose User Management > Change Password. Change the password and click Save.

Change Password - admin

Old password	required
New password	required
Confirm password	required

✓ Save

## Logout

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

- Click Logout in the top right corner, or close the tab or browser.


## Introduction to the Web Interface

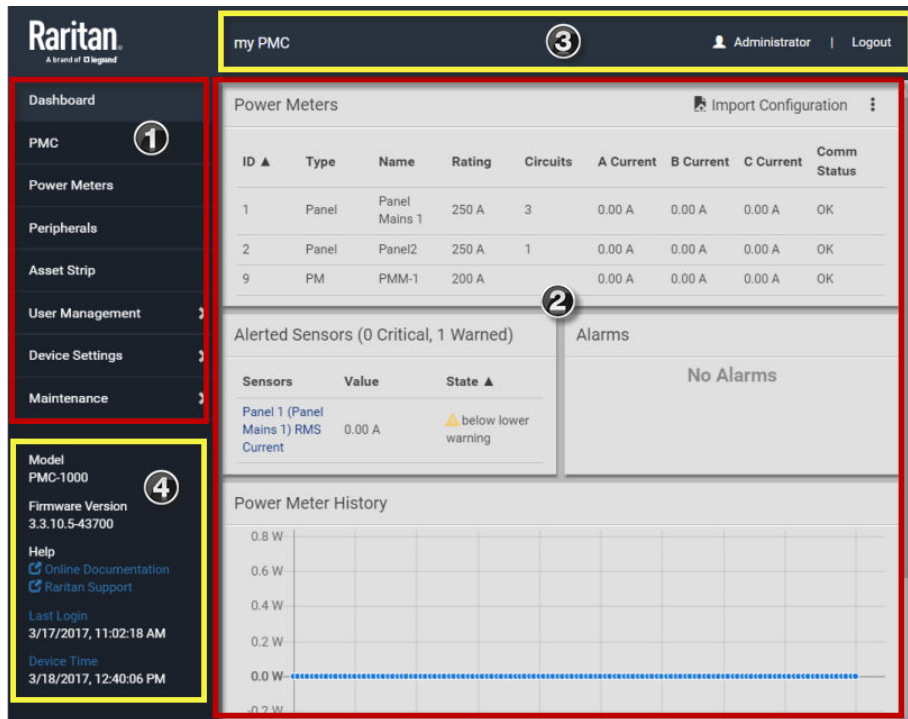
The web interface consists of four areas as shown below.

► *Operation:*

1. Click any menu or submenu item in the area of **1**.
2. That item's data/setup page is then opened in the area of **2**.
3. Now you can view or configure settings on the opened page.



To return to the main menu and the Dashboard page, click  on the top-left corner.

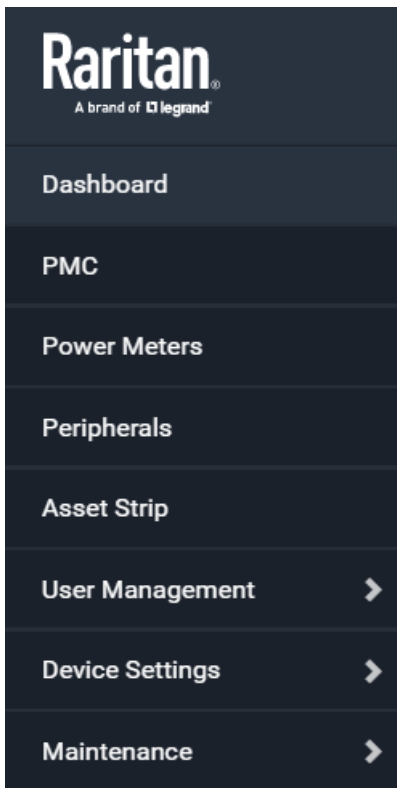


Number	Web interface element
1	Menu
2	Data/setup page of the selected menu item.
3	<ul style="list-style-type: none"> <li>Left side: <ul style="list-style-type: none"> <li>- BCM2 device name.</li> </ul> <hr/> <p><i>Note: To customize the device name, see .</i></p> <hr/> </li> <li>Right side: <ul style="list-style-type: none"> <li>- Displayed language, which is English (EN) by default. You can change it.</li> <li>- Your login name, which you can click to view your user account settings.</li> <li>- Logout button.</li> </ul> </li> </ul>
4	From top to bottom --

Number	Web interface element
	<ul style="list-style-type: none"> <li>Your BCM2 model.</li> <li>Current firmware version.</li> <li>Online Documentation: link to the online help of BCM2. <ul style="list-style-type: none"> <li>- See <b>Browsing through the Online Help</b>.</li> </ul> </li> <li>Raritan Support: link to Raritan Technical Support webpage.</li> <li>Date and time of your user account's last login. <ul style="list-style-type: none"> <li>- Click <b>Last Login</b> to view your login history.</li> </ul> </li> <li>BCM2 system time, which is converted to the time zone of your computer or mobile device. <ul style="list-style-type: none"> <li>- Click <b>Device Time</b> to open the <b>Date/Time</b> setup page.</li> </ul> </li> </ul>

## Menu

Depending on your model and hardware configuration, your menu may show some or all items.



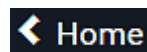
Menu	Information shown
Dashboard	Summary of the BCM2 status, including a list of alerted sensors and alarms, if any. See <a href="#">Viewing the Dashboard</a> (on page 54).
PMC	Device data and settings, such as the device name and MAC address.

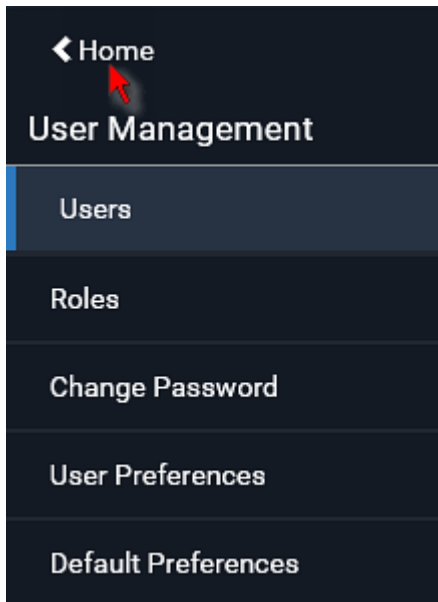
Menu	Information shown
	See PMC.
Power Meters	Power meters and panels data and settings. See Power Meters.
Peripherals	Status and settings of Raritan environmental sensor packages, if connected. See Peripherals.
Feature Port	Status and settings of the device connected to the Feature port(s), which can be one of the following. <ul style="list-style-type: none"> <li>• Asset Strip</li> <li>• External Beeper</li> <li>• LHX 20</li> <li>• SHX 30</li> <li>• LHX 40</li> <li>• Power CIM</li> </ul> See Feature Port.
Webcam, Webcam Snapshots	The webcam-related menu items appear only when there are webcam(s) connected to the BCM2. Webcam live snapshots/video and webcam settings. See Webcam Management.
User Management	Data and settings of user accounts and groups, such as password change. See User Management.
Device Settings	Device-related settings, including network, security, system time, event rules and more. See Device Settings.
Maintenance	Device information and maintenance commands, such as firmware upgrade, device backup and reset. See Maintenance.

If a menu item contains the submenu, the submenu is shown after clicking that item.

► *To return to the previous menu list, do any below:*

- Click the topmost link with the symbol <. For example, click





Click  on the top-left corner to return to the main menu.

## Quick Access to a Specific Page

If you often visit a specific page in the BCM2 web interface, you can bookmark or share the URL. This allows you to log in directly to the desired page.

## Sorting a List

Hover on a column header to see if it is sortable. Click headers that appear as a blue link to sort the list in ascending or descending order based on the selected column.

The arrow is displayed adjacent to the header currently sorted.

ID	Timestamp	Event Class ▲	Event
100	2/26/2022, 4:59:51 AM UTC-0500	Device	The ETH2 network interface link is now up.
101	2/26/2022, 4:59:52 AM UTC-0500	Device	System started.
169	2/26/2022, 5:00:01 AM UTC-0500	Device	[Link Unit 2] System started.
269	3/11/2022, 2:43:34 PM UTC-0500	Device	The ETH2 network interface link is now up.
270	3/11/2022, 2:43:35 PM UTC-0500	Device	System started.
338	3/11/2022, 2:43:44 PM UTC-0500	Device	[Link Unit 2] System started.

## Viewing the Dashboard

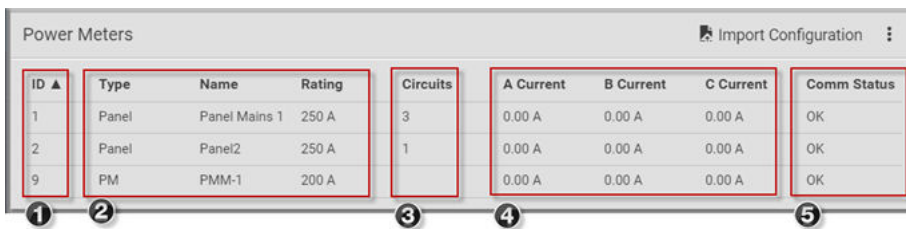
When you log in to the web interface, the Dashboard page is displayed by default. This page provides an overview of the BCM2 device's status.



- |          |  |
|----------|--|
| <b>1</b> | Configured power meters with basic details and current readings for each phase .<br>See <a href="#">Dashboard - Power Meters</a> (on page 55). |
| <b>2</b> | Enabled thresholds show alerts in red and yellow.<br>See <a href="#">Dashboard - Altered Sensors</a>   |
| <b>3</b> | Alarms that need attention.<br>See <a href="#">Dashboard - Alarms</a> .  |
| <b>4</b> | Chart of recent data.<br>See <a href="#">Dashboard - Power Meter History</a> (on page 58).   |

## Dashboard - Power Meters

The Power Meters section of the Dashboard shows all configured power meters and panels, with some details for each.



- 1** ID: The PMM rotary switch setting for the power meter.

2

Type: Panel or PM  
Name: The configured name  
Rating: The configured circuit rating.

3

Circuits: The number of configured circuits

4

A Current/B Current/C Current: The current reading in Amps for each phase.

## Dashboard - Alerted Sensors

When any internal sensors or environmental sensor packages connected to the BCM2 enter an abnormal state, the Alerted Sensors section in the Dashboard shows them for alerting users. This section also lists tripped circuit breakers or blown fuses, if available.

To view detailed information or configure each alerted sensor, click each sensor's name to go to individual sensor pages. See [Individual Sensor/Actuator Pages](#) (on page 87).

Alerted Sensors (1 Critical, 0 Warned)			Alarms
Sensor	Value	State ▲	No Alarms
Temperature 1	25.0 °C	▲ above upper critical	



► *Summary in the section title:*

Information in parentheses adjacent to the title is the total number of alerted sensors.

For example:

- 1 Critical: 1 sensor enters the critical or alarmed state. 1 Warned: 1 'numeric' sensor enters the warning state.
  - Numeric sensors enter warning or critical states, as their values enter the threshold ranges.
  - State sensors enter an alarmed state.

See [Sensor/Actuator States](#) (on page 82) for more details.

	Numeric sensors: <ul style="list-style-type: none"> <li>• Warning</li> </ul>
	Numeric sensors: <ul style="list-style-type: none"> <li>• Critical</li> </ul> State sensors: <ul style="list-style-type: none"> <li>• Alarmed state</li> </ul>



## Dashboard - Alarms

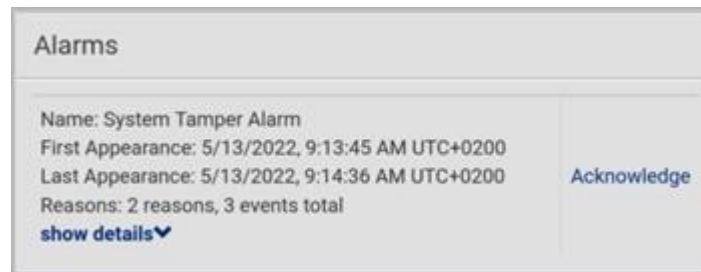
If configuring any event rules which create or emit device alarms, the Alarms section will list any event that hasn't been acknowledged yet.

---

Note: For information on event rules, see [Event Rules and Actions](#) (on page 175).

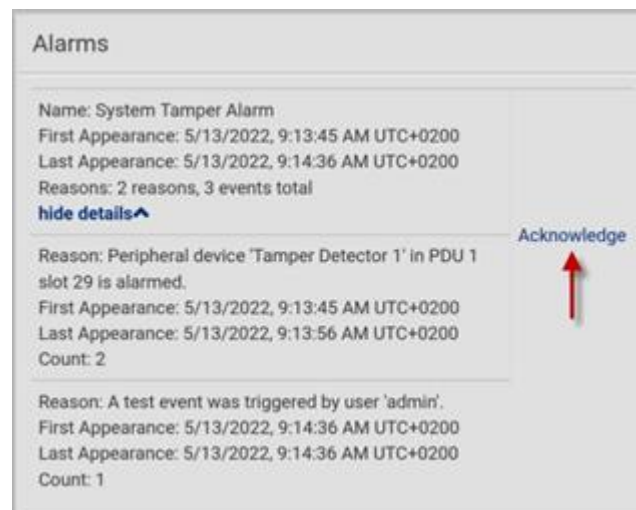
---

You must have the 'Acknowledge Alarms' permission to manually acknowledge an alarm.



► *To acknowledge an alarm:*

- Click Acknowledge, and that alarm then disappears from the Alarms section.



This table explains each field of the alarms list.

Field	Description
Name	Custom name of the Alarm action.
Reason	Shows the log message if the alarm was only triggered by one specific event.
Reasons	Short summary if there were multiple different events.

Field	Description
First Appearance	Date and time when the event indicated in the Reason column occurred for the first time.
Last Appearance	Date and time when the event indicated in the Reason column occurred for the last time.
Count	Number of times the event indicated in the Reason column has occurred.
Show details	<hr/> <hr/> <p>This field appears only when there are multiple types of events triggering the same alert.</p> <hr/> <hr/> <p>If there are other types of events (that is, other reasons) triggering the same alert, the total number of additional reasons is displayed. You can click it to view a list of all events.</p>

The date and time shown on the web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings to your computer or mobile device.

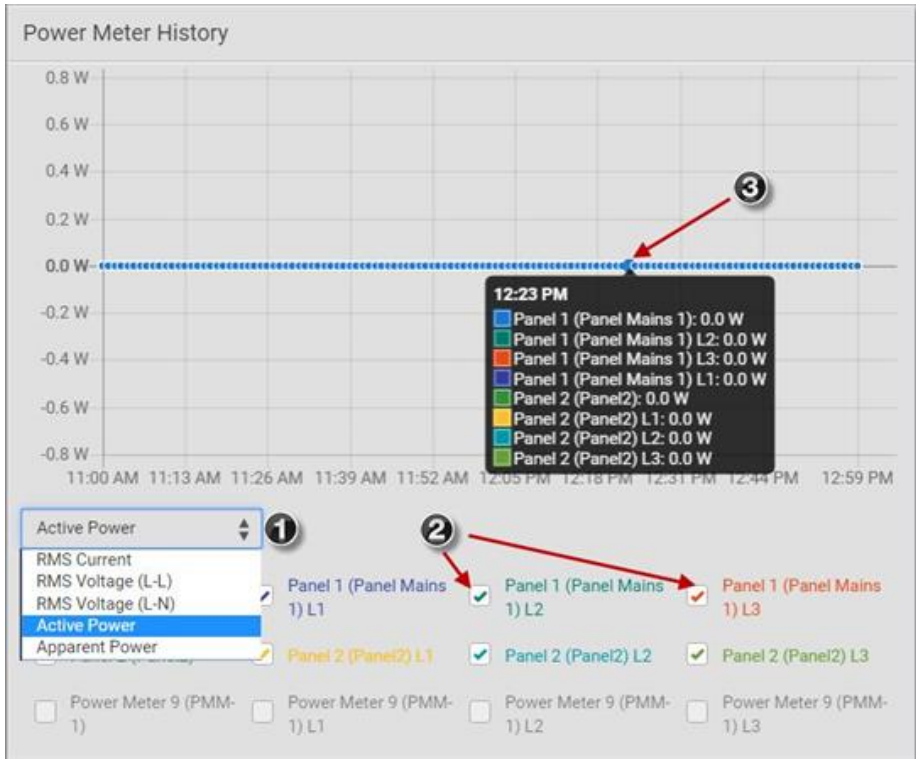
---

Tip: You can also acknowledge all alarms in the front panel display.

---

## Dashboard - Power Meter History

The history graph for the power meter helps you observe whether there were abnormal events within the past range of time. The default is to show the active power data.



- 1** Select a different data type by clicking the selector below the diagram.

  - RMS Current
  - RMS Voltage Line to Line
  - RMS Voltage Line to Neutral
  - Active power
  - Apparent power
- 2** Select the checkbox for the lines you want to add to the diagram. Each line is assigned a custom color.
- 3** Hover the mouse over the graph line to view details for the minute. Each line color is coordinated in the details.

### PMC Power Metering Controller

Click PMC in the Menu to open the Power Metering Controller page.

You can view details on the PMC:

- Firmware Version
- Serial Number
- MAC Address
- Internal beeper state

### Power Metering Controller

**Details**

Firmware version	4.0.10.5-48774
Model	PMC-1000
Serial number	1BZ262C123
MAC address	02:a7:ee:ff:d0:3e
Data log	<a href="#">Export as CSV</a>

**Settings** [Edit Settings](#)

Name	My PMC
Demand sensor update interval	1 min <span style="float: right;">▼</span>
Demand sensor averaging intervals	10

✕ Cancel
✓ Save

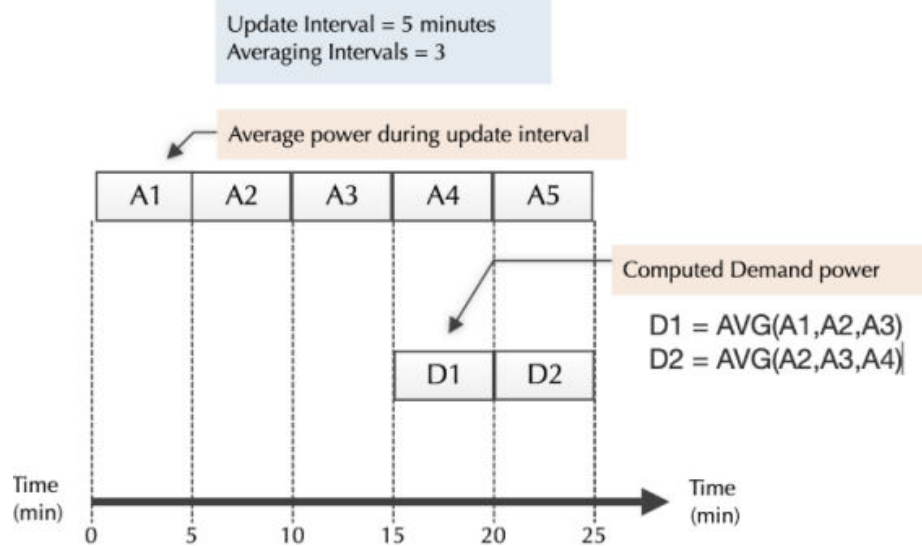
Internal Beeper ▼

Sensors ▼

► *To edit PMC settings:*

- Click the Edit Settings link. The following settings can be changed.
- 1. Name: The name of the PMC appears in the top bar of the web interface.
- 2. Demand sensor: Each power meter contains a demand sensor which measures the peak electrical power demand averaged over a user configurable time interval.
  - Demand sensor update interval: The time interval over which power is averaged to determine electrical demand.
    - Range: 15 seconds - 5 minutes
    - Default: 1 minute
  - Demand sensor averaging intervals: Defines over how many update intervals the sensor reading is averaged.
    - Range: 1-60 intervals
    - Default: 10 intervals (10 minutes)
- 3. Click Save.

## Demand Power Computation



### Power Meters

To view or manage the connected panels and power meters, click Power Meters in the menu.

The Power Meters page contains all configured power meters and panels, allows you to scan for unconfigured meters, and gives access to all configuration possibilities.

ID ▲	Type	Name	Rating	Circuits	A Current	B Current	C Current	Comm Status
1	Panel	Panel Mains 1	250 A	3	0.00 A	0.00 A	0.00 A	OK
2	Panel	Panel2	250 A	1	0.00 A	0.00 A	0.00 A	OK
9	PM	PMM-1	200 A		0.00 A	0.00 A	0.00 A	OK

ID ▲	Type	BCM Channels
No unconfigured meters found		

For help with configuring power meters and panels, see [Configuring Power Meters and Branch Circuit Monitors](#) (on page 34).

### Viewing the Power Meter Data

To view power meter data, go to the Power Meters page and click to select a power meter. You can also select a power meter from the dashboard.

ID ▲	Type	Name	Rating
1	Panel	Panel Mains 1	250 A
2	Panel	Panel2	250 A
9	PM	PMM-1	200 A

The Power Meter details page opens with a list of sensor data and readings.

Power Meter 9 (PMM-1)									
Sensor	Power Meter		Phase A		Phase B		Phase C		
	Value	State	Value	State	Value	State	Value	State	
RMS Voltage (L-L)	0.0 V	normal	0.0 V	normal	0.0 V	normal	0.0 V	normal	
RMS Voltage (L-N)	0.0 V	normal	0.0 V	normal	0.0 V	normal	0.0 V	normal	
Line Frequency	0.00 Hz	below lower critical	0.00 Hz	below lower critical	0.00 Hz	below lower critical	0.00 Hz	below lower critical	
RMS Current	0.00 A	below lower critical	0.00 A	below lower critical	0.00 A	below lower critical	0.00 A	below lower critical	
Phase Angle	0.0°	normal	0.0°	normal	0.0°	normal	0.0°	normal	
Active Power	0 W	normal	0 W	normal	0 W	normal	0 W	normal	
Reactive Power	0 var	normal	0 var	normal	0 var	normal	0 var	normal	
Apparent Power	0 VA	normal	0 VA	normal	0 VA	normal	0 VA	normal	
Power Factor	1.00	normal	1.00	normal	1.00	normal	1.00	normal	
Displacement Power Factor	1.00	normal	1.00	normal	1.00	normal	1.00	normal	
Active Energy	0 Wh	normal	0 Wh	normal	0 Wh	normal	0 Wh	normal	
Neutral Current	0.00 A	normal							
Earth Current	0.00 A	normal							

- 1 Sensor list
- 2 Readings in total for the power meter.
- 3 Readings for each phase.
- 4 If thresholds have been configured for a sensor, and a reading meets a threshold, the data is highlighted red or yellow.
- 5 Value contains the reading for the sensor.
- 6 State indicates if readings are normal, warning or critical.
- 7 Click actions menu for more options.

# Power Meter Management

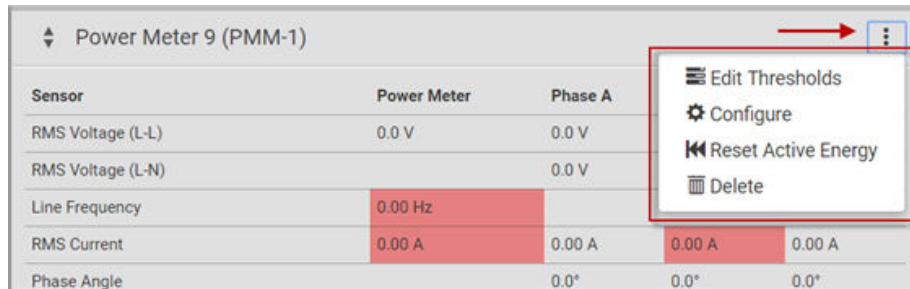
This section introduces the operations for a power meter module. For information on the power meter's sensor data, see [Viewing the Power Meter Data](#) (on page 61).

► *To access power meter management options:*

- Click Power Meters in the menu, then select a power meter. In the power meter details page, click the actions icon in the top right corner.

The following options are available:

- Edit Thresholds: See [Configure Thresholds](#) (on page 69).
- Configure: You can edit some details of the power meter configuration. See [Configure Power Meter](#) (on page 35).
- Reset Active Energy: See below.
- Delete: Click Delete to delete this power meter.



► *To reset active energy:*

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

---

Tip: To reset all active energy readings simultaneously, see [Resetting All Active Energy](#). To reset a branch circuit's active energy, see [Panel Branch Circuits Operations](#) (on page 67). To reset a panel's active energy, see [Panel Mains Circuit Management](#) (on page 67).

---

## Enable Modbus Access

For details on Modbus, see [Configuring Modbus TCP and/or RTU](#).

► *To enable Modbus access:*

1. Select the power meter or panel in the Power Meters page.
2. Click the actions icon to open the options, then choose Configure.
3. Select the Enable Modbus Access checkbox, and assign a "unique" Modbus address to the power meter.
  - This Modbus address must be different from that of the main controller, any panel or power meter module connected to this BCM2, or the BCM2 does NOT allow you to save this dialog.
  - If Modbus/RTU is enabled, make sure this Modbus address is also different from those of other devices on the same Modbus RTU bus.
4. Click OK to save.

## Viewing the Panel Data

To view panel data, including mains circuit and branch circuits, go to the Power Meters page and click to select a panel. You can also select a panel from the dashboard.

Power Meters				
ID ▲	Type	Name	Rating	Circuits
1	Panel	Panel Mains 1	250 A	3
2	Panel	Panel2	250 A	1
3	Panel	Rack3	250 A	0
9	PM	PMM-1	200 A	

The Panel details page opens with a list of sensor data and readings at the top, and a list of Panel Branch Circuits at the bottom.

Panel 1 (Panel Mains 1)										
Sensor		Panel		Phase A		Phase B		Phase C		
Value	State	Value	State	Value	State	Value	State	Value	State	
RMS Voltage (L-L)	0.0 V	normal	0.0 V	normal	0.0 V	normal	0.0 V	normal	0.0 V	normal
RMS Current	0.00 A	below lower warning	0.00 A	normal	0.00 A	normal	0.00 A	normal	0.00 A	normal
Phase Angle			0.0°	normal	0.0°	normal	0.0°	normal	0.0°	normal

Panel Branch Circuits															
Pos	Phase	Name	Rating	CT #	V	A	φ	Pos	Phase	Name	Rating	CT #	V	A	φ
1	A	Rack 1	20 A	1	0.0 V	0.00 A	0.0°	2	A	Rack 2	20 A	2	0.0 V	0.00 A	0.0°
3	B			3		0.00 A	0.0°	4	B			4		0.00 A	0.0°
5	C			5		0.00 A	0.0°	6	C			6		0.00 A	0.0°
7	A	Rack 3	20 A	7	0.0 V	0.00 A	0.0°	8	A	Rack 4	240 A	8	0.0 V	0.00 A	0.0°
9	B			9		0.00 A	0.0°	10	B			10		0.00 A	0.0°
11	C			11		0.00 A	0.0°	12	C			12		0.00 A	0.0°



Select Readings ▾

- Active Energy (Wh)
- Active Power (W)
- Active Power Demand (Demand)
- Apparent Power (VA)
- RMS Current (A)
- Displacement Power Factor (DPF)
- Earth Current
- Line Frequency
- Neutral Current
- Phase Angle ( $\varphi$ )
- Power Factor (PF)
- Reactive Power (var)
- RMS Voltage (L-L) (V)
- RMS Voltage (L-N)

- 1** A short list of readings is available by default.
- 2** To add more readings, click Select Readings, then choose the sensors to add. See graphic for menu details.  
Click actions menu for more options. See [Panel Mains Circuit Management](#) (on page 67).
- 3** Readings in total for the panel.  
If thresholds have been configured for a sensor, and a reading meets a threshold, the data is highlighted red or yellow.
- 4** Readings for each phase.
- 5** Value contains the reading for the sensor.

State indicates if readings are normal, warning or critical.

7

Branch circuit details and readings.

8

Click a branch circuit to show the menu: Circuit Details to open a new page. Or, delete a circuit.

► **Panel Branch Circuit Details page:**

Click a configured circuit, then choose Circuit Details to open a new page with panel branch circuits details. Similar to the panel details, the circuit details displays readings at the circuit level.

Sensor	Circuit		Phase A (CT #1)		Phase B (CT #3)		Phase C (CT #5)	
	Value	State	Value	State	Value	State	Value	State
RMS Current	0.00 A	normal	0.00 A	normal	0.00 A	normal	0.00 A	normal
RMS Voltage	0.0 V	normal						
Phase Angle			0.0°	normal	0.0°	normal	0.0°	normal
Active Power	0 W	normal	0 W	normal	0 W	normal	0 W	normal
Reactive Power	0 var	normal	0 var	normal	0 var	normal	0 var	normal
Apparent Power			0 VA	normal	0 VA	normal	0 VA	normal
Power Factor			1.00	normal	1.00	normal	1.00	normal
Displacement Power Factor			1.00	normal	1.00	normal	1.00	normal
Active Energy	0 Wh	normal	0 Wh	normal	0 Wh	normal	0 Wh	normal
Active Power Demand	0 W	normal						

Note: Branch circuit RMS voltage is the *minimum* of Line-Line or Line-Neutral RMS voltage readings. NO alerts will be available for a branch circuit's RMS voltage even when voltage thresholds are set for it.

1	Panel name and circuit name. Click the arrows to scroll through the configured branch circuits.
2	Click actions menu for more options. See <a href="#">Panel Branch Circuits Operations</a> (on page 67).
3	Sensor list. This list may be filtered by the Select Readings settings in the Panel Mains Circuit page.
4	Total readings for the whole circuit.
5	Readings for each phase. Each phase is labeled with the CT number.
	Value contains the reading for the sensor.
7	State indicates if readings are normal, warning or critical.

## Panel Mains Circuit Management

This section introduces the operations for a panel. For information on the panel's sensor data, see [Viewing the Panel Data](#) (on page 64).

► *To access panel management options:*

Click Power Meters in the menu, then select a panel. In the panel details page, click the actions icon in the top right corner.

The following options are available:

- Edit Thresholds: See [Configure Thresholds](#) (on page 69).
- Configure: You can edit some details of the panel configuration. See [Configure Panel Mains Circuit](#) (on page 36).
- Export Readings as CSV: See [Export Readings as CSV](#) (on page 74)
- Reset Energy Counter: See below.
- Delete: Click Delete to delete this power meter.



► *To reset Energy Counter:*

Click Reset Energy Counter to reset this panel's energy reading to 0 (zero) Wh. You must have the "Change PMC, PMB & PMM Configuration" permission.

## Panel Branch Circuits Operations

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

To manage branch circuits, click the desired branch circuit to open a menu.

Panel Branch Circuits							
Pos	Phase	Name	Rating	CT #	V	A	$\phi$
1 3 5	A	Rack 1	20 A	1	0.0 V	0.00 A	0.0°
	B						
	C						
7 9 11	A	Rack 3	20 A	7	0.0 V	0.00 A	0.0°
	B			9			
	C			11			

Note: For information on creating panel branch circuits, see [Configure Panel Branch Circuits](#) (on page 36). For information on the Panel Branch Circuits section's sensor data, see [Viewing the Panel Data](#) (on page 64).

► *Circuit Details:*

A circuit page showing the circuit readings and detailed information opens. Click the actions menu at top right corner. The following options are available:



- Edit Thresholds: See [Configure Thresholds](#) (on page 69).
- Configure Circuit: Click to open the circuit's setup dialog. See [Configure Panel Branch Circuits](#) (on page 36).
- Reset Energy Counter: This button resets this circuit's energy counter to 0 (zero) Wh. You must have the "Change PMC, PMB & PMM Configuration" permission.
- Delete: Click to delete this circuit.

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

## Setting Power Thresholds

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

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

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

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

---

Note: After setting the thresholds, remember to configure event rules. See Event Rules and Actions.

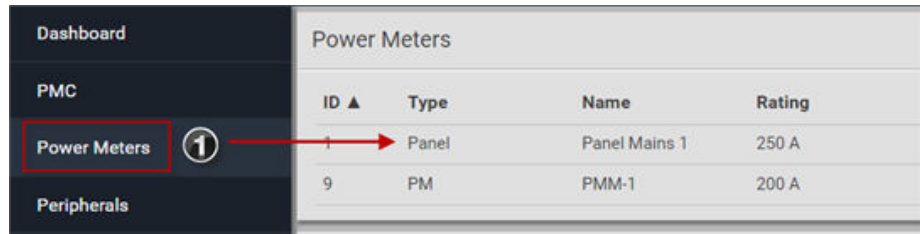
---

## Configure Thresholds

1

In the Power Meters page, click the panel or power meter.

The details page opens.



ID ▲	Type	Name	Rating
1	Panel	Panel Mains 1	250 A
9	PM	PMM-1	200 A

2

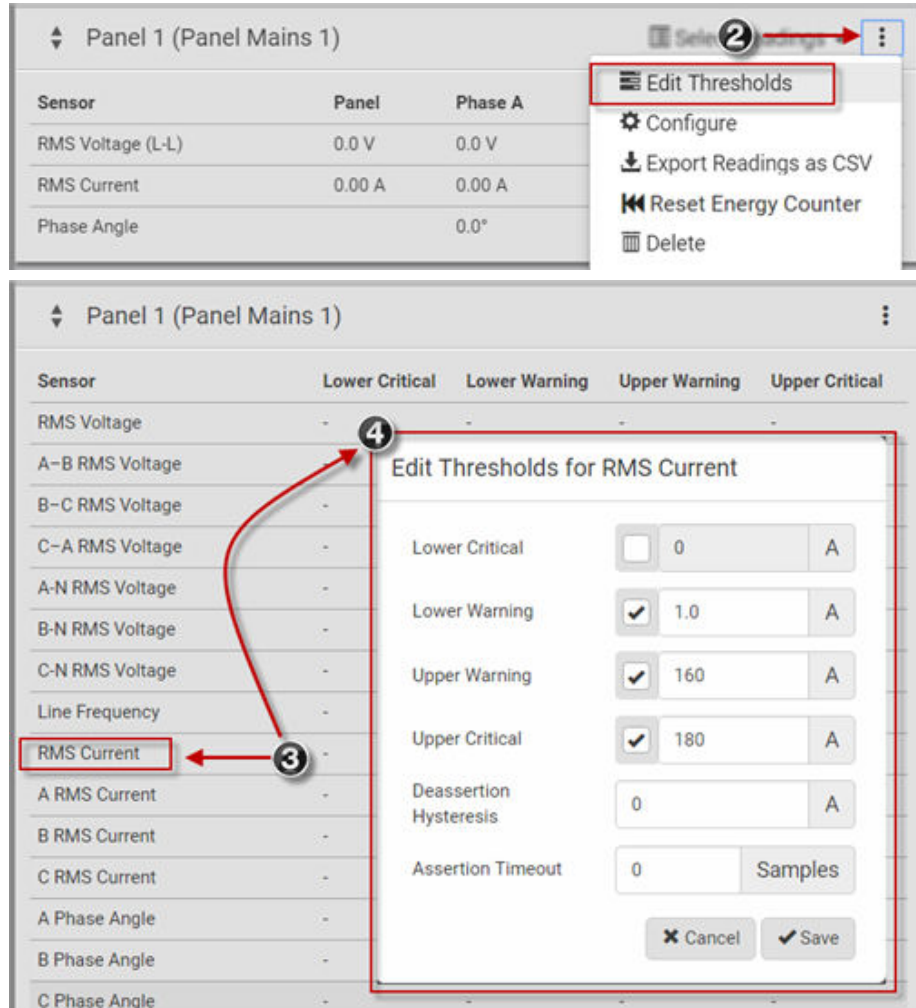
In the details page, click the actions icon, then choose Edit Thresholds.

3

The sensor list displays. Click a sensor to open the Edit Threshold dialog.

4

Select the checkbox for the level, and enter the threshold current in amps. Click OK. This example shows RMS Current set for upper warning and critical levels for the circuit max current rating, and a lower warning set for 1 amp.



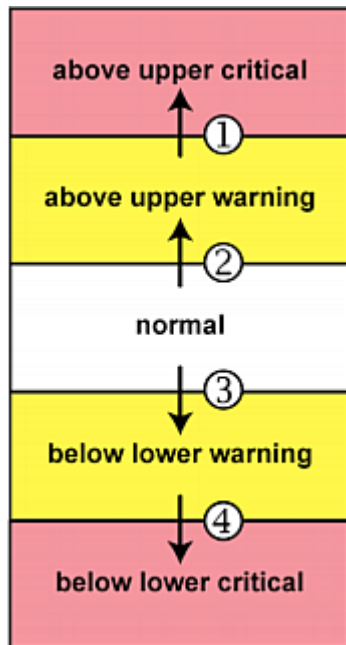
## "To Assert" and Assertion Timeout

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

► *To assert a state:*

To assert a state is to announce a new, "worse" state.

Below are bad state changes that cause the BCM2 to assert.



1. above upper warning --> above upper critical

2. normal --> above upper warning

3. normal --> below lower warning

4. below lower warning --> below lower critical

► *Assertion Timeout:*

Lower Critical	<input checked="" type="checkbox"/>	0	
Lower Warning	<input checked="" type="checkbox"/>	0	
Upper Warning	<input checked="" type="checkbox"/>	0	
Upper Critical	<input checked="" type="checkbox"/>	0	
Deassertion Hysteresis		0	
<b>Assertion Timeout</b>		0	Samples
		<input type="button" value="Cancel"/>	<input type="button" value="Save"/>

In the threshold settings, the Assertion Timeout field postpones the "assertion" action. It determines how long a sensor must remain in the "worse" new state before the BCM2 triggers the "assertion" action. If that sensor changes its state again within the specified wait time, the BCM2 does NOT assert the worse state.

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

---

Note: For most sensors, the measurement unit in the "Assertion Timeout" field is sample. Sensors are measured every second, so the timing of a sample is equal to a second. Raritan's BCM2 is an exception to this, with a sample of 3 seconds.

---

► *How "Assertion Timeout" is helpful:*

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

## "To De-assert" and Deassertion Hysteresis

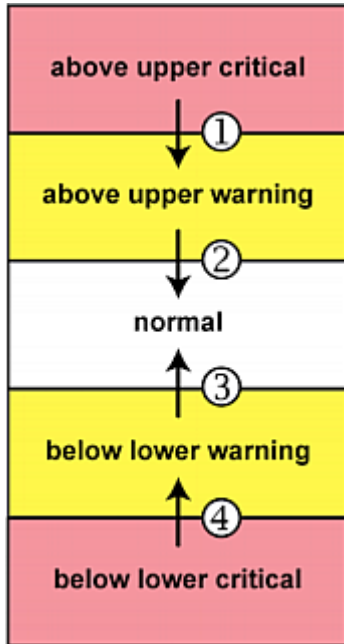
After the BCM2 asserts a worse state for a sensor, it may de-assert that state later on if the readings improve.

► *To de-assert a state:*

To de-assert a state is to announce the end of the previously-asserted worse state.

Below are good state changes that cause the BCM2 to de-assert the previous state.





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

► *Deassertion Hysteresis:*

Lower Critical	<input checked="" type="checkbox"/>	0	
Lower Warning	<input checked="" type="checkbox"/>	0	
Upper Warning	<input checked="" type="checkbox"/>	0	
Upper Critical	<input checked="" type="checkbox"/>	0	
<b>Deassertion Hysteresis</b>		0	
Assertion Timeout		0	Samples

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

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

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

For example, if Deassertion Hysteresis = 2, then the deassertion level of each threshold is either "+2" or "-2" as illustrated below.

Threshold value	Deassertion value
Upper Critical = 33	Deassertion level = 31 • $33 - 2 = 31$
Upper Warning = 25	Deassertion level = 23 • $25 - 2 = 23$
Lower Critical = 10	Deassertion level = 12 • $10 + 2 = 12$
Lower Warning = 18	Deassertion level = 20 • $18 + 2 = 20$

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

---

Note: The difference between Upper Warning and Lower Warning must be at least "two times" of the deassertion value.

---

► *How "Deassertion Hysteresis" is helpful:*

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

## Export Readings as CSV

Export instantaneous readings from the power meter controller as a CSV file. The export file may be helpful to diagnose issues.

You can export readings from each configured power meter and panel.

► *Power meter includes the following readings:*

- ID
- Name
- Line to Line Voltages
- L1-L2, L2-L3, L3-L1
- Line to Neutral voltages
- L1-N

- L2-N
- L3-N
- Frequency
- L1 Current, L2 Current, L3 Current
- L1 Active Power, L2 Active Power, L3 Active Power
- L1 Reactive Power, L2 Reactive Power, L3 Reactive Power

► *Panel includes the following readings:*

- Mains Sensors
  - Line to Line Voltages
    - L1-L2, L2-L3, L3-L1
- Line to Neutral voltages
  - L1-N
  - L2-N
  - L3-N
- Frequency
- L1 Current, L2 Current, L3 Current
- L1 Active Power, L2 Active Power, L3 Active Power
- L1 Reactive Power, L2 Reactive Power, L3 Reactive Power
- For each configured circuit
  - Name
  - For each circuit pole
    - Position
    - Phase
    - CT Number
    - Current
    - Active Power
    - Reactive Power

► *To export readings as CSV:*

1. Click Power Meters in the Menu.
2. Click the actions icon, then choose Export Readings as CSV.

ID ▲	Type	Name	Rating	Circuits	A Current	B Current	C Current	Status
1	Panel	Panel Mains 1	250 A	3	0.00 A	0.00 A	0.00 A	OK
2	Panel	Panel2	250 A	1	0.00 A	0.00 A	0.00 A	OK
9	PM	PMM-1	200 A		0.00 A	0.00 A	0.00 A	OK

## Peripherals

If there are environmental sensor packages connected, they are listed on the Peripherals page.

An environmental sensor package may contain:

- Numeric sensors: Detectors that show both readings and states, such as temperature sensors.
- State sensors: Detectors that show states only, such as contact closure sensors.
- Actuators: An actuator controls a system or mechanism so it shows states only.

BCM2 communicates with *managed* sensors/actuators only and retrieves their data. One BCM2 can manage a maximum of 64 sensors/actuators.


Open the Peripheral Devices page by clicking Peripherals in the *Menu*. Then you can:

- Perform actions on multiple sensors/actuators by using the control/action icons on the top-right corner.
- Go to an individual sensor's or actuator's data/setup page by clicking its name.

### ► *Sensor/actuator overview on this page:*


If any sensor enters an alarmed state, it is highlighted in yellow or red. An actuator is never highlighted.

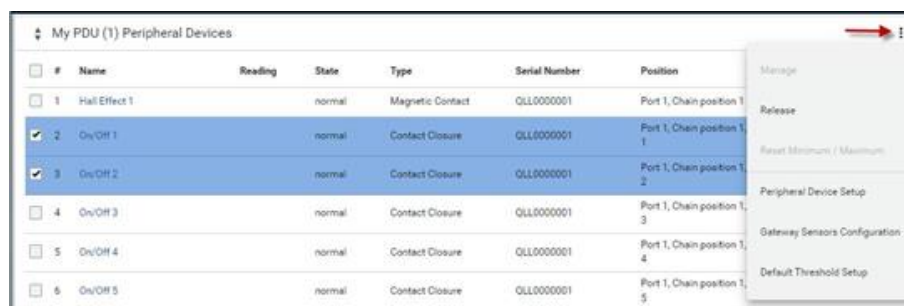
Column	Description
Name	By default, the name assigned contains: <ul style="list-style-type: none"> <li>• Sensor/actuator type, such as "Temperature" or "Dry Contact."</li> <li>• Sequential number of the same sensor/actuator type, like 1, 2, 3 and so on.</li> </ul> <p>You can customize the name. Customize names on the individual sensor page.</p>
Reading	Numeric sensors, such as temperature and humidity, show the reading.
Maximum	Maximum reading of all previously seen values since last reset.
Minimum	Minimum reading of all previously seen values since last reset.
State	Available for all sensors and actuators. <a href="#">Sensor/Actuator States</a> (on page 82)

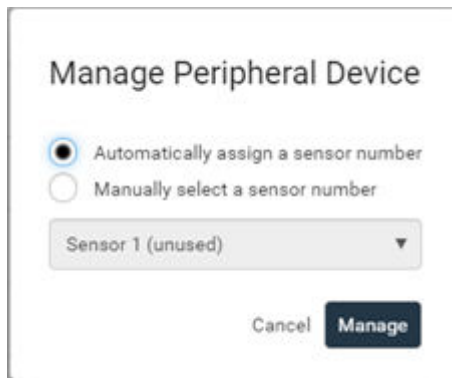
Column	Description
Type	Sensor or actuator type.
Serial Number	This is the serial number printed on the sensor package's label.
Position	Position indicates where this sensor or actuator is located in the sensor chain. <a href="#">Identifying the Sensor Position and Channel</a> (on page 84)
Actuator	Indicates whether this sensor package is an actuator or not. If yes, the checkmark symbol  is shown.

► *To release or manage sensors/actuators:*


You can multi-select sensors to release or manage them. Releasing is necessary when the maximum number of managed sensors are in use, and you need to make a change, such as replacing old sensors with new ones, or making space by removing an unneeded type and adding a different type. When you manage sensors individually, you can manually select ID numbers--this allows you to simultaneously release an old sensor if you select to reuse its assigned ID: [Managing One Sensor or Actuator](#) (on page 85). When you manage multiple sensors at once, ID numbers are automatically assigned, and nothing else is changed or released.

1. Select the sensors/actuators that you want to manage/release from management.
2. Click  to view options and select Manage or Release.
  - Release: The items are automatically released, and you return to the list. Newly released sensors show at the end of the list as "Manage Device" if they are still physically connected, otherwise they disappear.
  - Manage: "Manage Peripheral Device" dialog opens. Click Manage to accept automatic sensor numbers. If a single item was selected, you can choose the ID number by selecting "Manually select a sensor number." Click Manage and you return to the list. Newly managed sensors appear and will show a status in the State column. They can now be renamed and configured.





► To configure sensor/actuator-related settings:

1. Click  > Peripheral Device Setup.


Field	Function	Note
<b>Peripheral device Z coordinate format</b>	Options to describe the vertical locations (Z coordinates) of environmental sensor packages. <ul style="list-style-type: none"> <li>• <i>Rack units or Free-form</i></li> </ul> See <a href="#">Z Coordinate Format</a> (on page 92).	Every sensor has a Z Coordinate field. The format setting specifies whether those coordinates are required to be rack unit numbers or can contain arbitrary text.
<b>Peripheral device auto management</b>	Enables or disables the automatic management feature for Raritan environmental sensor packages. <ul style="list-style-type: none"> <li>• <i>Default is Enabled.</i></li> </ul>	<a href="#">Automatic Management of Sensors</a> (on page 85)
<b>Mute other door handle</b>	<ul style="list-style-type: none"> <li>• If selected, one door handle will be completely powered down (including any attached card reader or keypad) before opening the other lock of the same DX2-DH2C2.</li> </ul>	<ul style="list-style-type: none"> <li>• This option helps to avoid overload in power-limited setups with two door handles.</li> </ul>
<b>Altitude</b>	Specify the altitude of BCM2 above sea level when a differential air pressure sensor is attached. <ul style="list-style-type: none"> <li>• <i>Range: -425 to 3000 meters (-1394 to 9842 feet)</i></li> <li>• <i>Negative numbers indicate locations below sea level.</i></li> </ul>	<ul style="list-style-type: none"> <li>• The device's altitude is associated with the altitude correction factor.</li> <li>• The default altitude measurement unit is meter.</li> <li>• Your user preference for measurements will take effect here.</li> </ul>

Field	Function	Note
<b>Active powered dry contact limit</b>	Determines the maximum number of "active" powered dry contact actuators that is permitted concurrently. <ul style="list-style-type: none"> <li>• <i>Range: 0 to 24</i></li> <li>• <i>Default: 1</i></li> </ul>	<ul style="list-style-type: none"> <li>• An "active" actuator is turned ON, or, for a door handle, door is OPENED.</li> <li>• This setting only applies to "powered dry contact" (PD) actuators rather than normal "dry contact" actuators.</li> <li>• You need either 'Change Peripheral Device Configuration' privilege or 'Administrator Privileges' to change the setting.</li> </ul>

2. Click Save.

► *To configure default threshold settings:*

Note that default threshold settings affect all sensors already being managed, and establish the initial settings for any sensor added from now on. To customize the threshold settings on a per-sensor basis, go to [Individual Sensor/Actuator Pages](#) (on page 87).

1. Click  > Default Threshold Setup.
2. Click a sensor to open the threshold settings.
3. Make changes as needed.
  - To enable any threshold, select the corresponding checkbox.
  - Type a new value in the accompanying text box.


Lower critical	<input checked="" type="checkbox"/>	2	g/m <sup>3</sup>
Lower warning	<input checked="" type="checkbox"/>	4	g/m <sup>3</sup>
Upper warning	<input checked="" type="checkbox"/>	20	g/m <sup>3</sup>
Upper critical	<input checked="" type="checkbox"/>	22	g/m <sup>3</sup>
Deassertion hysteresis		1	g/m <sup>3</sup>
Assertion timeout		0	Samples

4. Deassertion hysteresis: An alarm is cleared when the sensor reading normalizes the specified amount away from the threshold. In the screenshot example above, if temperature normalizes by more than 1 degree of the threshold, the alarm is cleared. When the reading is within 1°C from the threshold, the alarm will remain active. For example: A warning is raised when the temperature exceeds 30°C. It has to drop to 29°C to clear the warning.
5. Assertion timeout: An alarm is raised when the sensor reading exceeds a threshold for more than the specified number of samples. In the screenshot example above, timeout is set to Zero. An alarm would be raised immediately when the reading exceeds the threshold. If the timeout were set for 20, the sensor reading would have to persist in exceeding a threshold for 20 data samples before an alarm would be raised.
6. Click Save.

► *To turn on or off any actuator:*

1. Select one or multiple actuators . This activates the power buttons at the top right corner in the web interface.
2. Click On or Off. For Door Handles, click Open or Close.

---

*Note: Per default you can turn on as many dry contact actuators as you want, but only one "powered dry contact" actuator can be turned on at the same time. Change this setting in  > Peripheral Device Setup.*

---

3. Confirm the operation when prompted.

## Yellow- or Red-Highlighted Sensors

The BCM2 highlights those sensors that enter the abnormal state with a yellow or red color. Note that numeric sensors can change colors when thresholds are enabled.

---







**Tip:** When an actuator is turned ON, it is also highlighted in red for drawing attention.

---



Name	Reading	State	Type	Serial Number	Position	Actuator
Temperature 2	24.0 °C	normal	Temperature	QMT0000005	Port 1, Chain position 5	
Temperature 1	25.0 °C	above upper warning	Temperature	QMS0000004	Port 1, Chain position 4	
Relative Humidity 1	40 %	above upper critical	Humidity	QMS0000004	Port 1, Chain position 4	
Powered Dry Contact 2		off	Powered Dry Contact	QU7000003	Port 1, Chain position 3, Channel 2	✓

In the following table, "R" represents any numeric sensor's reading. The symbol <= means "smaller than" or "equal to."

Sensor status	Color	States shown in the interface	Description
Unknown		unavailable	Sensor state or readings cannot be detected.
		unmanaged	Sensors are not being managed.
Normal		normal	<ul style="list-style-type: none"> <li>Numeric or state sensors are within the normal range.</li> <li>-- OR --</li> <li>No thresholds have been enabled for numeric sensors.</li> </ul>
Warning		above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
		below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
Critical		above upper critical	Upper Critical threshold < "R"
		below lower critical	"R" < Lower Critical threshold
Alarmed		alarmed	State sensors enter the abnormal state.
OCP alarm		Open	<ul style="list-style-type: none"> <li>Circuit breaker trips.</li> <li>-- OR --</li> <li>Fuse blown.</li> </ul>

## Managed vs Unmanaged Sensors/Actuators

### ► *Managed sensors/actuators:*

- BCM2 communicates with managed sensors/actuators and retrieves their data.
- Managed sensors/actuators are always listed on the Peripheral Devices page whether they are physically connected or not.

<input type="checkbox"/>	Name	Reading	State	Type ▼
<input type="checkbox"/>	Temperature 2	24.0 °C	normal	Temperature
<input type="checkbox"/>	Temperature 1	25.0 °C	normal	Temperature
<input type="checkbox"/>	Powered Dry Contact 2		off	Powered Dry Contact
<input type="checkbox"/>	Powered Dry Contact 1		off	Powered Dry Contact

- They show one of the managed states.
- For managed 'numeric' sensors, their readings are retrieved and displayed. If any numeric sensor is disconnected or its reading cannot be retrieved, it shows "unavailable" for its reading.

► *Unmanaged sensors/actuators:*

- BCM2 does NOT communicate with unmanaged sensors/actuators.
- Unmanaged sensors/actuators are listed only when they are physically connected to BCM2. They disappear from the web interface when they are no longer connected.
- They do *not* have an ID number.
- They show the "unmanaged" state.

## Sensor/Actuator States

An environmental sensor or actuator shows its real-time state after being managed.

Available sensor states depend on the sensor type -- numeric or state sensors. For example, a contact closure sensor is a state sensor so it switches between three states only -- *unavailable*, *alarmed* and *normal*.

Sensors will be highlighted in yellow or red when they enter abnormal states.

An actuator's state is marked in red when it is turned on.

► *Managed sensor states:*

In the following table, "R" represents any numeric sensor's reading. The symbol <= means "smaller than" or "equal to."

State	Description
normal	<ul style="list-style-type: none"> <li>• For numeric sensors, it means the readings are within the normal range.</li> <li>• For state sensors, it means they enter the normal state.</li> </ul>
below lower critical	"R" < Lower Critical threshold
below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold

State	Description
above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
above upper critical	Upper Critical threshold < "R"
alarmed	The state sensor enters the abnormal state.
unavailable	<ul style="list-style-type: none"> <li data-bbox="480 447 997 474">• Communication with the managed sensor is lost.</li> <li data-bbox="521 485 594 512">-- OR --</li> <li data-bbox="480 522 1044 550">• Sensor packages are upgrading their sensor firmware.</li> </ul>

Note that for a contact closure sensor, the normal state depends on the normal setting you have configured.

► *Managed actuator states:*

<b>State</b>	<b>Description</b>
<b>on</b>	<b>The actuator is turned on.</b>
<b>off</b>	<b>The actuator is turned off.</b>
<b>unavailable</b>	<ul style="list-style-type: none"> <li>● <b>Communication with the managed actuator is lost.</b></li> <li style="text-align: center;">-- OR --</li> <li>● <b>Sensor packages are upgrading their sensor firmware.</b></li> </ul>

► *Unmanaged sensor/actuator states:*

<b>State</b>	<b>Description</b>
<b>unmanaged</b>	<b>Sensors or actuators are physically connected to the BCM2 but not managed yet.</b>

---

Note: Unmanaged sensors or actuators will disappear from the web interface after they are no longer physically connected.

---

## Finding the Sensor's Serial Number

A sensor package has a serial number tag attached to its rear side.

The serial number for each sensor or actuator appears listed in the web interface when it is detected. Match the serial number from the tag to those listed in the sensor table.

#	Name	Reading	State	Type	Serial Number	
1	Hall Effect 1		normal	Magnetic Contact	QLL0000001	
2	On/Off 1		normal	Contact Closure	QLL0000001	
3	On/Off 2		normal	Contact Closure	QLL0000001	

## Identifying the Sensor Position and Channel

The Peripheral Devices page shows where each sensor or actuator is connected.

Name	Reading	Serial Number	Position	Actuator
Temperature 2	24.0 °C	QMT0000005	Port 1, Chain position 5	
Temperature 1	25.0 °C	QMS0000004	Port 1, Chain position 4	
Powered Dry Contact 2		QU70000003	Port 1, Chain position 3, Channel 2	✓
Powered Dry Contact 1		QU70000003	Port 1, Chain position 3, Channel 1	✓

- The position information includes the port name and the sensor's position in a sensor chain.  
For example: *Port 'Sensor', Chain Position 3*
- If a sensor hub is involved, the hub port information is also indicated for most sensors.  
For example: *Port 'Sensor', Hub port 2, Chain Position 3*
- If a sensor/actuator contains channels, such as a contact closure sensor or dry contact actuator, the channel information is included.  
For example, *Port 'Sensor', Hub port 2, Chain Position 3, Channel 1*

## Automatic Management of Sensors

To configure automatic management, go to Peripherals >  > Peripheral Device Setup.

### ► *After enabling the automatic management function:*

When the maximum number of sensors are not yet managed, newly-connected environmental sensors and actuators are automatically managed upon detection.

### ► *After disabling the automatic management function:*

You must manually manage all sensors to start communications. Until you do this, they will not have ID numbers or show sensor readings or states.

## Managing One Sensor or Actuator

If you are managing only one sensor or actuator, you can assign the desired ID number to it. When managing multiple sensors/actuators at a time, the IDs are automatically assigned.

---

Tip: When the total of managed sensors/actuators reaches the maximum value, you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace the managed ones. To replace a managed one, assign an ID number to it by following the procedure below.

---

### ► *To manage only one sensor/actuator:*

1. Click Peripherals in the Menu.
2. Unmanaged sensors/actuators appear at the end of the list as "Manage Device". You can identify the sensor/actuator by the Type, Serial Number, and Position columns.

<input type="checkbox"/>	Name	Reading	State ▼	Type	Serial Number
	Manage Device		unmanaged	Absolute Humidity	QMS0000004
	Manage Device		unmanaged	Door Handle	1GE0000001
	Door Lock 2		unavailable	Door Lock	1GE0000001
	Door Lock 1		unavailable	Door Lock	1GE0000001

3. Click the Manage Device link, and the Manage Peripheral Device dialog appears.

## Manage Peripheral Device

- Automatically assign a sensor number  
 Manually select a sensor number

Sensor 31 (unused) ▼

Cancel

Manage

- Select "Automatically assign a sensor number" to assign an unused ID number. This method does not release any managed sensor or actuator.
- Select "Manually select a sensor number" to select a desired ID number from the list. Selecting an ID already in use will release the sensor currently managed with that ID. IDs already in use show the sensor package's serial number. Available IDs show "unused."

4. Click Manage.

► *Special note for Legrand humidity sensors:*

A Legrand humidity sensor is able to provide three measurements - relative and absolute, and humidity values.

- A relative humidity value is measured in percentage (%).
- An absolute humidity value is measured in grams per cubic meter ( $g/m^3$ ).
- A dew point is measured in degree celsius ( $^{\circ}C$ ).

However, only relative humidity sensors are "automatically" managed if the automatic management function is enabled. You must "manually" manage absolute humidity sensors as needed.

---

Note: Relative and absolute values of the same humidity sensor do NOT share the same ID number though they share the same serial number and position.

---

## Individual Sensor/Actuator Pages

A sensor's or actuator's data/setup page is opened after clicking any sensor or actuator name on the Peripheral Devices page.

Note that only a numeric sensor has threshold settings, while a state sensor or actuator has no thresholds.

Threshold settings, if enabled, help you identify whether any numeric sensor enters the warning or critical level. In addition, you can have BCM2 automatically generate alert notifications for any warning or critical status.

► *To configure a numeric sensor's threshold settings:*

1. Click Edit Thresholds.



Sensor		
	Value	Last time changed or reset
Actual	24.0 °C	
State	normal	
Minimum	24.0 °C	8/16/2021, 10:52:55 AM UTC-0400
Maximum	24.0 °C	7/29/2023, 3:27:09 AM UTC-0400
Reset Minimum / Maximum	<input type="button" value="Reset"/>	8/16/2021, 10:52:55 AM UTC-0400

---

*Tip: The date and time shown on the BCM2 web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone to your computer or mobile device.*

---

2. Select or deselect 'Use default thresholds' according to your needs.

Sensor
Edit Thresholds

Use default thresholds	<input checked="" type="checkbox"/>	
Lower critical	<input checked="" type="checkbox"/>	10 °C
Lower warning	<input checked="" type="checkbox"/>	15 °C
Upper warning	<input checked="" type="checkbox"/>	30 °C
Upper critical	<input checked="" type="checkbox"/>	35 °C
Deassertion hysteresis	1	°C
Assertion timeout	0	Samples

✕ Cancel ✔ Save

- To have this sensor follow the default threshold settings configured for its own sensor type, select the 'Use default thresholds' checkbox.

The default threshold settings are configured on the page of *Peripherals*.

- To customize the threshold settings for this particular sensor, deselect the 'Use default thresholds' checkbox, and then modify the threshold fields below it.

---

*Note: For concepts of thresholds, deassertion hysteresis and assertion timeout, see [Sensor Threshold Settings](#) (on page 496).*

---

3. Click Save.

► *To set up a sensor's or actuator's physical location and additional settings:*

1. Click Edit Settings.



Settings

[Edit Settings](#)

Name	Temperature 2
Description	<input type="text"/>
Location (X)	<input type="text"/>
Location (Y)	<input type="text"/>
Location (Z: Rack Units)	<input type="text"/>

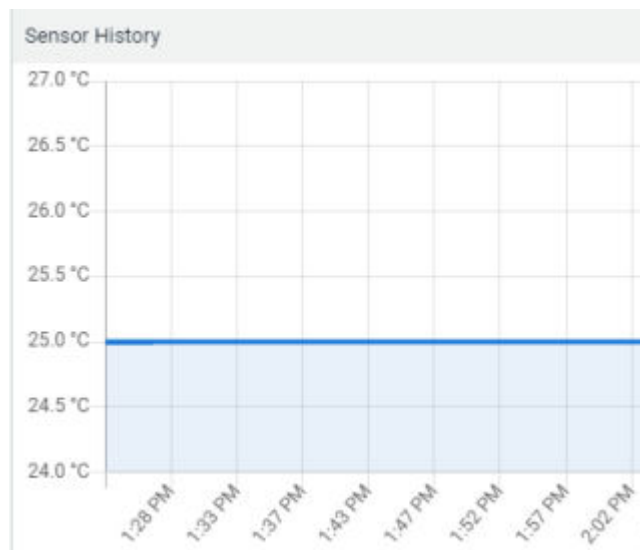
2. Make changes to available fields, and then click Save.

Fields	Description
Name	A name for the sensor or actuator.
Description	Any descriptive text you want.
Location (X, Y and Z)	Describe the sensor's or actuator's location in the data center by typing alphanumeric values for the X, Y and Z coordinates. See <a href="#">Sensor/Actuator Location Example: X, Y, Z Coordinates</a> (on page 92) If the term "Rack Units" appears in parentheses in the Z location, you must type an integer number. The Z coordinate's format is determined on the page of <i>Peripherals</i> .
Alarmed to Normal Delay	<hr/> <hr/> This field is available for the DX2-PIR presence detector only. <hr/> <hr/> It determines the wait time before the BCM2 announces that the presence detector is back to normal after it already returns to normal. Adjust the value in seconds.
Binary Sensor Subtype	<hr/> <hr/> This field is available for any Raritan contact closure sensor except for DX2-DH2C2's contact closure sensors. <hr/> <hr/> Determine the sensor type of your contact closure detector. <ul style="list-style-type: none"> <li>• <i>Contact Closure</i> detects the door lock or door open/closed status.</li> <li>• <i>Smoke Detection</i> detects the appearance of smoke.</li> <li>• <i>Water Detection</i> detects the appearance of water on the floor.</li> <li>• <i>Vibration</i> detects the vibration of the floor.</li> </ul>

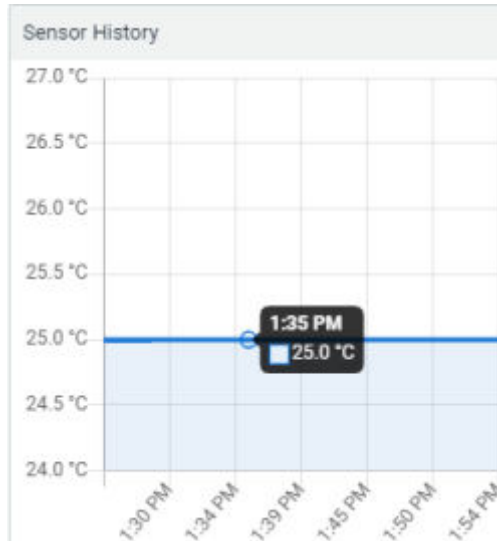
Fields	Description
Sensor Polarity	<p>This field is available for DX2-CC2 contact closure sensors only.</p> <hr/> <p>Determine the normal state of your DX2-CC2.</p> <ul style="list-style-type: none"> <li>• <i>Normal Open</i>: The open status of the connected detector/switch is considered normal. An alarm is triggered when the detector/switch turns closed.</li> <li>• <i>Normal Closed</i>: The closed status of the connected detector/switch is considered normal. An alarm is triggered when the detector/switch turns opened.</li> </ul>

► *To view a numeric sensor's chart*

This sensor's data within the past tens of minutes is shown in the chart. Note that only a numeric sensor has this diagram. State sensors and actuators do not have such data.




- To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data are displayed as illustrated below.



► To turn on or off an actuator:

1. Click the desired control button.

My PDU (1) Peripheral Devices							On	Off
Name	Reading	State	Type	Serial Number	Position	Actuator		
Manage Device		unmanaged	Door Handle	10E0000001	Port 1, Chain position 5, Channel 2			
Manage Device		unmanaged	Absolute Humidity	0M00000004	Port 1, Chain position 4			
Door Handle 1		unavailable	Door Handle	10E0000001	Port 1, Chain position 6, Channel 1			
Door Lock 1		unavailable	Door Lock	10E0000001	Port 1, Chain position 6, Channel 1	✓		
Door Lock 2		unavailable	Door Lock	10E0000001	Port 1, Chain position 6, Channel 2	✓		
Door State 1		closed	Door State	10E0000001	Port 1, Chain position 6, Channel 1			
Door State 2		closed	Door State	10E0000001	Port 1, Chain position 6, Channel 2			
Dry Contact 1		off	Dry Contact	QLL0000001	Port 1, Chain position 1, Channel 1	✓		
Dry Contact 2		off	Dry Contact	QLL0000001	Port 1, Chain position 1, Channel 2	✓		
<input checked="" type="checkbox"/> Dry Contact 3		off	Dry Contact	QLL0000002	Port 1, Chain position 2, Channel 1	✓		
Dry Contact 4		off	Dry Contact	QLL0000002	Port 1, Chain position 2, Channel 2	✓		
Input Module 1		normal	Master Contact	0110000001	Slot 1, Chain position 1			

 On : Turn ON.

 Off : Turn OFF.


2. Confirm the operation on the confirmation message.

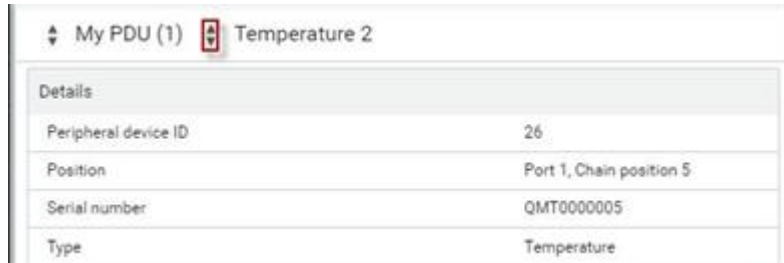
---

Note: Per default you can turn on as many dry contact actuators as you want, but only one "powered dry contact" actuator can be turned on at the same time. To change this limitation of "powered dry contact" actuators, modify the active powered dry contact setting on the Peripherals page.

---

► *Other operations:*

You can go to another sensor's or actuator's data/setup page by clicking the selector  on the top-left corner.



Details	
Peripheral device ID	26
Position	Port 1, Chain position 5
Serial number	QMT0000005
Type	Temperature

## Z Coordinate Format

Z coordinates refer to vertical locations of environmental sensor packages. You can use either the number of rack units or a descriptive text to describe Z coordinates.

► *To configure Z coordinates:*

1. Determine the Z coordinate format in the main Peripheral Device Setup page. Available Z coordinate formats include:
  - Rack Units: Measurement of the height is in standard rack units. Number from 0-60.
  - Free-form: Enter any alphanumeric string to describe the Z coordinate. Up to 24 characters. Example, "Top of Rack", "Bottom of Rack".
2. Enter the Z coordinates in the individual sensor settings.

## Sensor/Actuator Location Example: X, Y, Z Coordinates

Use the X, Y and Z coordinates to describe each sensor's or actuator's physical location in the data center.

The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. Therefore, you can use non-measurement values.

► *Example:*

***X = Brown Cabinet Row***

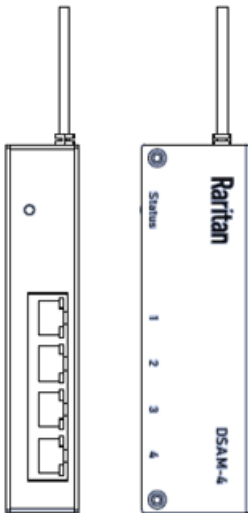
***Y = Third Rack***

***Z = Top of Cabinet***

► *Values of the X, Y and Z coordinates:*

- X and Y: They can be any alphanumeric values comprising 0 to 24 characters.
- Z: When the Z coordinate format is set to *Rack units*, it can be any number ranging from 0 to 60. When its format is set to *Free-form*, it can be any alphanumeric value comprising 0 to 24 characters.

### Serial Access With Dominion Serial Access Module



Connecting a BCM2 and a Dominion Serial Access Module (DSAM) provides access to devices such as LAN switches and routers that have a RS-232 serial port.

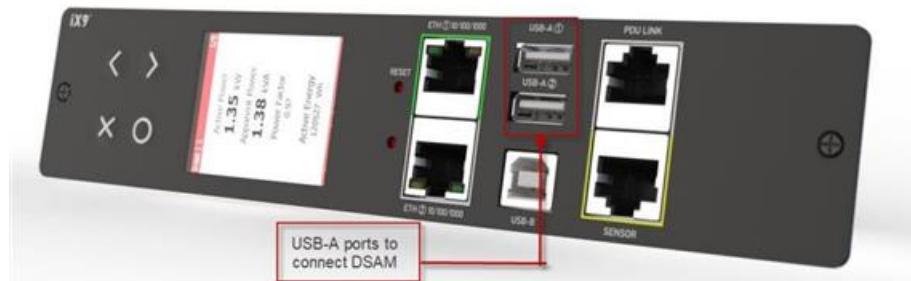
The DSAM is a 2- or 4 port serial module that derives power from the BCM2.

Connect a maximum of 2 DSAM modules to the BCM2 using USB cables. DSAM can be mounted in a 0U configuration.

## DSAM Connection

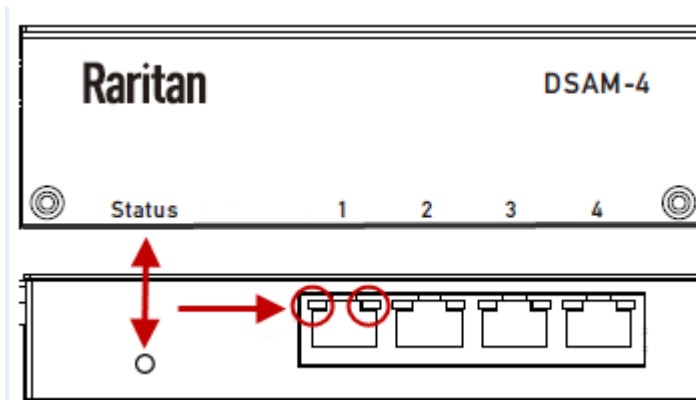
### ► To connect DSAM to BCM2:

- Connect the DSAM unit's USB cable to the BCM2 USB-A ports. No USB Hubs are supported
- Connect the serial devices to the serial ports on the DSAM unit.
- The serial access ports of DSAM can operate in DTE (Data Terminal Equipment) or DCE (Data Circuit Terminating Equipment) mode



## DSAM LED Operation

The DSAM unit has one LED for status, and 2 LEDs on each port.



### ► Status LED:

The Status LED is labeled on the unit front. Light is on back. The Status LED gives information at bootup and upgrade.

- Green LED - Slow blink: DSAM booting up but not controlled by BCM2.
- Blue LED - Slow blink: DSAM controlled by BCM2.
- Blue LED - Fast blink: Firmware upgrade in progress.

► *Port LEDs:*

Each port has a left Green LED and a right Yellow LED.

- Green LED: Port is set as DCE
- Yellow LED: Port is set as DTE
- LEDs off: Port is set as AUTO and no target is connected

## View DSAM Serial Ports

When a DSAM unit is connected to the BCM2, a DSAM Serial Ports page is available.

#▲	Name	Type	Status	Availability	
1.1	DSAM 1 - Port 1	DTE	Available	Connected	►Connect
1.2	DSAM 1 - Port 2	Auto	Available	Disconnected	►Connect
1.3	DSAM 1 - Port 3	Auto	Available	Disconnected	►Connect
1.4	DSAM 1 - Port 4	Auto	Available	Disconnected	►Connect

► *To view DSAM serial ports:*

Click DSAM Serial Port Access. You can access and configure serial ports from this page.

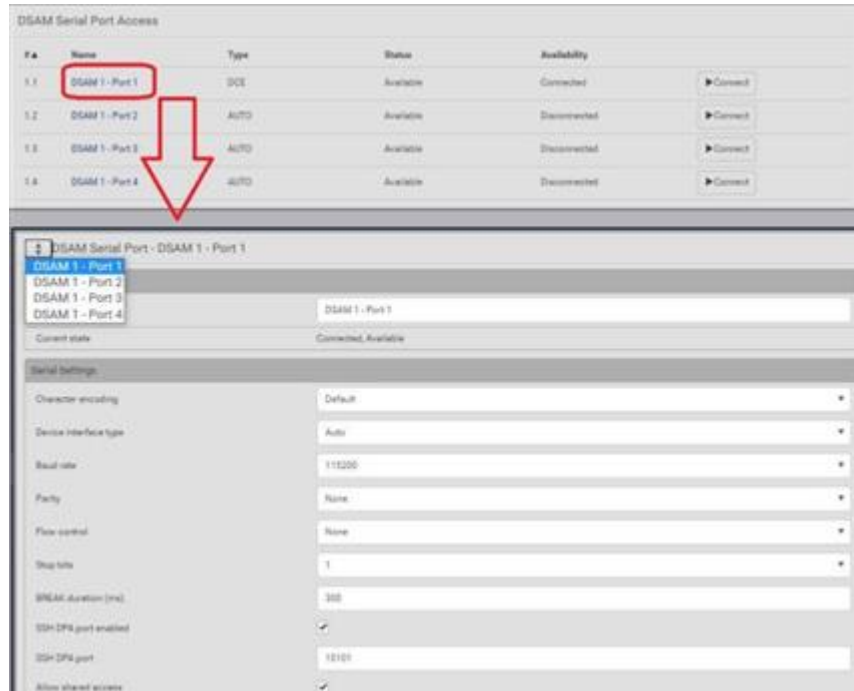
- Ports are listed by physical USB position on the DSAM unit.
- # column indicates which BCM2 USB port DSAM is plugged into.
- Type column indicates port's DTE/DCE setting.
- Status and Availability columns show current activity.

## Configure DSAM Serial Ports

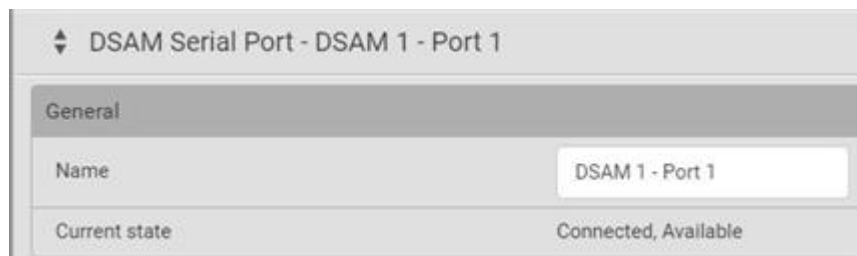
You can rename serial ports and configure their settings.

► *To configure DSAM serial ports:*

1. Click DSAM Serial Port Access, then click the name of the port for the port you want to configure.



2. In the General section:



- Enter a Name for the port.
  - Check the Current State of the port. Status and Availability are listed.
3. In the Serial Settings section, check or change the following settings:



Serial Settings

Device interface type: Auto

Baud rate: 9600

Parity: None

Flow control: None

Stop bits: 1

BREAK duration (ms): 300

SSH DPA port enabled:

SSH DPA port: 10101

Allow shared access:

Cancel Save

## Connect to DSAM Serial Targets in the Web Interface

Dashboard

PDU

Inlet

Outlets

Outlet Groups

OCPs

Peripherals

DSAM Serial Port Access

User Management >

Device Settings >

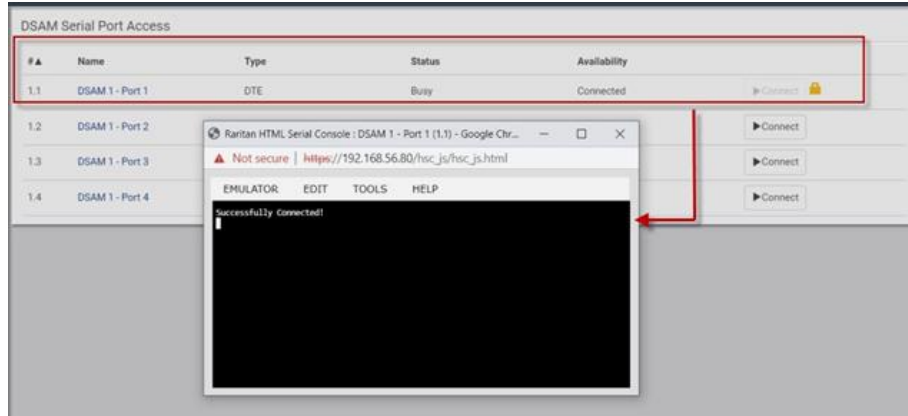
Maintenance >

DSAM Serial Port Access

# ▲	Name	Type	Status	Availability	
1.1	DSAM 1 - Port 1	DTE	Available	Connected	▶ Connect
1.2	DSAM 1 - Port 2	Auto	Available	Disconnected	▶ Connect
1.3	DSAM 1 - Port 3	Auto	Available	Disconnected	▶ Connect
1.4	DSAM 1 - Port 4	Auto	Available	Disconnected	▶ Connect

► To connect to DSAM serial targets in the web interface:

1. Click DSAM Serial Port Access to view the list of ports.
2. Click Connect button of the port you want to connect to.  
HSC launches in a new window.



## DSAM CLI Commands

- show
  - show sxport [<sxportid>]  
Shows serial access port parameters
  - sxportid Serial access port id (or 'all') (1.1/1.2/all) [all]  
Shows DSAM serial port parameters

Example:

```
# show sxport 1.1
Port ID: 1.1
Name: DSAM 1 - Port 1
Device connected: No
Device interface type: Automatic
Baud rate: 9600
Parity: None
Data bits: 8
Stop bits: 1
Flow control: None
BREAK duration: 300 ms
SSH DPA port enabled: No
SSH DPA port: 10101
Allow shared access: No
Status: Available
```

- connect:
  - Connect to a DSAM serial port
    - connect [<sxportid>]

---

Note: You have write access to this port

---

During connecting to target, Pressing the escape sequence (CONTROL-]) the following target port CLI command can be reached:

clientlist Display all users on the port  
close Close this target connection  
getwrite Get write access for the port  
resetport Reset port  
return Return to the target session  
sendbreak Send a break to the connected target  
writelock Lock write access to this port  
writeunlock Unlock write access to this port  
Pressing ? will provide help

- config  
You can configure only connected DSAMs ports
  - config:# sxport  
sxport <sxportid> [name <name>] [devinterfacetype <deviftype>] [baudrate <baudrate>] [parity <parity>] [stopbits <stopbits>] [flowcontrol <flowcontrol>] [breakduration <breakduration>] [sshdpaportenabled <sshdpaportenabled>] [sshdpaport <sshdpaport>] [allowsharedaccess <allowsharedaccess>]  
Configure serial access port settings:  
sxportid Serial access port id (1.1/1.2)  
name Port name  
devinterfacetype Device interface type (AUTO/DTE/DCE)  
baudrate Serial port speed (baud rate) in bits-per-second (1200/1800/2400/4800/9600/19200/38400/57600/115200/230400)  
parity Parity type (none/odd/even)  
stopbits Number of stop bits (1..2)  
flowcontrol Flow control type (none/hw/sw)  
breakduration Duration of BREAK signal in ms (0..1000)  
sshdpaportenabled Enable direct port access via Secure Shell (SSH) (true/false)  
sshdpaport TCP port for direct port access via Secure Shell (SSH) (1024..49999)  
allowsharedaccess Allow shared (r/o) access (true/false)

## Connect to DSAM Serial Targets via SSH

► *To connect to DSAM serial targets via SSH:*

1. Make sure that SSH Access is enabled in Device Settings > Network Services > SSH.
2. Connect to the port in two ways:
  - Via configured SSH DPA port:
    1. Type command `ssh -p <SSH DPA port> user@device`

---

*Note: Make sure SSH DPA port enabled is selected in DSAM Serial Port Access >DSAM Port #.*

---

- Via regular TCP port:
  1. Type command `ssh user:1.2@device`
- 1. After login, user will enter CLI interface.
- 2. Press Escape Sequence `^]`
- 3. Type commands See: [DSAM CLI Commands](#) (on page 98)

---

*Example: show slexport 1.1*

---

4. To exit serial target, type escape-key-sequence, default is Ctrl-], then enter port sub-menu CLI interface.
5. Type "close", then enter main CLI interface.

### Asset Strips

After connecting and detecting asset management strips (asset strips), the BCM2 shows 'Asset Strip' in the menu.

On this page, you can configure the rack units of asset strips and asset tags. A rack unit refers to a tag port on the asset strips. The "Change Asset Strip Configuration" permission is required.

► *To configure asset strip and rack unit settings:*

1. Click Asset Strips in the menu, then click the Asset Strip you want to configure.
2. Click Edit Settings.

Settings
⤴

[Edit Settings](#)

Name	
Number of rack units	64
Numbering mode	Bottom-up ▾
Numbering offset	1 ⬆ ⬇ ⬆
Color with connected tag	<div style="background-color: #00ff00; width: 100px; height: 15px; margin: 0 auto;"></div>
Color without connected tag	<div style="background-color: #ff0000; width: 100px; height: 15px; margin: 0 auto;"></div>

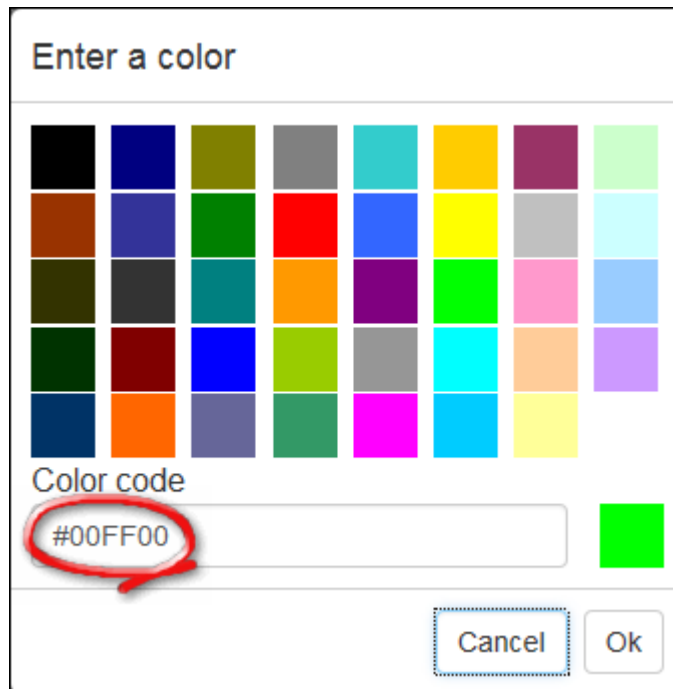
✕ Cancel
✓ Save

3. Make changes to the settings by directly typing a new value, or clicking that field to select a different option.












Field	Description
Name	Name for this asset strip assembly.
Number of rack units	The number of rack units is auto-detected for all supported AMS, the input field is always disabled.
Numbering mode	The rack unit numbering method in a rack/cabinet. <ul style="list-style-type: none"> <li><i>Top-Down</i>: The numbering starts from the highest rack unit of a rack/cabinet.</li> <li><i>Bottom-Up</i>: The numbering starts from the lowest rack unit of a rack/cabinet.</li> </ul>
Numbering offset	The start number in the rack unit numbering. For example, if this value is set to 3, then the first number is 3, the second number is 4, and so on.
Color with connected tag	Click this field to determine the LED color denoting the presence of an asset tag. <ul style="list-style-type: none"> <li>Default is green.</li> </ul>
Color without connected tag	Click this field to determine the LED color denoting the absence of an asset tag. <ul style="list-style-type: none"> <li>Default is red.</li> </ul>

For color settings, there are two ways to set the color.

- Click a color in the color palette.
- Type the hexadecimal RGB value of the color, such as #00FF00.



4. Click Ok. The rack unit numbering and LED color settings are immediately updated on the Rack Units list illustrated below.
  - The 'Index' number is the physical tag port number printed on the asset strip, which is not configurable. However, its order will change to reflect the latest rack unit position.

Rack Units							Program Asset IDs
Position ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	1		Krizia I		Manual override	On	
2	2				Auto (based on tag)	On	
3	3				Auto (based on tag)	On	
4	4				Auto (based on tag)	On	
5	5			DEADBEEF0000	Auto (based on tag)	On	
6	6				Auto (based on tag)	On	
7	7				Auto (based on tag)	On	
8	8				Auto (based on tag)	On	
9	9				Auto (based on tag)	On	
10	10				Auto (based on tag)	On	
11	11				Auto (based on tag)	On	

- A blade extension strip and a *programmable* tag are marked with the word 'programmable' in the Asset/ID column. You can customize their Asset IDs.

► *To customize a single rack unit's settings:*

You can make a specific rack unit's LED behave differently from the others on the asset strip, including the LED light and color.

1. Click the desired rack unit position on the Rack Units list. The setup dialog for the selected one appears.

### Setup of Rack Unit 3

**Name**

**Operation Mode**

Auto (based on Tag) ▼

**LED Mode**

On ▼

**LED Color**

2. Make changes to the information by typing a new value or clicking that field to select a different option.

Field	Description
Name	Name for this rack unit. For example, you can name it based on the associated IT device.
Operation Mode	Determine whether this rack unit's LED behavior automatically changes according to the presence and absence of the asset tag. <ul style="list-style-type: none"> <li><i>Auto</i>: The LED behavior varies, based on the asset tag's presence.</li> <li><i>Manual Override</i>: This option differentiates this rack unit's LED behavior.</li> </ul>
LED Mode	<hr/> <hr/> <p>This field is configurable only after the Operation Mode is set to Manual Override.</p> <hr/> <hr/> <p>Determine how the LED light behaves for this particular rack unit.</p> <ul style="list-style-type: none"> <li><i>On</i>: The LED stays lit.</li> <li><i>Off</i>: The LED stays off.</li> <li><i>Slow blinking</i>: The LED blinks slowly.</li> <li><i>Fast blinking</i>: The LED blinks quickly.</li> </ul>



Field	Description
LED Color	<hr/> <hr/> <p>This field is configurable only after the Operation Mode is set to Manual Override.</p> <hr/> <hr/> <p>Determine what LED color is shown for this rack unit if the LED is lit.</p>

► *To expand a blade extension strip:*


A blade extension strip, like an asset strip, has multiple tag ports. An extension strip is marked with a grayer color on the Asset Strip page, and its tag ports list is collapsed by default.

---

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

---

1. Locate the rack unit (tag port) where the blade extension strip is connected. Click its slot number,

whose format is similar to **1-N** , where N is the total number of its tag ports.

Rack Units							Program Asset IDs
Position ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	1			000015B914BB	Auto	On	
2	2	1-16 		0000ABC12345 (programmable)	Auto	On	
3	3			000015B9152E	Auto	On	
4	4				Auto	On	

2. All tag ports of the blade extension strip are listed below it. Their port numbers are displayed in the Slot column.

Rack Units							Program Asset IDs
Position ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	1			000015B9148B	Auto	On	
2	2	1-16 ▼		0000ABC12345 (programmable)	Auto	On	
	Extension	1		000015B9160A			
	Extension	2		000015B91610			
	Extension	3		000015B91622			
	Extension	4		000015B9158C			
	Extension	5		000015B91600			
	Extension	6		000015B91546			
	Extension	7					
	Extension	8					
	Extension	9					
	Extension	10					
	Extension	11					
	Extension	12					
	Extension	13					
	Extension	14					
	Extension	15					
	Extension	16					
3	3			000015B9152E	Auto	On	







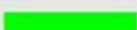
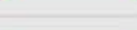


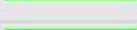
- To hide the blade extension slots list, click **1-N ▼**.

► *To customize asset IDs on programmable asset tags:*

You can customize asset IDs only when the asset tags are "programmable" ones. Non-programmable tags do not support this feature. In addition, you can also customize the ID of a blade extension strip.

If a barcode reader is intended, connect it to the computer you use to access the BCM2.

1. Click Program Asset IDs.

Rack Units							Program Asset IDs
Position ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	16				Auto	On	
2	15				Auto	On	
3	14				Auto	On	
4	13				Auto	On	
5	12				Auto	On	
6	11				Auto	On	
7	10			(programmable)	Auto	On	
8	9			(programmable)	Auto	On	
9	8			(programmable)	Auto	On	
10	7			00001492BD47	Auto	On	
11	6			00001492CB50	Auto	On	

2. In the Asset/ID column, enter the customized asset IDs by typing values or scanning the barcode.
  - When using a barcode reader, first click the desired rack unit, and then scan the asset tag. Repeat this step for all desired rack units.
  - An asset ID contains up to 12 characters that comprise only numbers and/or UPPER CASE letters. Lower case letters are NOT accepted.

Rack Units				
Position ▲	Index	Slot	Name	Asset / ID
1	16			Tag ID
2	15			Tag ID
3	14			Tag ID
4	13			Tag ID
5	12			Tag ID
6	11			Tag ID
7	10			WINDOWS
8	9			LINUX
9	8			ROUTER <input type="text"/> X
10	7			00001492BD47

3. Verify the correctness of customized asset IDs and modify as needed.
4. Click Apply at the bottom of the page to save changes.

## Asset Strip Automatic Firmware Upgrade

After connecting the asset strip, it automatically checks its own firmware version against the version of the asset strip firmware stored in the BCM2. If two versions are different, the asset strip automatically starts downloading the new firmware from the BCM2 to upgrade its own firmware.

During the firmware upgrade, the following events take place:

- The asset strip is completely lit up, with the blinking LEDs cycling through diverse colors.
- A firmware upgrade process is indicated in the web interface.
- An SNMP trap is sent to indicate the firmware upgrade event.

### External Beeper

After connecting and detecting a supported external beeper, the BCM2 shows 'External Beeper' in the menu.

The External Beeper page shows an external beeper's status, including:

- Number of the FEATURE port where this external beeper is connected
- Device type
- Connection status
- The beeper's state - off or active

## Power CIM

After connecting and detecting a Power CIM, the BCM2 shows 'Power CIM' in the menu.

The Power CIM page shows the CIM's status, including:

- Number/information on the port where this CIM is connected.
- Device type
- Connection status

## User Management


User Management deals with user accounts, permissions, and preferred measurement units on a per-user basis.

BCM2 is shipped with one built-in administrator account. You cannot delete this administrator account or change its roles, but you can rename it. Besides the default administrator account, you can create an additional administrative user that can be disabled, renamed or removed. The Admin role is the system-defined administrator role that includes all privileges. You can create additional users and roles. User roles determine the tasks/actions a user is permitted to perform, so you must assign one or multiple roles to each user.

If you are using remote authentication, you do not have to create users accounts locally. Settings are in Device Settings > Security > Authentication. See [Setting Up External Authentication](#) (on page 161).

## Creating Users

All local users must have a user account, containing the login name and password. Multiple users can log in simultaneously using the same login name.

To add users, choose User Management > Users > then click the Add User icon  New User .



<input type="checkbox"/>	User Name	Full Name	Roles	Enabled ▲
	admin	Administrator	Admin	✓
	tom	Tom Smith	Alarm Management	✓

► *User information:*

<b>Field/setting</b>	<b>Description</b>
<b>User name</b>	<p><b>The name the user enters to log in.</b></p> <ul style="list-style-type: none"> <li>• 1 to 32 characters</li> <li>• Case sensitive</li> <li>• Colon character ;, forward slash /, and spaces are NOT permitted.</li> </ul>
<b>Full name</b>	<p><b>The user's first and last names.</b></p>
<b>Password, Confirm password</b>	<ul style="list-style-type: none"> <li>• 4 to 64 characters</li> <li>• Case sensitive</li> <li>• Spaces are permitted.</li> </ul>
<b>Telephone number</b>	<p><b>The user's telephone number</b></p>
<b>Email address</b>	<p><b>The user's email address</b></p> <ul style="list-style-type: none"> <li>• Up to 128 characters</li> <li>• Case sensitive</li> </ul>
<b>Enable</b>	<p><b>When selected, the user can log in.</b></p>
<b>Force password change on next login</b>	<p><b>When selected, a password change request automatically appears the next time the user logs in.</b></p>

► *SSH:*

You need to enter the SSH public key only if public key authentication for SSH is enabled.

1. Open the SSH public key with a text editor.
2. Copy and paste all content in the text editor into the SSH Public Key field.

► *SNMPv3:*

The SNMPv3 access permission is disabled by default.

<b>Field/setting</b>	<b>Description</b>
Enable SNMPv3	<p>Select this checkbox when intending to permit the SNMPv3 access by this user.</p> <hr/> <p>Note: The SNMPv3 protocol must be enabled for SNMPv3 access.</p> <hr/>

Field/setting	Description
Security level	Click the field to select a preferred security level from the list: <ul style="list-style-type: none"> <li>• None</li> <li>• Authentication: Authentication and no privacy.</li> <li>• Authentication &amp; Privacy: Authentication protocol SHA-1, privacy protocol AES-128. Default.</li> </ul>

- Authentication Password: This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

Field/setting	Description
Same as user password	Select this checkbox if the authentication password is identical to the user's password.  To specify a different authentication password, disable the checkbox.
Password, Confirm password	Type the authentication password if the 'Same as User Password' checkbox is deselected.  The password must consist of 8 to 32 ASCII printable characters.

- Privacy Password: This section is configurable only when 'Authentication & Privacy' is selected.

Field/setting	Description
Same as authentication password	Select this checkbox if the privacy password is identical to the authentication password.  To specify a different privacy password, disable the checkbox.
Password, Confirm password	Type the privacy password if the 'Same as Authentication Password' checkbox is deselected.  The password must consist of 8 to 32 ASCII printable characters.

- Protocol: This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

Field/setting	Description
Authentication	Click this field to select the desired authentication protocol. Two protocols are available: <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA-1 (default)</li> <li>• SHA-224</li> <li>• SHA-256</li> <li>• SHA-384</li> <li>• SHA-512</li> </ul>

Field/setting	Description
Privacy	Click this field to select the desired privacy protocol. Two protocols are available: <ul style="list-style-type: none"> <li>• DES</li> <li>• AES-128 (default)</li> <li>• AES-192</li> <li>• AES-256</li> <li>• AES-192 (3DES key extension)</li> <li>• AES-256 (3DES key extension)</li> </ul>

► *Preferences:*

This section determines the measurement units displayed in the web interface and CLI for this user. The user can also change these in the User Management > User Preferences page. SNMP uses the defaults set in User Management > Default Preferences.

Field	Description
Temperature unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length unit	Preferred units for length or height -- Meter or Feet.
Pressure unit	Preferred units for pressure -- Pascal or Psi. <ul style="list-style-type: none"> <li>• Pascal = one newton per square meter</li> <li>• Psi = pounds per square inch</li> </ul>

► *Roles:*

Select one or multiple roles to determine the user's permissions. A user can have a maximum of 32 roles. Note: With multiple roles selected, a user has the union of all roles' permissions.

If the built-in roles do not satisfy your needs, add new roles by clicking New Role. This newly-created role will be then automatically assigned to the user account currently being created.

Built-in role	Description
<b>Admin</b>	Provide full permissions.





Built-in role	Description
<b>Operator</b>	Provide frequently-used permissions, including: <ul style="list-style-type: none"> <li>• Acknowledge Alarms</li> <li>• Change Own Password</li> <li>• Change Pdu, Inlet, Outlet &amp; Overcurrent Protector Configuration (if your model is a PDU)</li> <li>• Switch Outlet (if your model supports it)</li> <li>• Switch Outlet Group (if your model supports it)</li> <li>• Change PMC, PMB, &amp; PMM Configuration (if your model is a branch circuit monitor)</li> <li>• View Event Settings</li> <li>• View Local Event Log</li> </ul>

## Editing or Deleting Users


To edit or delete users, choose User Management > Users to open the Users page.

Users				<a href="#">+ New User</a>	<a href="#">Delete</a>
<input type="checkbox"/>	User Name	Full Name	Roles	Enabled ▲	
<input type="checkbox"/>	test		Operator	✘	
<input checked="" type="checkbox"/>	admin	Administrator	Admin	✔	
<input type="checkbox"/>	tom	Tom Smith	Alarm Management	✔	

In the Enabled column:

-  : The user is enabled.
-  : The user is disabled.
- Sort the list by clicking the header.

► *To edit or delete a user account:*

1. On the Users page, click the desired user. The Edit User page for that user opens.
  - You can rename the user. This action is logged.
  - To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password remains unchanged.
  - To delete this user, click  **Delete**, and confirm the operation.

Edit User - tom → Delete

**User**

User name: tom

Full name: Tom Smith

Password:

Confirm password:

Telephone number:


Email address:

Enable:

Force password change on next login:

2. Click Save for changes.

► *To delete multiple user accounts:*

1. On the Users page, select users by clicking the checkboxes.
2. Click the Delete icon  Delete then click to confirm.

---

Note: You cannot delete the original factory-default Administrator account, but you can disable it.

---

Users <span style="float: right;">+ New User Delete</span>				
<input checked="" type="checkbox"/>	User Name	Full Name	Roles	Enabled ▲
<input checked="" type="checkbox"/>	test		Operator	<input type="checkbox"/>
<input type="checkbox"/>	admin	Administrator	Admin	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	tom	Tom Smith	Alarm Management	<input checked="" type="checkbox"/>

## Creating Roles

A role is a combination of permissions. Each user must have at least one role.


The BCM2 provides two built-in roles.

Built-in role	Description
Admin	Provide full permissions.

Built-in role	Description
Operator	Provide frequently-used permissions, including: <ul style="list-style-type: none"> <li>• Acknowledge Alarms</li> <li>• Change Own Password</li> <li>• Change Pdu, Inlet, Outlet &amp; Overcurrent Protector Configuration</li> <li>• Switch Outlet (for supported models)</li> <li>• Switch Outlet Group (for supported models)</li> <li>• View Event Settings</li> <li>• View Local Event Log</li> </ul>

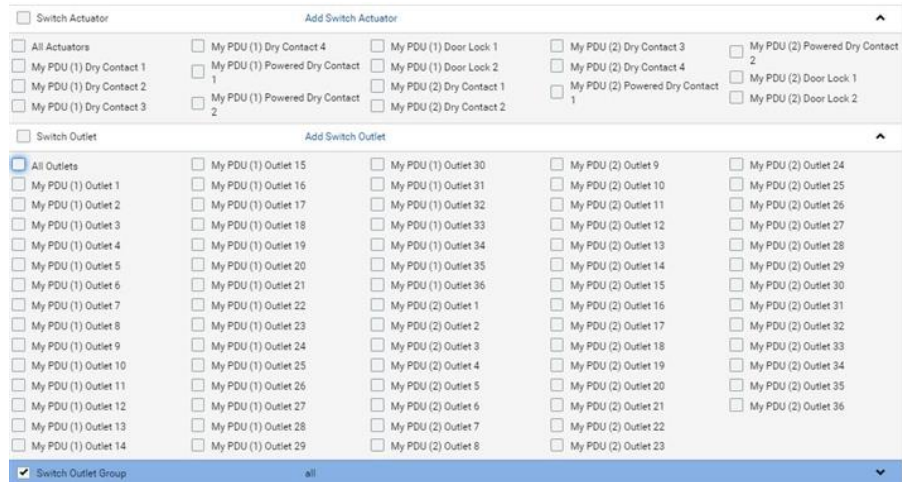
If the two roles do not satisfy your needs, add new roles. Up to 64 roles are supported.

► *To create a role:*

1. Choose User Management > Roles > New icon  **New Role** .



2. Assign a role name.
  - 1 to 32 characters long
  - Case sensitive
  - Spaces are permitted
3. Type a description for the role in the Description field.
4. Select the desired privilege(s).
  - The 'Administrator Privileges' includes all privileges.
  - The 'Unrestricted View Privileges' includes all 'View' privileges.
5. Some privileges have additional selections. These rows contain a blue hyperlink and expand arrow. Click either to view options.
  - For example, in the Switch Actuator and Switch Outlet privileges, you can specify the actuators and outlets that users can switch on/off.




6. Click Save. The role is created and you can assign it to any user.

## Editing or Deleting Roles


Roles cannot be renamed, but you can delete them or change their included privileges.

Choose User Management > Roles to open the Roles page, which lists all roles.

The built-in Admin role displays the lock icon . You cannot delete it or change it.




► *To edit a role:*

1. On the Roles page, click the desired role. The Edit Role page opens.
  - You can edit the description or change the privileges.
  - To delete this role, click  Delete, and confirm the operation.

2. Click Save.

► *To delete any roles:*

1. On the Roles page, select the checkboxes for roles you want to delete.
2. Click the Delete icon  Delete then click Delete in the confirmation message.

## Permissions

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

## Setting Your Preferred Measurement Units

You can change the measurement units shown in the user interface according to your own preferences regardless of the permissions you have.

Measurement unit changes apply to the web interface and CLI. SNMP uses the default measurement units. See [Setting Default Measurement Units](#) (on page 118).

Setting your own preferences does not change the default measurement units.

► *To set user preferences:*

1. Choose User Management > User Preferences.
2. Make changes as needed.

Field	Description
Temperature unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length unit	Preferred units for length or height -- Meter or Feet.
Pressure unit	Preferred units for pressure -- Pascal or Psi. <ul style="list-style-type: none"> <li>• Pascal = one newton per square meter</li> <li>• Psi = pounds per square inch</li> </ul>

3. Click Save.

## Setting Default Measurement Units

User preferences apply to displays in the GUI and CLI for locally authenticated users. Default preferences apply to the front panel and SNMP, and to remote-authenticated users.

► *To set up default user preferences:*

1. Click User Management > Default Preferences.
2. Make changes as needed.

Field	Description
Temperature unit	Preferred units for temperatures -- Celsius or Fahrenheit.
Length unit	Preferred units for length or height -- Meter or Feet.
Pressure unit	Preferred units for pressure -- Pascal or Psi. <ul style="list-style-type: none"> <li>• Pascal = one newton per square meter</li> <li>• Psi = pounds per square inch</li> </ul>

3. Click Save.

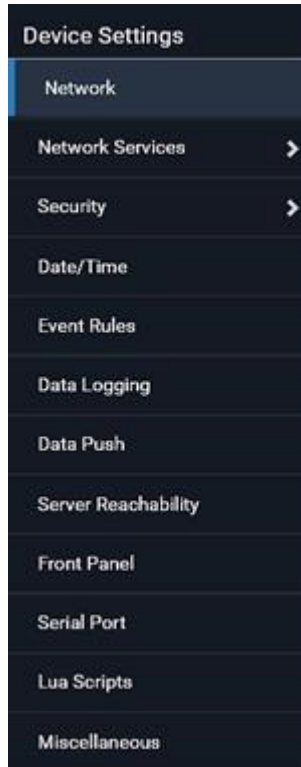
## User Interfaces Showing Default Units

Default measurement units will apply to the following user interfaces or data:

- Web interface for "newly-created" local users when they have not configured their own preferred measurement units.
- Web interface for users who are remotely authenticated.
- The sensor report triggered by the "Send Sensor Report" action.
- Front panel LCD display.

### Device Settings

Click 'Device Settings' in the *Menu*.



## Network Settings

Configure wired, wireless, and Internet protocol-related settings on the Network page after connecting the BCM2 to your network.

You can enable both the wired and wireless networking so that there are multiple IP addresses -- wired and wireless IP. For example, you can obtain one IPv4 and/or IPv6 address by enabling one Ethernet interface, and obtain one more IPv4 and/or IPv6 address by enabling/configuring the wireless interface. This also applies in port forwarding mode so that BCM2 has more than one IPv4 or IPv6 address.

However, in the BRIDGING mode, there is only one IP address for wired networking. Wireless networking is NOT supported in this mode.

Default gateways are configured per interface.

---

**Important: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.**

---

- ▶ *After enabling either or both Internet protocols:*

After enabling IPv4 and/or IPv6, all but not limited to the following protocols will be compliant with the selected Internet protocol(s):

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

---

Note: BCM2 disables TLS 1.0 and 1.1 by default. It enables only TLS 1.2 and 1.3.

---

## Common Network Settings

Common Network Settings are OPTIONAL, not required. Therefore, leave them unchanged if there are no specific local networking requirements.

Field	Description
Cascading mode	Leave it to the default "None" unless you are establishing a cascading chain. <ul style="list-style-type: none"> <li>• <a href="#">Setting the Cascading Mode</a> (on page 134)</li> </ul>
DNS resolver preference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. <ul style="list-style-type: none"> <li>• IPv4 address: Use the IPv4 addresses.</li> <li>• IPv6 address: Use the IPv6 addresses.</li> </ul>
DNS suffixes (optional)	Specify a DNS suffix name if needed.



Field	Description
First/Second/ Third DNS server	<p>Manually specify static DNS server(s).</p> <ul style="list-style-type: none"> <li>• If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server.</li> <li>• If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, DHCP-assigned DNS servers are used.</li> </ul>

You can manually configure or the route information using IPv4 and IPv6 static routes. See [Static Route Examples](#) (on page 131) and [Static Route Interface Names](#) (on page 133).

The screenshot displays two sections for configuring static routes. The top section is for IPv4 routes, featuring a table with columns for '#', 'Destination', and 'Next Hop / Interface'. Below the table, it indicates 'no routes defined' and includes an 'Add Route' button. The bottom section is for IPv6 routes, also with a table for '#', 'Destination', and 'Next Hop / Interface', indicating 'no routes defined' and an 'Add Route' button.

## 802.1x Security Overview

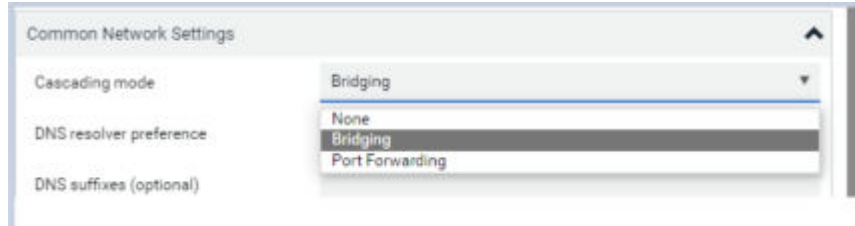
You can configure IEEE 802.1X authentication separately on each LAN port to give the BCM2 a secure access on your LAN or WLAN. This authentication protocol will authenticate a user's identity based on their credentials or certificate, which will be verified by their RADIUS authentication server. 802.1X uses the uploaded certificate from the Certificate Repository to verify the user's identity. EAP\_TLS or EAP\_PEAP are two authentication methods used in BCM2 to exchange the secure information. See [Setting Up a TLS Certificate](#) (on page 157) to configure and upload the proper certificate.

## Ethernet (Wired) Interface Settings

On the Network page, click the ETHERNET section if the BCM2 has one port or click ETH1 and ETH2 sections respectively to configure each port. By default, both ETH1 and ETH2 interfaces are enabled.

### ► *Bridging Cascading mode:*

If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings.



► *IPv4 settings:*

<b>Field/setting</b>	<b>Description</b>
<b>Enable IPv4</b>	<b>Enable or disable the IPv4 protocol.</b>
<b>IP auto configuration</b>	<b>Select the method to configure IPv4 settings.</b> <ul style="list-style-type: none"> <li>● <b>DHCP: Auto-configure IPv4 settings via DHCP servers.</b></li> <li>● <b>Static: Manually configure the IPv4 settings.</b></li> </ul>
<b>Preferred hostname</b>	<b>Enter the hostname you prefer for IPv4 connectivity</b>

- DHCP settings: Optionally specify the preferred hostname, which must meet the following requirements:
  - 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
- Static settings:
  - Assign a static IPv4 address, which follows this syntax "IP address/prefix length".  
Example: *192.168.84.99/24*
  - Assign a Default Gateway.

► *IPv6 settings:*

<b>Field/setting</b>	<b>Description</b>
<b>Enable IPv6</b>	<b>Enable or disable the IPv6 protocol.</b>
<b>IP auto configuration</b>	<b>Select the method to configure IPv6 settings.</b> <ul style="list-style-type: none"> <li>● <b>Automatic: Auto-configure IPv6 settings via DHCPv6.</b></li> <li>● <b>Static: Manually configure the IPv6 settings.</b></li> </ul>

<b>Field/setting</b>	<b>Description</b>
<b>Preferred hostname</b>	<ul style="list-style-type: none"> <li>• Enter the hostname you prefer for IPv6 connectivity</li> </ul>

- Automatic settings: Optionally specify the preferred hostname, which must meet the above requirements.
- Static settings:
  - Assign a static IPv6 address, which follows this syntax "IP address/prefix length".  
Example: `fd07:2fa:6cff:1111::0/128`
  - Assign a Default Gateway.

► **Enable Interface:**

Make sure the Ethernet interface is enabled, or all networking through this interface fails. This setting is available in the ETH1/ETH2 or ETHERNET section, but not available in the BRIDGE section.

Enable interface

► **Other Ethernet settings:**

<b>Field</b>	<b>Description</b>
Speed	Select a LAN speed. <ul style="list-style-type: none"> <li>• <i>Auto</i>: System determines the optimum LAN speed through auto-negotiation.</li> <li>• <i>10 MBit/s</i>: Speed is always 10 Mbps.</li> <li>• <i>100 MBit/s</i>: Speed is always 100 Mbps.</li> <li>• <i>1 GBit/s</i>: Speed is always 1 Gbps (1000 Mbps).</li> </ul>
Duplex	Select a duplex mode. <ul style="list-style-type: none"> <li>• <i>Auto</i>: Selects the optimum transmission mode through auto-negotiation.</li> <li>• <i>Full</i>: Data is transmitted in both directions simultaneously.</li> <li>• <i>Half</i>: Data is transmitted in one direction at a time.</li> </ul>
Current state	Show the LAN's current status, including the current speed and duplex mode.
MTU	<ul style="list-style-type: none"> <li>• Set the MTU from 1280 to 1500.</li> </ul>

Field	Description
Enable LLDP	<ul style="list-style-type: none"> <li>• Default is enabled.</li> </ul> <p>When LLDP is enabled, device discovery is possible with LLDP management software that is often present in network switches.</p>
Authentication	<p>Select an authentication method.</p> <ul style="list-style-type: none"> <li>• <i>No Authentication</i>: No authentication data is required.</li> <li>• <i>EAP</i>: BCM2 supports 802.1X (EAP) Network Authentication. You must have a client-side certificate to communicate with the authentication server. Enter required authentication data in the fields that appear.</li> </ul>
Outer authentication	<hr/> <hr/> <p>This field appears when 'EAP' is selected.</p> <hr/> <hr/> <p>There are two authentication methods for EAP.</p> <ul style="list-style-type: none"> <li>• <i>PEAP</i>: A TLS tunnel is established, and an inner authentication method can be specified for this tunnel.</li> <li>• <i>TLS</i>: Authentication between the client and authentication server is performed using TLS certificates.</li> </ul>
Inner authentication	<hr/> <hr/> <p>This field appears when both 'EAP' and 'PEAP' are selected.</p> <hr/> <hr/> <ul style="list-style-type: none"> <li>• <i>MS-CHAPv2</i>: Authentication based on the given password using MS-CHAPv2 protocol.</li> <li>• <i>TLS</i>: Authentication between the client and authentication server is performed using TLS certificates.</li> </ul>
Identity	<hr/> <hr/> <p>This field appears when 'EAP' is selected.</p> <hr/> <hr/> <p>Type your user name.</p>
Password	<hr/> <hr/> <p>This field appears only when 'EAP', 'PEAP' and 'MS-CHAPv2' are all selected.</p> <hr/> <hr/> <p>Type your password.</p>

Field	Description
Client certificate, Client private key, Client private key password	<p>A client certificate is required for two scenarios: (1) EAP+TLS, (2) EAP+PEAP+TLS .</p> <p>PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional.</p> <ul style="list-style-type: none"> <li>Private keys in PKCS#1 and PKCS#8 formats are supported.</li> <li>Client Private Key Password should be entered only when your private key is encrypted with a password.</li> <li>To view the uploaded certificate, click Show Client Certificate.</li> <li>To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.</li> </ul>
CA certificate	<p>This field appears when 'EAP' is selected.</p> <p>CA certificate is required when "Enable verification of TLS certificate chain" is selected by default; and strongly recommended</p>
RADIUS authentication server name	<p>This field appears when 'EAP' is selected.</p> <p>Type the name of the RADIUS server if it is present in the TLS certificate.</p> <ul style="list-style-type: none"> <li>The name must match the fully qualified domain name (FQDN) of the host shown in the certificate</li> </ul> <p>Do not leave this field blank as it reduces security.</p>

Note: Auto-negotiation is disabled after setting both the speed and duplex settings to NON-Auto values, which may result in a duplex mismatch.

- Available settings for the CA Certificate:

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see TLS Certificate Chain.

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox to verify the certificate of the EAP authentication server. Then you must upload the certificate of the issuing CA in the next field.

Field/setting	Description
Browse button	Click this button to import the certificate of the issuing CA. Then you can: <ul style="list-style-type: none"> <li>• Click Show to view the certificate's content.</li> <li>• Click Remove to delete the installed certificate if it is inappropriate.</li> </ul>
Allow expired and not yet valid certificates	<ul style="list-style-type: none"> <li>• Select this checkbox to make the authentication succeed regardless of the certificate's validity period.</li> <li>• After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.</li> </ul>
Allow connection if system clock is incorrect	<p>If powered off for a long time, the system time may be incorrect.</p> <p>When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the network connection to fail.</p> <p>When this checkbox is selected, it will make the network connection successful when the system time is earlier than the firmware build before synchronizing with any NTP server.</p>

## Wireless Network Settings

---



---

Wireless network is not supported for Bridging mode or for Expansion units in port forwarding mode.

---



---

Wireless interface is disabled by default. Enable it to use wireless networking.

On the Network page, click the WIRELESS section to configure wireless and IPv4/IPv6 settings.

### ► *Interface Settings:*

Field/setting	Description
Enable interface	Enable or disable the wireless interface. When disabled, the wireless networking fails.
Hardware state	Check this field to ensure that a wireless USB LAN adapter is detected. If not, verify that the USB LAN adapter is firmly connected or that it is supported.
SSID	Type the name of the wireless access point (AP).
Force AP BSSID	If the BSSID is available, select this checkbox.
BSSID	Type the MAC address of an access point.

Field/setting	Description
MTU	Set the Maximum Transmission Unit from 1280 to 1500.
Enable High Throughput (802.11n)	Enable or disable 802.11n protocol.
Authentication	Select an authentication method. <ul style="list-style-type: none"> <li><i>No Authentication</i>: No authentication data is required.</li> <li><i>PSK</i>: A Pre-Shared Key is required.</li> <li><i>EAP</i>: BCM2 supports 802.1X (EAP) Network Authentication. Enter required authentication data in the fields that appear.</li> </ul>
Pre-Shared Key	<hr/> <hr/> This field appears only when PSK is selected. <hr/> <hr/> Type the PSK string.
Outer authentication	<hr/> <hr/> This field appears when 'EAP' is selected. <hr/> <hr/> There are two authentication methods for EAP. <ul style="list-style-type: none"> <li><i>PEAP</i>: A TLS tunnel is established, and an inner authentication method can be specified for this tunnel.</li> <li><i>TLS</i>: Authentication between the client and authentication server is performed using TLS certificates.</li> </ul>
Inner authentication	<hr/> <hr/> This field appears when both 'EAP' and 'PEAP' are selected. <hr/> <hr/> <ul style="list-style-type: none"> <li><i>MS-CHAPv2</i>: Authentication based on the given password using MS-CHAPv2 protocol.</li> <li><i>TLS</i>: Authentication between the client and authentication server is performed using TLS certificates.</li> </ul>
Identity	<hr/> <hr/> This field appears when 'EAP' is selected. <hr/> <hr/> Type your user name.
Password	<hr/> <hr/> This field appears only when 'EAP', 'PEAP' and 'MS-CHAPv2' are all selected. <hr/> <hr/> Type your password.

Field/setting	Description
Client certificate, Client private key, Client private key password	<p>This field appears when 'EAP', 'PEAP' and 'TLS' are all selected.</p> <p>PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional.</p> <ul style="list-style-type: none"> <li>Private keys of PKCS#1 and PKCS#8 formats are supported.</li> <li>Client Private Key Password should be entered only when your private key is encrypted with a password.</li> <li>To view the uploaded certificate, click Show Client Certificate.</li> <li>To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.</li> </ul>
CA certificate	<p>This field appears when 'EAP' is selected.</p> <p>A third-party CA certificate may or may not be needed. If needed, follow the steps below.</p>
RADIUS authentication server name	<p>This field appears when 'EAP' is selected.</p> <p>Type the name of the RADIUS server if it is present in the TLS certificate.</p> <ul style="list-style-type: none"> <li>The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.</li> </ul>

- Available settings for the CA Certificate:

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see TLS Certificate Chain.

Field/setting	Description
Enable verification of TLS certificate chain	<p>Select this checkbox for the BCM2 to verify the validity of the TLS certificate that will be installed.</p> <ul style="list-style-type: none"> <li>For example, the certificate's validity period against the system time is checked.</li> </ul>
Browse button	<p>Click Browse to import a certificate file. Then you can:</p> <ul style="list-style-type: none"> <li>Click Show to view the certificate's content.</li> <li>Click Remove to delete the installed certificate if it is inappropriate.</li> </ul>



Field/setting	Description
Allow expired and not yet valid certificates	<ul style="list-style-type: none"> <li>• Select this checkbox to make the authentication succeed regardless of the certificate's validity period.</li> <li>• After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.</li> </ul>
Allow connection if system clock is incorrect	<p>When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail.</p> <p>When this checkbox is selected, it will make the wireless network connection successful when the BCM2 system time is earlier than the firmware build before synchronizing with any NTP server.</p>

► *IPv4 settings:*

<i>Field/setting</i>	<i>Description</i>
<i>Enable IPv4</i>	<i>Enable or disable the IPv4 protocol.</i>
<i>IP auto configuration</i>	<i>Select the method to configure IPv4 settings.</i> <ul style="list-style-type: none"> <li>• <i>DHCP: Auto-configure IPv4 settings via DHCP servers.</i></li> <li>• <i>Static: Manually configure the IPv4 settings.</i></li> </ul>
<i>Preferred hostname</i>	<i>Enter the hostname you prefer for IPv4 connectivity</i>

- DHCP settings: Optionally specify the preferred hostname, which must meet the following requirements:
  - 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
- Static settings: Assign a static IPv4 address, which follows this syntax "IP address/prefix length".  
Example: *192.168.84.99/24*

► *IPv6 settings:*

<i>Field/setting</i>	<i>Description</i>
<i>Enable IPv6</i>	<i>Enable or disable the IPv6 protocol.</i>
<i>IP auto configuration</i>	<i>Select the method to configure IPv6 settings.</i> <ul style="list-style-type: none"> <li>• <i>Automatic: Auto-configure IPv6 settings via DHCPv6.</i></li> <li>• <i>Static: Manually configure the IPv6 settings.</i></li> </ul>

<b>Field/setting</b>	<b>Description</b>
<b>Preferred hostname</b>	<ul style="list-style-type: none"> <li>• Enter the hostname you prefer for IPv6 connectivity</li> </ul>

- Automatic settings: Optionally specify the preferred hostname, which must meet the above requirements.
- Static settings: Assign a static IPv6 address, which follows this syntax "IP address/prefix length". Example: `fd07:2fa:6cff:1111::0/128`

► (Optional) To view the wireless LAN diagnostic log:

- Click Show WLAN Diagnostic Log. See [Diagnostic Log for Network Connections](#) (on page 130)



## Diagnostic Log for Network Connections

A diagnostic log for inspecting connection errors that occurred during the EAP authentication or the wireless network connection is provided. The information is useful for technical support.

The diagnostic log shows data only after connection errors are detected.



Each entry in the log consists of:

- ID number
- Date and time
- Description

► *To view the log:*

1. Access the diagnostic log with either method below.
  - Choose Device Settings > Network > ETH1/ETH2 > Show EAP Authentication Log.
  - Choose Device Settings > Network > WIRELESS > Show WLAN Diagnostic Log.
2. The log is refreshed automatically at a regular interval of five seconds.
  - To avoid any new events' interruption during data browsing, you can suspend the automatic update by clicking Pause.
  - To restore automatic update, click Resume. Those new events that have not been listed yet due to suspension will be displayed in the log now.

► *To clear the diagnostic log:*

1. On the top-right corner of the log, click  >  Clear Log .
2. Click Clear Log on the confirmation message.

## Static Route Examples

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

Most of local multiple networks are not directly reachable and require the use of a gateway. Therefore, we will select Gateway in the following examples. If your local multiple networks are directly reachable, you should select Interface rather than Gateway.

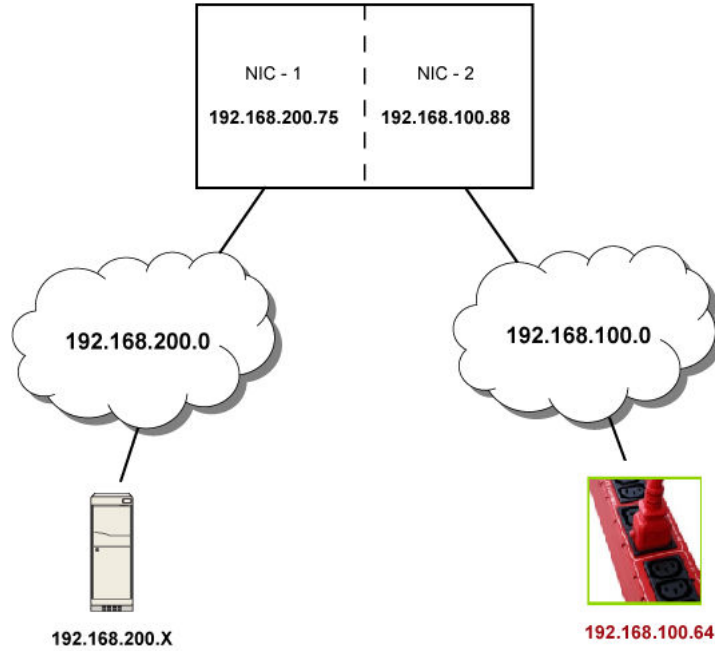
---

Note: If Interface is selected, you should select an interface name instead of entering an IP address.

---

► *IPv4 example:*

- Your BCM2: *192.168.100.64*
- Two NICs: *192.168.200.75* and *192.168.100.88*
- Two networks: *192.168.200.0* and *192.168.100.0*
- Prefix length: *24*






In this example, NIC-2 (192.168.100.88) is the next hop router for your BCM2 to communicate with any device in the other subnet 192.168.200.0.

In the IPv4 "Static Routes" section, you should enter the data as shown below. Note that the address in the first field must be of the Classless Inter-Domain Routing (CIDR) notation.

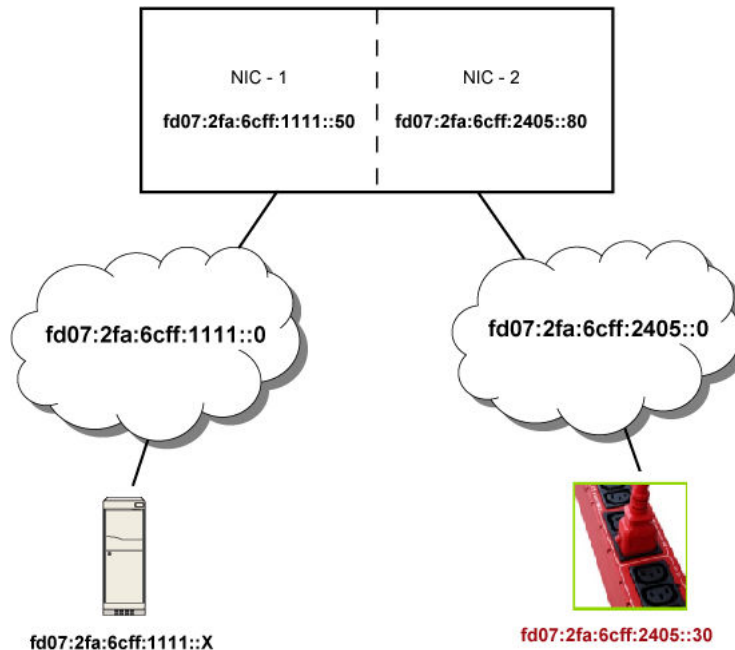
1	192.168.200.0/24	Gateway	192.168.100.88	↑	↓	🗑️
---	------------------	---------	----------------	---	---	----

Tip: If you have configured multiple static routes, you can click on any route and then make changes,

use  or  to re-sort the priority, or click  to delete it.

► *IPv6 example:*

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



In this example, NIC-2 (fd07:2fa:6cff:2405::80) is the next hop router for your BCM2 to communicate with any device in the other subnet fd07:2fa:6cff:1111::0.

In the IPv6 "Static Routes" section, you should enter the data as shown below. Note that the address in the first field must be of the Classless Inter-Domain Routing (CIDR) notation.

1	fd07:2fa:6cff:2405::0/64	Gateway	fd07:2fa:6cff:2405::80	↑	↓	🗑️
---	--------------------------	---------	------------------------	---	---	----

Tip: If you have configured multiple static routes, use the arrow buttons to sort the priority, or click



to delete it.

## Static Route Interface Names

When your local multiple networks are "directly reachable", you should select Interface for static routes. Then choose the interface where another network is connected.

192.168.200.0/24	Interface		↑	↓	🗑️
<ul style="list-style-type: none"> <li>BRIDGE</li> <li>ETH1</li> <li>ETH2</li> <li>WIRELESS</li> </ul>					

► *Interface list:*

<b>Interface name</b>	<b>Description</b>
<b>BRIDGE</b>	<i>When another wired network is connected to the Ethernet port of your BCM2, and your BCM2 has been set to the bridging mode, select this interface name instead of the Ethernet interface.</i>
<b>ETH1</b>	<i>When another wired network is connected to the ETH1 port of your BCM2, select this interface name.</i>
<b>ETH2</b>	<i>When another wired network is connected to the ETH2 port of your BCM2, select this interface name.</i>
<b>WIRELESS</b>	<i>When another wireless network is connected to your BCM2, select this interface name.</i>

## Setting the Cascading Mode

---

---

See the Cascading Solution Guide for full details on network setup, physical setup, and supported configurations for all cascades across products. The sections documented here are a brief overview.

---

---

The cascading mode configured on the primary device determines the Ethernet sharing method, which is either network bridging or port forwarding. The cascading mode of all devices in the chain must be the same.

You must have the Change Network Settings permission to configure the cascading mode.

Note: Port Forwarding mode does not support APIPA.

► *To configure the cascading mode:*

1. Choose Device Settings > Network > Common Network Settings section.
2. Select the preferred mode in the Cascading Mode field.

<b>Mode</b>	<b>Description</b>
<b>None</b>	No cascading mode is enabled. This is the default.
<b>Bridging</b>	Each device in the cascading chain is accessed with a different IP address.
<b>Port Forwarding</b>	Each device in the cascading chain is accessed with the same IP address(es) but with a different port number assigned.

---

*Tip: If selecting Port Forwarding, the Device Information page will show a list of port numbers for all cascaded devices. Choose Maintenance > Device Information > Port Forwarding.*

---

1. For the Port Forwarding mode, you must also configure the following settings.  
Note that if either setting below is incorrectly configured, a networking issue occurs.

Field	Description
<b>Port forwarding role</b> (available on all cascaded devices)	<i>Primary or Expansion.</i> This is to determine which device is the primary and which ones are expansion devices.
<b>Downstream interface</b> (available on the primary device only)	<i>USB or ETH1/ETH2.</i> This is to determine which port on the primary device is connected to Expansion 1. If ETH1 or ETH2 is selected as the downstream interface, make sure the selected Ethernet interface is enabled.

2. (Optional) Configure the network settings by clicking the BRIDGE, ETH1/ETH2, or WIRELESS section on the same page.
  - In the Bridging mode, each cascaded device can have different network settings. You may need to configure each device's network settings in the BRIDGE section.
  - In the Port Forwarding mode, all cascaded devices share the primary device's network settings. You only need to configure the primary device's network settings in the ETH1/ETH2 and/or WIRELESS section.

---

*Tip: You can enable/configure multiple network interfaces in the Port Forwarding mode so that the cascading chain has multiple IP addresses.*

---

3. Click Save.

► **Recommendations for cascade loops:**

You can connect both the first and the last PDU to your network (cascade loop) under the following conditions:

- Bridging mode only.
  - The remaining network MUST use R/STP to avoid network loops.
- AND
- Both the first and the last PDUs MUST either attach to the same switch or, if they are attached to two separate switches, you must configure both ports of these switches so that the STP costs are high. This prevents the STP protocol from sending unrelated traffic through the PDU cascade, which can cause bottlenecks that lead to connectivity issues in the whole network.

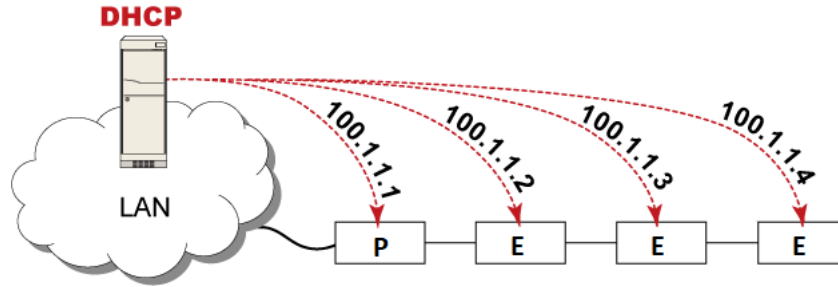
### Cascading Modes Overview

The cascading mode is a network configuration setting that determines how each device in the chain is accessed.

There are two cascading modes: Bridging and Port Forwarding.

In the following illustration, it is assumed that users enable the DHCP networking for the cascading chain comprising four devices. In the diagrams, "P" is the primary device and "E" is an expansion device.

► **"Bridging" mode:**

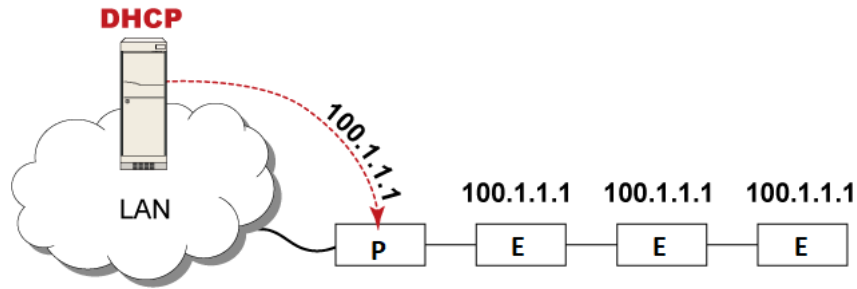


***In this mode, the DHCP server communicates with every cascaded device respectively and assigns four different IP addresses. Each device has its own IP address.***

***The way to remotely access each cascaded device is completely the same as accessing a standalone device in the network.***



► "Port Forwarding" mode:



***In this mode, the DHCP server communicates with the primary device alone and assigns one IP address to the primary device. All expansion devices share the same IP address as the primary device.***

***You must specify a 5XXXX port number (where X is a number) when remotely accessing any expansion device with the shared IP address. See [Port Number Syntax](#) (on page 137).***

► Comparison between cascading modes:

- The Bridging mode supports the wired network only, while the Port Forwarding mode supports both wired and wireless networks.
- Both cascading modes support a maximum of 32 devices in a chain.
- Both cascading modes support both DHCP and static IP addressing.
- In the Bridging mode, each cascaded device has a unique IP address.

In the Port Forwarding mode, all cascaded devices share the same IP address(es) as the primary device.

- In the Bridging mode, each cascaded device has only one IP address.

In the Port Forwarding mode, each cascaded device can have multiple IP addresses as long as the primary device has multiple network interfaces enabled/configured properly.

For example:

- When the primary device has two Ethernet ports (ETH1/ETH2), you can enable ETH1, ETH2 and WIRELESS interfaces so that the Port-Forwarding chain has two wired IP addresses and one wireless IP address.

### Port Number Syntax

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

- Primary device: The port number is either 5NNXX or the standard TCP/UDP port.
- Expansion device: The port number is 5NNXX.

► 5NNXX port number syntax:

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

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

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

Position	XX	Position	XX
Primary device	00	Expansion 8	08
Expansion 1	01	Expansion 9	09
Expansion 2	02	Expansion 10	10
Expansion 3	03	Expansion 11	11
Expansion 4	04	Expansion 12	12
Expansion 5	05	Expansion 13	13
Expansion 6	06	Expansion 14	14
Expansion 7	07	Expansion 15	15

For example, to access the Expansion 4 device via Modbus/TCP, the port number is 50604.

---

Tip: The full list of each cascaded device's port numbers can be retrieved from the web interface. Choose Maintenance > Device Information > Port Forwarding.

---

► *Standard TCP/UDP ports:*

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

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

Protocols	Port Numbers
MODBUS	502

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

## Port Forwarding Examples

*In this example, Port Forwarding mode is applied to a cascading chain comprising three devices. The IP address is 192.168.84.77.*

### ► Primary device:

Position code for the primary device is '00' so each port number is 5NN00 as listed below.

Protocols	Port numbers
HTTPS	50000
HTTP	50100
SSH	50200
TELNET	50300
SNMP	50500
MODBUS	50600

Examples using "5NN00" ports:

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

Examples using standard TCP/UDP ports:

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

► *Expansion 1 device:*

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

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

Examples:

- To access Expansion 1 via HTTPS, the IP address is:  
*https://192.168.84.77:50001/*
- To access Expansion 1 via HTTP, the IP address is:  
*http://192.168.84.77:50101/*
- To access Expansion 1 via SSH, the command is:  
*ssh -p 50201 192.168.84.77*

► *Expansion 2 device:*

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

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

Examples:

- To access Expansion 2 via HTTPS, the IP address is:  
*https://192.168.84.77:50002/*
- To access Expansion 2 via HTTP, the IP address is:

*http://192.168.84.77:50102/*

- To access Expansion 2 via SSH, the command is:  
*ssh -p 50202 192.168.84.77*

## Adding, Removing or Swapping Cascaded Devices

Change a device's cascading mode first before adding that device to a cascading chain, or before disconnecting that device from the chain.

If you only want to change the cascading mode of an existing chain, or swap the primary and expansion device, always start from the expansion device.

---

Note: If the following procedures are not followed, a networking issue occurs. When a networking issue occurs, check the cascading connection and/or software settings of all devices in the chain.

---

### ► *To add a device to an existing chain:*

1. Connect the device you will cascade to the LAN and find its IP address, or connect it to a computer.
2. Log in to this device and set its cascading mode to be the same as the existing chain's cascading mode.
3. (Optional) If this device will function as an expansion device, disconnect it from the LAN after configuring the cascading mode.
4. Connect this device to the chain, using either a USB or Ethernet cable.

### ► *To remove a device from the chain:*

1. Log in to the desired cascaded device, and change its cascading mode to None.

---

*Exception: If you are going to connect the removed device to another cascading chain, set its cascading mode to be the same as the mode of another chain.*

---

2. Now disconnect it from the cascading chain.

### ► *To swap the primary and expansion device:*

- In the Bridging mode, you can swap the primary and expansion devices by disconnecting ALL cascading cables from them, and then reconnecting cascading cables. No changes to software settings are required.
- In the Port Forwarding mode, you must follow the procedure below:

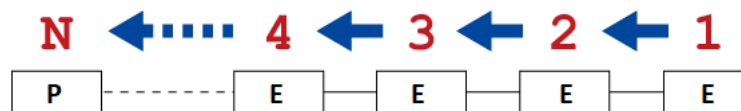
- a. Access the expansion device that will replace the primary device, and set its role to 'Primary', and correctly set the downstream interface.
- b. Access the primary device, set its role to 'Expansion'.
- c. Swap the primary and expansion device now.
  - You must disconnect the LAN cable and ALL cascading cables connected to the two devices first before swapping them, and then reconnecting all cables.

► *To change the cascading mode applied to a chain:*

1. Access the last expansion device, and change its cascading mode.
  - If the new cascading mode is 'Port Forwarding', you must also set its role to 'Expansion'.
2. Access the second to last, third to last and so on until the first expansion device to change their cascading modes one by one.
3. Access the primary device, and change its cascading mode.
  - If the new cascading mode is 'Port Forwarding', you must also set its role to 'Primary', and correctly select the downstream interface.

The following diagram indicates the correct sequence. 'N' is the final one.

- P = Primary device
- E = Expansion device



## Configuring Network Services

BCM2 supports the following network communication services.

Network Services
HTTP
SNMP
SMTP Server
SSH
Telnet
Modbus
Redfish
Service Advertising

HTTPS and HTTP enable the access to the web interface. Telnet and SSH enable the access to the command line interface.

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.

---

**Important: BCM2 uses TLS rather than SSL.**

---

## Changing HTTP(S) Settings

HTTPS uses Transport Layer Security (TLS) technology to encrypt all traffic to and from the BCM2 so it is a more secure protocol than HTTP. BCM2 disables TLS 1.0 and 1.1 by default. It enables only TLS 1.2 and 1.3.

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

### ► *HTTP and HTTPS settings:*

1. Choose Device Settings > Network Services > HTTP.
2. HTTP settings:
  - Enable or disable HTTP access.
  - Default port is 80. You can enter a custom port.
  - Enforce use of HTTPS: Select the checkbox to Redirect HTTP connections to HTTPS.
3. HTTPS settings:

- Enable or disable HTTPS access.
- Enable HSTS: Default is enabled.
- Default port is 443. You can enter a custom port.

---

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

---

► *Special note for AES ciphers:*

*The BCM2 device's TLS-based protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between BCM2 and the client (such as a web browser), which is impacted by the cipher priority of BCM2 and the client's cipher availability/settings.*

---

Tip: To force BCM2 to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings. For example, you can enable a cipher and disable the other in the browser via the "about:config" command.

---

## Regaining Access with HSTS and Expired Certificate

HSTS is enabled by default in the Device Settings > Security > HTTP settings. When HSTS is enabled, you can only access BCM2 via web browser when a valid, unexpired certificate is installed. HSTS removes the ability for users to click through warnings about invalid certificates.

If access is lost due to HSTS restrictions, there are 2 methods to regain access.

► *Replace the certificate locally on the BCM2:*

1. Save the new key and certificate to a USB drive.
2. Use one of the USB configuration methods to upload the new certificate to the device.

► *Replace the certificate over an insecure connection:*

1. Disable the client web browser HSTS security, and then access the BCM2 "insecurely."
2. Replace the certificate in Device Settings > Security > TLS Certificates, then enable the HSTS security.

## Configuring SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the BCM2. Enabling SNMP communication allows the manager to retrieve and even control the power status of each outlet.

You may also 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 175).

► *To configure SNMP communication:*

1. Choose Device Settings > Network Services > SNMP.



SNMP Agent	
Enable SNMP v1 / v2c	<input type="checkbox"/>
Read community string	public
Write community string	
Enable SNMP v3	<input type="checkbox"/>
MIB-II System Group	
sysContact	
sysName	
sysLocation	
SNMP Notifications	
Enable SNMP notifications	<input checked="" type="checkbox"/>
Notification type	SNMPv3 trap
Engine ID	0x800035ae808172c7c4e307523e5f3d3503ed99dcd3bec366a324c5d9c9e163a3
Host	required
Port	162
User ID	required
Security level	authPriv
Authentication protocol	SHA-1
Authentication passphrase	required
Confirm authentication passphrase	required
Privacy protocol	AES-128
Privacy passphrase	required
Confirm privacy passphrase	required
Download MIBs	

2. Enable or disable "SNMP v1 / v2c" and/or "SNMP v3" by clicking the corresponding checkbox.
  - The SNMP v1/v2c read-only access is enabled by default. The default 'Read community string' is "public."
  - To enable read-write access, type the 'Write community string.' Usually the string is "private."
3. Enter the MIB-II system group information, if applicable.
  - sysContact - the contact person in charge of the system
  - sysName - the name assigned to the system
  - sysLocation - the location of the system
4. To configure SNMP notifications:
  - a. Select the 'Enable SNMP notifications' checkbox.
  - b. Select a notification type -- SNMPv2c trap, SNMPv2c inform, SNMPv3 trap, and SNMPv3 inform.
  - c. Specify the SNMP notification destinations and enter necessary information. For details, refer to:
    - SNMPv2c Notifications
    - SNMPv3 Notifications

---

*Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. To add more than three SNMP destinations, you can create new SNMP notification actions.*

---

5. You must download the SNMP MIB for your BCM2 to use with your SNMP manager.
  - a. Click the Download MIBs title bar to show the download links.



- b. Click the PDU2-MIB download link. See Downloading SNMP MIB.
6. Click Save.

## Configuring SMTP Settings

The BCM2 can be configured to send alerts or event messages to a specific administrator by email. To send emails, 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.

### ► To set SMTP server settings:


1. Choose Device Settings > Network Services > SMTP Server.
2. Enter the information needed.

Field	Description
IP address/host name	Type the name or IP address of the mail server.
Port	Type the port number. <ul style="list-style-type: none"><li>• Default is 25</li></ul>
Sender email address	Type an email address for the sender.
Number of sending retries	Type the number of email retries. <ul style="list-style-type: none"><li>• Default is 2 retries</li></ul>
Time between sending retries	Type the interval between email retries in minutes. <ul style="list-style-type: none"><li>• Default is 2 minutes.</li></ul>
Server requires authentication	Select this checkbox if your SMTP server requires password authentication.
User name, Password	Type a user name and password for authentication after selecting the above checkbox. <ul style="list-style-type: none"><li>• The length of user name and password ranges between 4 and 64. Case sensitive.</li><li>• Spaces are not allowed for the user name, but allowed for the password.</li></ul>

Field	Description
Enable SMTP over TLS (StartTLS)	If your SMTP server supports the Transport Layer Security (TLS), select this checkbox.

- Settings for the CA Certificate:

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see TLS Certificate Chain.

Field/setting	Description
	Click this button to import a certificate file. Then you can: <ul style="list-style-type: none"> <li>• Click Show to view the certificate's content.</li> <li>• Click Remove to delete the installed certificate if it is inappropriate.</li> </ul>
Allow expired and not yet valid certificates	<ul style="list-style-type: none"> <li>• Select this checkbox to make the authentication succeed regardless of the certificate's validity period.</li> <li>• After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.</li> </ul>

3. Now that you have set the SMTP settings, you can test it to ensure it works properly.
  - 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.
4. Click Save.

► *Special note for AES ciphers:*

*The BCM2 device's TLS-based protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between BCM2 and the client (such as a web browser), which is impacted by the cipher priority of BCM2 and the client's cipher availability/settings.*

---

Tip: To force BCM2 to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

---

## Changing SSH Settings

You can enable or disable the SSH access to the command line interface, change the TCP port, or set a password or public key for login over the SSH connection.

► *To change SSH settings:*

1. Choose Device Settings > Network Services > SSH.
2. To enable or disable the SSH access, select or deselect the checkbox.
3. To use a different port, type a port number.
4. Select one of the authentication methods.
  - *Password authentication only:* Enables the password-based login only.
  - *Public key authentication only:* Enables the public key-based login only. You must enter a valid SSH public key for each user profile to log in over the SSH connection.
  - *Password and public key authentication:* Enables both the password- and public key-based login. This is the default.
5. Click Save.

## Changing Telnet Settings

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

► *To change Telnet settings:*

1. Choose Device Settings > Network Services > Telnet.
2. To enable the Telnet access, select the checkbox.
3. To use a different port, type a new port number.
4. Click Save.

## Changing Modbus Settings

The BCM2 supports both the Modbus/TCP and Modbus Gateway features. Enable either or both Modbus features according to your needs.

► *Modbus/TCP Access:*

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

1. Choose Device Settings > Network Services > Modbus.
2. To enable the Modbus/TCP access, select the Enable Modbus/TCP access checkbox.
3. To use a different port, type a new port number.
4. To enable the Modbus read-only mode, select the "Enable read-only mode" checkbox. To enable the read-write mode, deselect it.

► *Modbus Gateway:*

You can connect Raritan's USB-MOD-DONGLE to the USB-A Port of the BCM2 and the green connector to an external third-party device terminal. The gateway service runs on a dedicated TCP port and forwards incoming requests to the Modbus/RTU bus. Enable the Modbus Gateway feature and configure the Modbus gateway service independent of the Modbus/TCP service. The Modbus TCP clients on your network will be able to communicate with the Modbus RTU devices connected to BCM2.

Once configured, connected devices appear in the Peripherals page.



1. To allow the Modbus TCP clients on the network to communicate with the Modbus RTU devices connected to the BCM2, select the 'Enable Modbus gateway' checkbox.

Modbus Gateway	
Enable Modbus gateway	<input type="checkbox"/>
TCP port	503
Parity	Even ▼
Line speed	19200 ▼
Default address	1

2. Now configure the fields shown.

Field	Description
<b>TCP port</b>	Use the default port 503, or assign a different port. Valid range is 1 to 65535. <hr/> <b>Note:</b> Port 502 is the default Modbus/TCP port for BCM2, so you cannot use that port for the Modbus Gateway. <hr/>
<b>Parity, Line speed</b>	Use the default values, or update if the Modbus RTU devices are using different communication parameters.

Field	Description
<b>Default address</b>	<p>If the Modbus TCP client does not support Modbus RTU unit identifier addressing, enter a Default Address.</p> <p>If you must provide a unit identifier address:</p> <ul style="list-style-type: none"> <li>• Only one Modbus RTU device is supported.</li> <li>• The unit identifier address you provide is applied to the Modbus RTU device connected to BCM2.</li> </ul> <p>Note that each Modbus RTU device's unit identifier address must be unique.</p> <hr/> <p>Warning: If the connected Modbus RTU device's address does not match the address entered in this field, communications between the Modbus TCP clients and Modbus RTU device fail.</p> <hr/>

## Enabling Redfish Services

You can enable or disable the Redfish services to manage the device through the Redfish API. By default, this service is enabled.

Enabling Redfish services allows you to retrieve the following details.

- configuration details, such as thresholds, names, etc.
- metric readings
- event polling

It also allows you to do the following actions

- power actions
- unit control, such as restart

---

Note: Go to the online Support page for your product to find full documentation of the Redfish API.

---

### ► *To enable or disable Redfish:*

Choose Device Settings > Network Services > Redfish.

## Enabling Service Advertising

The BCM2 advertises all enabled services that are reachable using the IP network. This feature uses DNS-SD (Domain Name System-Service Discovery) and MDNS (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

By default, this feature is enabled.

Enabling this feature also enables Link-Local Multicast Name Resolution (LLMNR) and/or MDNS, which are required for resolving APIPA host names. See APIPA and Link-Local Addressing.

The service advertisement feature supports both IPv4 and IPv6 protocols.

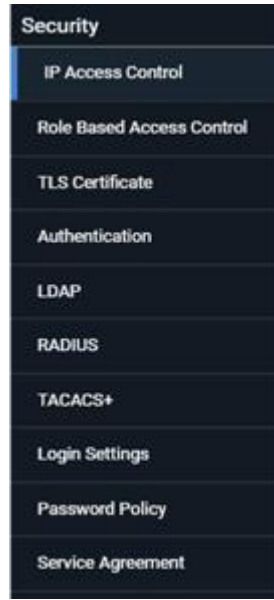
If you have set a preferred host name for IPv4 and/or IPv6, that host name can be used as the zero configuration .local host name, that is, *<preferred\_host\_name>.local*, where *<preferred\_host\_name>* is the preferred host name you have specified for BCM2. The IPv4 host name is the first priority.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

### ► *To enable or disable service advertising:*

1. Choose Device Settings > Network Services > Service Advertising.
2. To enable the service advertising, select either or both checkboxes.
  - To advertise via MDNS, select the Multicast DNS checkbox.
  - To advertise via LLMNR, select the Link-Local Multicast Name Resolution checkbox.
3. Click Save.

## Configuring Security Settings

The BCM2 provides tools to control access. You can enable the internal firewall, create firewall rules, and set login limitations. In addition, you can create and install the certificate or set up external authentication servers for access control. This product supports SHA-2 TLS certificates.



## Creating IP Access Control Rules

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

- Rule order is important.  
When traffic reaches or is sent from the BCM2, 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.
- Prefix length is required.  
When typing the IP address, you must specify it in the CIDR notation. That is, BOTH the address and the prefix length are included. For example, to specify a single address with the 24-bit prefix length, use this format:  
*x.x.x.x/24*  
*/24* = the prefix length.

---

*Note: Valid IPv4 addresses range from 0.0.0.0 through 255.255.255.255.*

---

► *To configure IPv4 or IPv6 access control rules:*

1. Choose Device Settings > Security > IP Access Control.
2. Select the 'Enable IPv4 access control' or "Enable IPv6 access control" checkboxes to enable the access control rules.
3. For either type, determine the default policy.



- *Accept*: Accepts traffic from all IPv4 OR IPv6 addresses.
  - *Drop*: Discards traffic from all IPv4 OR IPv6 addresses, without sending any failure notification to the source host.
  - *Reject*: Discards traffic from all IPv4 OR IPv6 addresses, and an ICMP message is sent to the source host for failure notification.
4. Go to the Inbound Rules section or the Outbound Rules section according to your needs.
    - Inbound rules control the data sent to the BCM2.
    - Outbound rules control the data sent from the BCM2.
  5. Create rules.
    - Click Append to add a row, then add the IP address and subnet mask. Select Policy. For each rule, the policy affects only the specified IP address.
    - Click Insert Above to add a rule above another rule.
    - The system automatically numbers the rules.
    - Use the arrow buttons to sort the priority order.
  6. Click Save. The rules are applied. Make sure to click Save in each section if changes are made.

**IPv4**

Enable IPv4 access control

---

**Inbound Rules**

Default policy: Drop ▼

#	IP/Mask	Policy	
1	192.168.8.8/32	Accept	
2	192.168.28.33/24	Drop	
3	192.168.53.38/24	Reject	

Append    Insert Above

---

**Outbound Rules**

Default policy: Accept ▼

#	IP/Mask	Policy	
1	192.168.89.100/24	Drop	

Append    Insert Above

## Editing or Deleting IP Access Control Rules

When an existing IP access control rule requires updates of IP address range and/or policy, modify them accordingly. Or you can delete any unnecessary rules.

► *To modify or delete a rule:*

1. Choose Device Settings > Security > IP Access Control.
2. Go to the IPv4 or IPv6 section.
3. Select the desired rule in the list.
  - Ensure the IPv4 or IPv6 checkbox has been selected, or you may not edit or delete any rule.
4. Perform the desired action.

- Click  to remove it.

- To re-sort its order, click  or .

5. Click Save.
  - IPv4 rules: Make sure you click the Save button in the IPv4 section, or the changes made to IPv4 rules are not saved.
  - IPv6 rules: Make sure you click the Save button in the IPv6 section, or the changes made to IPv6 rules are not saved.

## Creating Role Based Access Control Rules

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

Same as IP access control rules, the order of role-based access control rules is important, since the rules are executed in numerical order.

► *To create IPv4 role-based access control rules:*

1. Choose Device Settings > Security > Role Based Access Control.
2. Select the 'Enable role based access control for IPv4' checkbox to enable IPv4 access control rules.
3. Determine the IPv4 default policy.
  - *Accept*: Accepts traffic when no matching rules are present.
  - *Deny*: Rejects any user's login attempt when no matching rules are present.
4. Create rules. Refer to the tables below for different operations.

**ADD a rule to the end of the list**

- Click Append.
- Type a starting IP address in the Start IP field.
- Type an ending IP address in the End IP field.
- Select a role in the Role field. This rule applies to members of this role only.
- Select an option in the Policy field.
  - *Accept*: Accepts traffic from the specified IP address range when the user is a member of the specified role.
  - *Deny*: Rejects the login attempt of a user from the specified IP address range when that user is a member of the specified role.

#### INSERT a rule between two rules

- 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 Above.
- Type a starting IP address in the Start IP field.
- Type an ending IP address in the End IP field.
- Select a role in the Role field. This rule applies to members of this role only.
- Select *Accept* or *Deny* in the Policy field. Refer to the above table for details.

The system automatically numbers the rule.

5. When finished, the rules are listed on this page.

- You can select any existing rule and then click  or  to change its priority.

IPv4

Enable IPv4 access control

Inbound Rules

Default policy Drop

#	IP/Mask	Policy	
1	192.168.8.34/24	Drop	↑ ↓ 🗑️
2	192.168.28.33/32	Accept	

Append Insert Above

Outbound Rules

Default policy Accept

#	IP/Mask	Policy
no rules defined		

Append Insert Above

Save

6. Click Save. The rules are applied.

► *To configure IPv6 access control rules:*

1. On the same page, select the 'Enable role based access control for IPv6' checkbox to enable IPv6 access control rules.
2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.
3. Make sure you click the Save button in the IPv6 section, or the changes made to IPv6 rules are not saved.

## Editing or Deleting Role Based Access Control Rules

You can modify existing rules to update their roles/IP addresses, or delete them when they are no longer needed.

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

1. Choose Device Settings > Security > Role Based Access Control.
2. Go to the IPv4 or IPv6 section.
3. Select the desired rule in the list.
  - Ensure the IPv4 or IPv6 checkbox has been selected, or you may not edit or delete any rule.
4. Perform the desired action.

- Make changes to the selected rule, and then click Save.



- Click  to remove it.



- To resort its order, click  or .

5. Click Save.

- IPv4 rules: Make sure you click the Save button in the IPv4 section, or the changes made to IPv4 rules are not saved.
- IPv6 rules: Make sure you click the Save button in the IPv6 section, or the changes made to IPv6 rules are not saved.

## Setting Up a TLS Certificate

### ► To obtain a CA-signed certificate:

1. Create a Certificate Signing Request (CSR) in Device Settings > TLS Certificates.
2. Submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with a certificate.
3. Install the CA-signed certificate onto the BCM2.

---

Note: If you are using a certificate that is part of a chain of certificates, each part of the chain is signed during the validation process. You can upload active and pending certificates and private keys saved in PEM format on a flash drive.

---

### ► A CSR is not required in either scenario below:

- Make the BCM2 create a *self-signed* certificate.
- Appropriate, valid certificate and key files are already available, and you only need to import them.

### Creating a TLS Certificate or CSR

Follow this procedure to create the CSR.

### ► To create a CSR:

1. Choose Device Settings > Security > TLS Certificate.
2. In the New CSR section, provide the information requested.
  - Subject:

Field	Description
Country	The country where your company is located. Use the standard ISO country code, which comprises two uppercase letters. For a list of ISO codes, google ISO 3166 country codes.
State or province	The full name of the state or province where your company is located.
Locality	The city where your company is located.

Field	Description
Organization	The registered name of your company.
Organizational unit	The name of your department.
Common name	The fully qualified domain name (FQDN) of your BCM2.
Email address	An email address where you or another administrative user can be reached.

---

**Warning:** If you generate a CSR without values entered in the required fields, you cannot obtain third-party certificates.

---

- Subject Alternative Names:

If you want a certificate to secure multiple hosts across different domains or subdomains, you can add additional DNS host names or IP addresses of the wanted hosts to this CSR so that a single certificate will be valid for all of them.

Click Add Name when there are more than one additional hosts to add.

- Examples of subject alternative names: *support.raritan.com*, *help.raritan.com*, *help.raritan.net*, and *192.168.77.50*.

- Key Creation Parameters:

Field	Description
Key Type/Key Length	Key type RSA requires you to select Key Length: <ul style="list-style-type: none"> <li>• 2048 bits</li> <li>• 3072 bits</li> </ul>
Key Type/Elliptic Curve	Key type ECDSA requires you to select the elliptic curve: <ul style="list-style-type: none"> <li>• NIST-P-256</li> <li>• NIST P-384</li> <li>• NIST P-521</li> </ul>
Self-sign	For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.
Challenge, Confirm challenge	Type a password. The password is used to protect the certificate or CSR. The value should be 4 to 64 characters long. Case sensitive.

1. Click Create CSR to create both the CSR and private key. This may take several minutes to complete.
2. Click Download Certificate Signing Request to download the CSR to your computer.
  - a. You are prompted to open or save the file. Click Save to save it onto your computer.
  - b. Submit it to a CA to obtain the digital certificate.
  - c. If the CSR contains incorrect data, click Delete Certificate Signing Request to remove it, and then repeat the above steps to re-create it.
1. To store the newly-created private key on your computer, click Download Key in the New TLS Certificate or CSR section.

---

*Note: The Download Key button in the Active TLS Certificate section is for downloading the private key of the currently-installed certificate rather than the newly-created one.*

---

- You are prompted to open or save the file. Click Save to save it onto your computer.

### Installing a CA-Signed Certificate

To get a certificate from a certificate authority (CA), first create a CSR and send it to the CA. See [Creating a TLS Certificate or CSR](#) (on page 157).

After receiving the CA-signed certificate, install it onto the BCM2.

► *To install the CA-signed certificate:*

1. Choose Device Settings > Security > TLS Certificate.
2. Click Browse to navigate to the CA-signed certificate file in the New TLS Certificate or CSR section.
3. Click Upload to upload the certificate.
4. Once complete, do the following:
  - a. Double check the data shown in the New TLS Certificate or CSR section.
  - b. If correct, click "Install Key and Certificate" to install the CA-signed certificate and private key.

---

*Tip: To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.*

---

If incorrect, click "Delete Key and Certificate" to remove the CA-signed certificate and private key, and then repeat the above steps to re-create them.

5. (Optional) To download the CA-signed certificate and/or private key, click Download Certificate or Download Key in the New TLS Certificate section.
  - You are prompted to open or save the file. Click Save to save it onto your computer.

---

*Note: The Download Key button in the Active TLS Certificate section is for downloading the private key of the currently-installed certificate rather than the newly-created one.*

---

6. To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.

### Creating a Self-Signed Certificate

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

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

1. Choose Device Settings > Security > TLS Certificate.
2. Enter information.

Field	Description
Country	The country where your company is located. Use the standard ISO country code, which comprises two uppercase letters. For a list of ISO codes, google ISO 3166 country codes.
State or province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational unit	The name of your department.
Common name	The fully qualified domain name (FQDN) of your BCM2.
Email address	An email address where you or another administrative user can be reached.
Generate Key in Secure Element	<ul style="list-style-type: none"> <li>• This field appears for supported hardware only. Select this checkbox to allow the key to be generated within the Secure Element of the controller.</li> </ul>
Key Type/Key Length	Key type RSA requires you to select Key Length: <ul style="list-style-type: none"> <li>• 2048 bits</li> <li>• 3072 bits</li> </ul>
Key Type/Elliptic Curve	Key type ECDSA requires you to select the elliptic curve: <ul style="list-style-type: none"> <li>• NIST-P-256</li> <li>• NIST P-384</li> <li>• NIST P-521</li> </ul>
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.

A password is not required for a self-signed certificate so the Challenge and Confirm Challenge fields disappear.

3. Click Create Self-Signed Certificate to create both the self-signed certificate and private key. This may take several minutes to complete and saved.
4. Once complete, do the following:
  - a. Double check the data shown in the New TLS Certificate or CSR section.
  - b. If correct, click "Install Key and Certificate" to install the self-signed certificate and private key.

---

*Tip: To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.*

---



If incorrect, click "Delete Key and Certificate" to remove the self-signed certificate and private key, and then repeat the above steps to re-create them.

5. (Optional) To download the self-signed certificate and/or private key, click Download Certificate or Download Key in the New TLS Certificate section.
  - You are prompted to open or save the file. Click Save to save it onto your computer.

---

*Note: The Download Key button in the Active TLS Certificate section is for downloading the private key of the currently-installed certificate rather than the newly-created one.*

---

## Installing or Downloading Existing Certificate and Key

You can download the already-installed certificate and private key from any BCM2 for backup or file transfer. For example, you can install the files onto a replacement BCM2, add the certificate to your browser and so on.

If valid certificate and private key files are already available, you can install them on the BCM2 without going through the process of creating a CSR or a self-signed certificate.

---

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

---

### ► To download active key and certificate files from BCM2:

1. Choose Device Settings > Security > TLS Certificate.
2. In the *Active TLS Certificate* section, click Download Key and Download Certificate respectively.

---

*Note: The Download Key button in the New TLS Certificate section, if present, is for downloading the newly-created private key rather than the one of the currently-installed certificate.*

---

3. You are prompted to open or save the file. Click Save to save it onto your computer.

### ► To install available key and certificate files onto BCM2:

1. Choose Device Settings > Security > TLS Certificate.
2. Select the "Upload key and certificate" checkbox at the bottom of the page.
3. The 'Key File' and 'Certificate file' buttons appear. Click each button to select the key and/or certificate file.
4. Click Upload. The selected files are installed.
5. To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.

## Setting Up External Authentication

---

**Important:** Make sure your network infrastructure uses TLS rather than SSL.

---

BCM2 supports the following authentication mechanisms:

- Local user database
- LDAP
- RADIUS
- TACACS+

Local authentication is the default method. If you use this method, you only need to create user accounts. See [User Management](#) (on page 109).

If you prefer external authentication, you must provide information about the external Authentication and Authorization (AA) server.

If both local and external authentication is needed, create user accounts on the BCM2 in addition to providing the external AA server data.

When configured for external authentication, all users must have an account on the external AA server. Local-authentication-only users will have no access to the BCM2 except for the admin, who always can access.

If the external authentication fails, an "Authentication failed" message is displayed. Details regarding the authentication failure are available in the event log.

You must have the "Change Authentication Settings" permission to configure or modify the authentication settings.

### Adding LDAP/LDAPS Servers

To use LDAP authentication, enable it in the Device Settings > Authentication page, and enter the information about the LDAP server in the LDAP page.

---

Note: If the BCM2 clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, may be considered expired. To ensure proper synchronization, administrators should configure the BCM2 and the LDAP server to use the same NTP server(s).

---

► *To add LDAP/LDAPS servers:*

1. Choose Device Settings > Security > LDAP.
2. Click New.
3. Enter information.

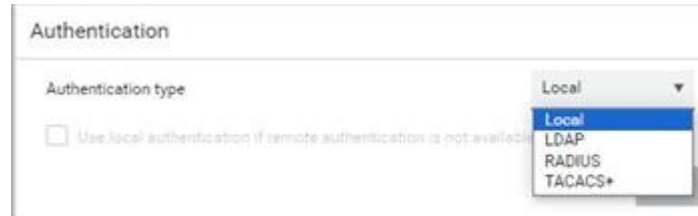
Field/setting	Description
IP address / hostname	The IP address or hostname of your LDAP/LDAPS server. <ul style="list-style-type: none"> <li>• Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.</li> </ul>
Copy settings from existing LDAP server	This checkbox appears only when there are existing AA server settings on the BCM2. To duplicate any existing AA server's settings, refer to the duplicating procedure below.

Field/setting	Description
Type of LDAP server	Choose one of the following options: <ul style="list-style-type: none"> <li>• OpenLDAP</li> <li>• Microsoft Active Directory.</li> </ul>
Security	Determine whether you would like to use Transport Layer Security (TLS) encryption, which allows the BCM2 to communicate securely with the LDAPS server. Three options are available: <ul style="list-style-type: none"> <li>• StartTLS</li> <li>• TLS</li> <li>• None</li> </ul>
Port (None/StartTLS)	<ul style="list-style-type: none"> <li>• The default Port is 389. Either use the standard LDAP TCP port or specify another port.</li> </ul>
Port (TLS)	Configurable only when "TLS" is selected in the Security field. The default is 636. Either use the default port or specify another one.
Enable verification of LDAP server certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the BCM2 prior to the connection. If the certificate validation fails, the connection is refused.
CA certificate	Consult your AA server administrator to get the CA certificate file for the LDAPS server. Click Browse to select and install the certificate file. <ul style="list-style-type: none"> <li>• Click Show to view the installed certificate's content.</li> <li>• Click Remove to delete the installed certificate if it is inappropriate.</li> </ul> <hr/> <p><i>Note: If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see TLS Certificate Chain.</i></p> <hr/>
Allow expired and not yet valid certificates	<ul style="list-style-type: none"> <li>• Select this checkbox to make the authentication succeed regardless of the certificate's validity period.</li> <li>• After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.</li> </ul>
Anonymous bind	Use this checkbox to enable or disable anonymous bind. <ul style="list-style-type: none"> <li>• To use anonymous bind, select this checkbox.</li> <li>• When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.</li> </ul>
Bind DN	Required after deselecting the Anonymous Bind checkbox. Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base.
Bind password, Confirm bind password	Required after deselecting the Anonymous Bind checkbox. Enter the Bind password.

Field/setting	Description
Base DN for search	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search. <ul style="list-style-type: none"> <li>• Example: <code>ou=dev,dc=example,dc=com</code></li> </ul>
Login Name Attribute	The attribute of the LDAP user class which denotes the login name. <ul style="list-style-type: none"> <li>• Usually it is the <code>uid</code>.</li> </ul>
User entry object class	The object class for user entries. <ul style="list-style-type: none"> <li>• Usually it is <code>inetOrgPerson</code>.</li> </ul>
User search subfilter	Search criteria for finding LDAP user objects within the directory tree.
Group lookup using memberOf attribute	<ul style="list-style-type: none"> <li>• Select this checkbox to determine group membership by consulting the user's memberOf attribute(s).</li> <li>• Deselect this checkbox to determine group membership by doing a non-recursive search for groups containing the user's DN as member.</li> </ul>
Group member attribute	<ul style="list-style-type: none"> <li>• Required only when "Group lookup using memberOf attribute" is not selected.</li> <li>• Required for OpenLDAP only.</li> </ul>
Support nested groups	<ul style="list-style-type: none"> <li>• Select this checkbox to support the Active Directory LDAP nested groups.</li> <li>• Deselect this checkbox means no support.</li> </ul>
Group entry object class	<ul style="list-style-type: none"> <li>• Required only when "Group lookup using memberOf attribute" is not selected.</li> <li>• Required for OpenLDAP only.</li> </ul>
Group search subfilter	<ul style="list-style-type: none"> <li>• Required only when "Group lookup using memberOf attribute" is not selected.</li> <li>• Required for OpenLDAP only.</li> </ul>
Active Directory domain	The name of the Active Directory Domain. <ul style="list-style-type: none"> <li>• Example: <code>testradius.com</code></li> </ul>

4. Click Add Server. The new LDAP server is listed. To verify, click Test Connection to check whether the BCM2 can connect to the new server successfully.

5. To add more servers, repeat the same steps.
6. In the LDAP page, use the arrow buttons to arrange the servers in the order they should be accessed, then click Save.
7. Make sure LDAP is enabled: Go to Device Settings > Security > Authentication, and select LDAP as the Authentication Type.



► *To duplicate LDAP/LDAPS server settings:*

If you have added any LDAP/LDAPS server to the BCM2, and the server you will add shares identical settings with an existing one, the most convenient way is to duplicate that LDAP/LDAPS server's data and then revise the IP address/hostname.

1. Choose Device Settings > Security > LDAP, then click New.
2. Select the "Copy settings from existing LDAP server" checkbox.
3. Select the LDAP/LDAPS server whose settings you want to copy.
4. Modify the IP Address/Hostname field.
5. Click Add Server.

### Adding Radius Servers

To use Radius authentication, enable it and enter the information you have gathered.

---

Note: The RADIUS NAS Identifier is "DPC PDU SN:<device serial number>".

---

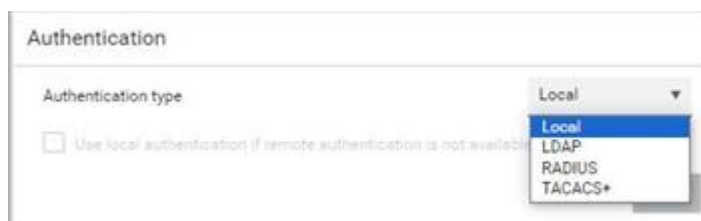
► *To add Radius servers:*

1. Choose Device Settings > Security > RADIUS.
2. Click New.
3. Enter information.

Field/setting	Description
IP address / hostname	The IP address or hostname of your Radius server.

Field/setting	Description
Type of RADIUS authentication	<p>Select an authentication protocol.</p> <ul style="list-style-type: none"> <li>• PAP (Password Authentication Protocol)</li> <li>• CHAP (Challenge Handshake Authentication Protocol)</li> <li>• MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol)</li> </ul> <p>CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear.</p> <p>MS-CHAPv2 provides stronger security than the above two. Selecting this option will support both MS-CHAPv1 and MS-CHAPv2.</p> <hr/> <p><i>Note: All authentication methods are insecure. It is strongly recommended to use RADIUS only in a secure networking environment. A warning displays for all methods.</i></p> <hr/>
Authentication port, Accounting port	<p>The defaults are standard ports -- 1812 and 1813.</p> <p>To use non-standard ports, type a new port number.</p>
Accounting Enabled?	<p>Default is enabled.</p> <p>Accounting allows you to log activity executed on the RADIUS server.</p> <p>When RADIUS accounting is enabled and the RADIUS server does not support accounting, then authentication will fail.</p>
Timeout	<p>This sets the maximum amount of time to establish contact with the Radius server before timing out.</p> <p>Type the timeout period in seconds.</p>
Retries	Type the number of retries.
Shared secret, Confirm shared secret	The shared secret is necessary to protect communication with the Radius server.

4. To verify settings, click Test Connection to check if you can connect to the new server successfully.
5. Click Add Server. The new Radius server is listed on the RADIUS page.
6. To add more servers, repeat the same steps.
7. In the RADIUS page, use the arrow buttons to arrange the servers in the order they should be accessed, then click Save.
8. Make sure RADIUS is enabled: Go to Device Settings > Security > Authentication, and select RADIUS as the Authentication Type.



## Adding TACACS+ Servers

To use TACACS+ authentication, add the server information and enable TACACS+.

---

**Note:** You need to create a new custom service attribute called Xerus on the TACACS+ server. This attribute value will match the role name (case sensitive) on the BCM2. In the authorization request to the TACACS+ server, the BCM2 will send a request for Xerus as a custom service attribute. TACACS+ server then returns the roles of the authenticated user in the Xerus: roles attribute. Returning multiple roles separated by a slash, for example, role1/role2, is supported. See [Cisco ISE Xerus TACACS+ Authentication](#) (on page 480) for configuration.

---

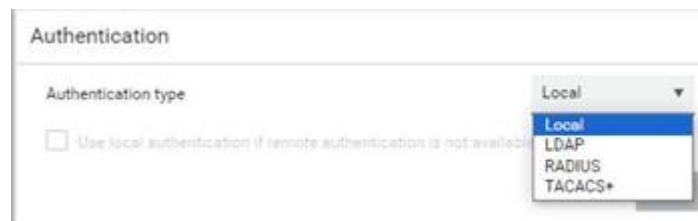
► To add TACACS+ servers:

1. Choose Device Settings > Security > TACACS+.
2. Click New.
3. Enter information.

Field/setting	Description
IP address / hostname	The IP address or hostname of your TACACS+ server.
Type of TACACS+ authentication	Select an authentication protocol. <ul style="list-style-type: none"><li>• ASCII</li><li>• PAP (Password Authentication Protocol)</li><li>• CHAP (Challenge Handshake Authentication Protocol)</li><li>• MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)</li></ul> CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear. MS-CHAP provides stronger security than the other options. <hr/> <i>Note: All authentication methods are insecure. It is strongly recommended to use TACACS+ only in a secure networking environment. A warning displays for all methods.</i> <hr/>
Port	The default port is 49 To use non-standard port, type a new port number.
Enable Accounting?	Default is enabled. Accounting allows you to log activity executed on the TACACS+ server.
Timeout	Default is 10 seconds. Maximum amount of time to establish contact with the server before timing out. Enter the timeout period in seconds.
Retries	Default is 3. Enter the number of retries.

Field/setting	Description
Shared secret, Confirm shared secret	The shared secret is necessary to protect communication with the server.

1. Click Add Server or Test Connection to verify the settings.
2. To add more servers, repeat the same steps.
3. In the TACACS+ page, use the arrow buttons to arrange the servers in the order they should be accessed, then click Save.
4. To begin using the configuration, make sure TACACS+ is enabled: Go to Device Settings > Security > Authentication, and select TACACS+ as the Authentication Type.



## Configuring Login Settings

Choose Device Settings > Security > Login Settings to open the Login Settings page, where you can:

- Configure the user blocking feature.

---

*Note: The user blocking function applies only to local authentication instead of external authentication through AA servers.*

---

- Determine the timeout period for any inactive user.
- Prevent simultaneous logins using the same login name.

### ► To configure user blocking:

1. To enable the user blocking feature, select the 'Block user on login failure' checkbox.
2. In the 'Block timeout' field, select a time option. This setting determines how long the user is blocked.
  - If you type a value, the value must be followed by a time unit, such as '4 min.'
3. In the 'Maximum number of failed logins' field, type a number. This is the maximum number of login failures the user is permitted before the user is blocked from accessing the BCM2.
4. Timeout for Failed Login Attempts: select a time option after which a failed attempt no longer counts against the user. For example, if "Maximum number of failed logins" is 3, but the "Timeout for Failed Login Attempts" has passed since the last failed attempt, the counter of failed logins restarts.
5. Click Save.




---

Tip: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command over a local connection. See Unblocking a User.

---

► *To set limitations for login timeout and use of identical login names:*

1. In the "Idle timeout period" field, type a value or click  to select a time option. This setting determines how long users are permitted to stay idle before being forced to log out.
  - If you type a value, the value must be followed by a time unit, such as '4 min.' See Time Units.
  - Keep the idle timeout to 20 minutes or less if possible. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to the BCM2.
2. Select the 'Prevent concurrent login with same username' checkbox to prevent multiple users from using the same login name simultaneously.
3. Click Save.

## Configuring Password Policy

Choose Device Settings > Security > Password Policy to open the Password Policy page, where you can:

- Force users to use strong passwords.
- Force users to change passwords at a regular interval -- that is, password aging.

► *To configure password aging:*

1. Select the 'Enabled' checkbox of Password Aging.
2. In the 'Password aging interval' field, type a value or select a time option. This setting determines how often users are requested to change their passwords.
  - If you type a value, the value must be followed by a time unit, such as '10 d.'
3. Click Save.

► *To force users to create strong passwords:*

1. Select the 'Enabled' checkbox of Strong Passwords 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 forbidden previous passwords = 5

2. Make changes to the default settings as needed.
3. Click Save.

## Enabling the Restricted Service Agreement

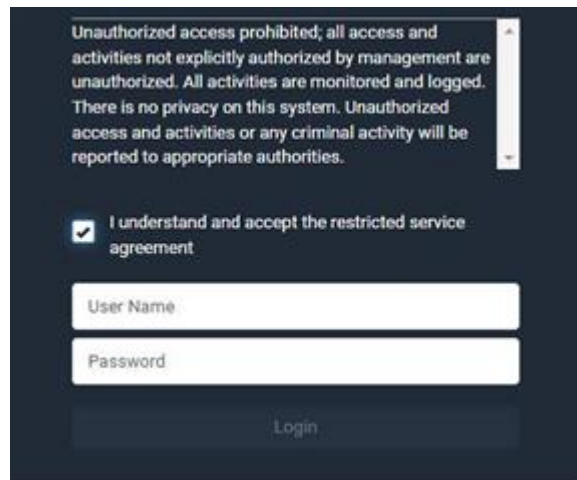
The restricted service agreement feature, if enabled, forces users to read a security agreement when they log in to the BCM2. Users must accept the agreement, or they cannot log in. You can configure an event notifying you if a user has accepted or declined the agreement.

### ► *To enable the service agreement:*

1. Click Device Settings > Security > Service Agreement.
2. Select the 'Enforce restricted service agreement' checkbox.
3. Edit or paste the content as needed.
  - A maximum of 10,000 characters can be entered.
4. Click Save.

### ► *Login manner after enabling the service agreement:*

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed on the login screen.



The screenshot shows a dark-themed login interface. At the top, a scrollable text box contains the following text: "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." Below this text is a checkbox labeled "I understand and accept the restricted service agreement", which is checked. Underneath the checkbox are two input fields: "User Name" and "Password". At the bottom center is a "Login" button.

To log in when a restricted service agreement appears:

- In the web interface, select the checkbox labeled "I understand and accept the restricted service agreement."
- In the CLI, type `y` when the confirmation message "I understand and accept the restricted service agreement" is displayed.

## Setting the Date and Time

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

BCM2 follows the NTP server sanity check per the IETF RFC.

---

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

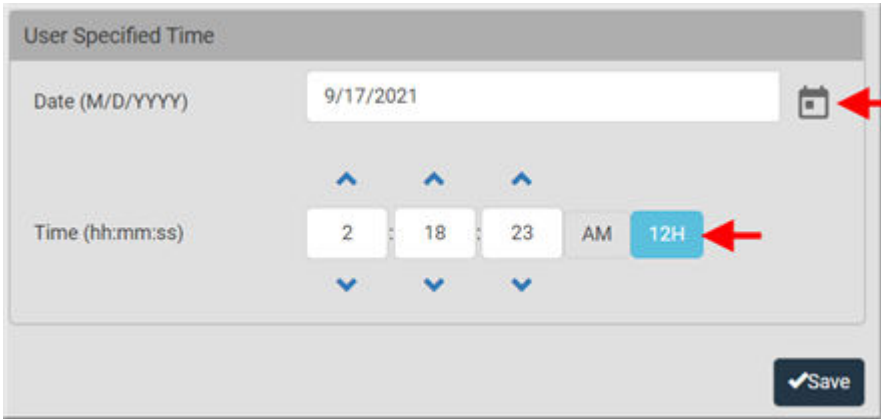
---

► *To set the date and time:*

1. Choose Device Settings > Date/Time.
2. Click the 'Time zone' field to 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.
4. Select the method for setting the date and time. Choose settings and click Save.

*Customize the date and time*

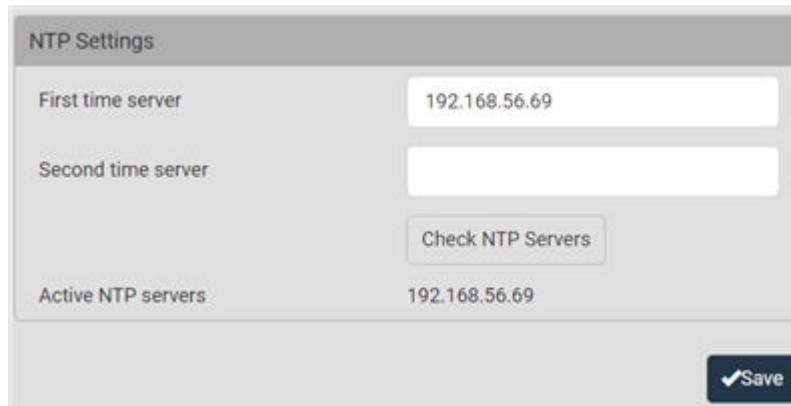
- Select 'User specified time'.
- Enter the date or click the calendar icon to select a date.
- Click 12H/24H button to toggle time formats.
- Click the AM/PM button to toggle.
- Enter the time or click the arrows to set it.



The screenshot shows a web interface for setting the date and time. The title is "User Specified Time". There are two main sections: "Date (M/D/YYYY)" and "Time (hh:mm:ss)". The date field contains "9/17/2021" and has a calendar icon to its right. The time field has three spinners for hours, minutes, and seconds, with values "2", "18", and "23" respectively. To the right of the spinners are buttons for "AM" and "12H". A "Save" button is at the bottom right. Red arrows point to the calendar icon and the "12H" button.

### Use the NTP server

- Select "Synchronize with NTP server."
  - The DHCP-assigned NTP servers are available when DHCP is enabled. The IP address appears as Active NTP Server. To use this server, leave the primary and secondary server fields blank.
  - To specify NTP servers, enter the primary NTP server in the "First time server" field. A secondary NTP server is optional.
- Click Check NTP Servers to verify accessibility.



## Windows NTP Server Synchronization Solution

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

---

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

---

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

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

1. Access the registry settings associated with the root dispersion on the Windows NTP server.  
*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config*
2. *AnnounceFlags* must be set to 0x05 or 0x06.
  - 0x05 = 0x01 (Always time server) and 0x04 (Always reliable time server)
  - 0x06 = 0x02 (Automatic time server) and 0x04 (Always reliable time server)

---

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

---

3. *LocalClockDispersion* must be set to 0.

## Door Access

SmartLock enabled cabinets integrated with PowerIQ or other third party systems authorize door access remotely. In the event that the remote authorization is not accessible, local rules can be configured as an alternative or in addition to PIQ rules.

A door access rule can contain the following components:

- Selected door locks: must be configured in advance.
- Authorization via card: specify which card ID and card reader must be used
- Authorization via keypad: specify the PIN and keypad that must be used
- Two-factor authorization: a timeout that requires both card and keypad conditions to be met. For example: when a certain card is inserted, the correct PIN must be entered in the next 10 seconds.
- Absolute time conditions: grant access for a specific date and time
- Periodic time conditions: grant access on certain days of the week and certain times

---

Note: In one access rule you can set 2 card IDs as 2-factor authorization.

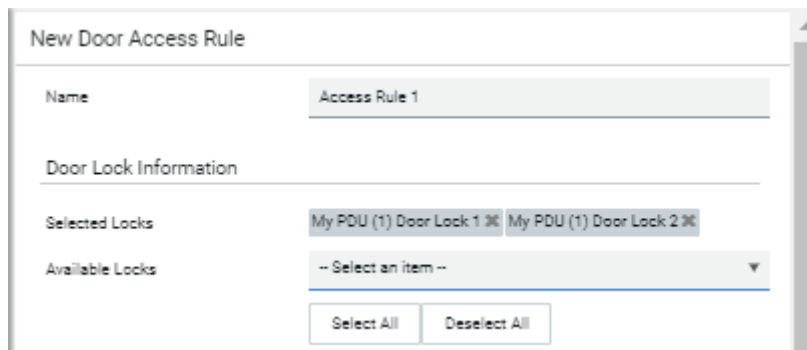
---

### ► To create a door access rule:

1. Choose Device Settings > Door Access.
2. Click New Access Rule.



3. The New Door Access Rule page opens. Enter a name for the rule. 128 characters maximum.
4. Select the door locks this rule applies to in the Available Door Handle Locks list. Each selected door lock appears in the Selected Locks section.

A screenshot of the "New Door Access Rule" configuration form. It has a title bar "New Door Access Rule" with an upward arrow. The form contains:

- A "Name" field with the value "Access Rule 1".
- A "Door Lock Information" section header.
- A "Selected Locks" field containing two items: "My PDU (1) Door Lock 1 3K" and "My PDU (1) Door Lock 2 3K".
- An "Available Locks" dropdown menu currently showing "-- Select an item --".
- At the bottom, there are "Select All" and "Deselect All" buttons.

- To allow authorization via card reader, select the Card Access checkbox, then select the correct Card Reader and click Read Card to retrieve the Card ID. Card IDs are hidden for security. Click the eyeball icon to reveal and verify the Card ID.

The screenshot shows a configuration panel titled "Authorization via Card". It contains three rows: "Card Access" with a checked checkbox, "Card Reader" with a dropdown menu showing "-- Select a Card Reader --", and "Card ID" with a text input field containing "QRead Card" and an eyeball icon to the right.

- To allow Authorization via Keypad, select the Keypad Access checkbox, then select the correct keypad and enter the PIN. PINs are hidden for security. Click the eyeball icon to reveal and verify the PIN. PIN length varies by keypad, and a minimum PIN length of 4 is required.

The screenshot shows a configuration panel titled "Authorization via Keypad". It contains three rows: "Keypad Access" with a checked checkbox, "Keypad" with a dropdown menu showing "-- Select a Keypad --", and "PIN" with a text input field and an eyeball icon to the right.

- When both Card and Keypad authorization are required, the Two-Factor Configuration controls are required. Enter a Timeout in seconds during which both Card and Keypad authorization must occur.

The screenshot shows a configuration panel titled "Two-Factor Configuration". It features a "Timeout" field with a value of "10" and a unit selector set to "s". Below the field is an information box that reads: "Info: Timeout for matching a card and a keypad authorization in seconds."

- To allow authorization with an Absolute Time Condition, select the Absolute Time checkbox, then use the calendar tool to set the start and end dates, and the clock tools to set the start and end times during which access is granted. Note: Click the 12H/24H icon to toggle between clock styles.

**Absolute Time Condition**

Absolute Time

From Date (M/D/YYYY) 8/22/2023 11 : 55 : 35 AM 12H

To Date (M/D/YYYY) 8/22/2023 12 : 55 : 35 PM 12H

Info: Times are in device local time (UTC-05:00) Eastern Time (US & Canada)

- To allow authorization with a Periodic Time Condition, select the Periodic Time checkbox, then select the Days of Week and range of hours on which access is granted. Note: Click the 12H/24H icon to toggle between clock styles.

**Periodic Time Condition**

Periodic Time

Days of Week  Sunday  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday

From Time (hh:mm) 11 : 55 AM 12H

To Time (hh:mm) 12 : 55 PM 12H

Info: If the end time is less than or equal to the start time, this applies until the following day. Times are in device local time (UTC-05:00) Eastern Time (US & Canada)

- Click Create to save the rule. All rules appear on the main Door Access Rule page.

**Door Access Rules**

<input type="checkbox"/>	Name	Door Locks	Card ID	Card Reader	Periodic Time	Absolute Time
<input type="checkbox"/>	3/5/21 Daniel access cab1 (1)	My SRC (1) Door Handle Lock 1 My SRC (1) Door Handle Lock 2	*****	My SRC (1) Southco H3-EM - 10E000007-1	Mon, Tue, Wed, Thu, Fri From: 9:49 AM UTC-0500 To: 10:49 AM UTC-0500	From: 4/11/2021, 9:49:43 AM UTC-0500 To: 4/15/2021, 7:49:43 PM UTC-0500
<input type="checkbox"/>	Derek access (2)	My SRC (1) Door Handle Lock 1	*****	My SRC (1) Southco H3-EM - 10E000007-1		

## Event Rules and Actions

Create event rules and actions to notify you of or react to a change in conditions.

An event rule consists of two parts:

- **Event:** This is the situation where the BCM2 or a device connected to it meets a certain condition. For example, the inlet's voltage reaches the warning level.
- **Action:** This is the response to the event. For example, the system administrator is notified of the event via email.

Some actions can be scheduled at regular intervals instead of occurring in reaction to an event. For example, you can schedule the emailing of the temperature report every hour.

You must have the Administrator Privileges to configure event rules.

► *To create an event rule:*

1. Choose Device Settings > Event Rules.
2. If the needed action is not available yet, click New Action to create it.
  - a. Assign a name to this action.
  - b. Select the desired action and configure it as needed.
  - c. Click Create.
3. Click New Rule to create a new rule.
  - a. Assign a name to this rule.
  - b. Make sure the Enabled checkbox is selected, to make the new rule active.
  - c. In the Event field, select the event to react to.
  - d. In the 'Available actions' field, select the desired action(s) to respond to the selected event.
  - e. Click Create.

► *To create a scheduled action:*

1. Click New Scheduled Action to schedule the desired action.
  - a. Assign a name to this scheduled action.
  - b. Make sure the Enabled checkbox is selected to make the scheduled action active.
  - c. Set the interval time, which ranges from every minute to yearly.
  - d. In the 'Available actions' field, select the desired action(s).
  - e. Click Create.

## Built-in Rules and Rule Configuration

There are several built-in event rules, which cannot be deleted. If the built-in event rules do not satisfy your needs, create new rules.

► *Built-in rules:*

- *System Event Log Rule:*  
This causes ANY event occurred to the BCM2 to be recorded in the internal log. It is enabled by default.



---

*Note: Default log messages are generated for each event.*

---

- *System SNMP Notification Rule:*  
This causes SNMP traps or informs to be sent to specified IP addresses or hosts when ANY event occurs to the BCM2. It is disabled by default.
- *System Tamper Detection Alarmed:*  
This causes alarm notifications if a connected tamper sensor is detected to be in an alarmed state. It is enabled by default.
- *System Tamper Detection Unavailable:*  
This causes alarm notifications if a previously available tamper sensor is not detected. It is enabled by default.

► *Event rule configuration illustration:*

1. Choose Device Settings > Event Rules > New Rule.
2. Click the Event field to select an event type.
  - <Any sub-event> means all events shown on the list.
  - <Any Numeric Sensor> means all numeric sensors, including internal and environmental sensors. <Any Numeric Sensor> is especially useful if you want to receive the notifications when any numeric sensor's readings pass through a specific threshold.
3. In this example, the Peripheral Device Slot is selected, which is related to the environmental sensor packages. Then a sensor ID field for this event type appears. Click this additional field to specify which sensor should be the subject of this event.
4. In this example, sensor ID 3 (Slot 3) is selected, which is a temperature sensor. Then a new field for this sensor appears. Click this field to specify the type of event(s) you want.
5. In this example, Numeric Sensor is selected because we want to select numeric-sensor-related event(s). Then a field for numeric-sensor-related events appears. Click this field to select one of the numeric-sensor-related events from the list.
6. In this example, 'Above upper critical threshold' is selected because we want the BCM2 to react only when the selected temperature sensor's reading enters the upper critical range. A "Trigger condition" field appears, requiring you to define the "exact" condition related to the "upper critical" event.
7. Select the desired radio button to finish the event configuration. Refer to the following table for different types of radio buttons.
  - See [Sample Event Rules](#) (on page 222).
8. Add and/or remove actions to configure the rule. Select actions from the 'Available actions' list to create the Select actions list.

**New Rule**

Rule name:

Enabled:

Event:

Trigger condition:  Asserted  Deasserted  Both

Selected actions:

Available actions:

► *Radio buttons for different events:*

Some events require you to configure the "Trigger condition".

Event types	Radio buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	<ul style="list-style-type: none"> <li>Asserted: action occurs only when the selected event occurs. That is, the status of the event transits from FALSE to TRUE.</li> <li>Deasserted: action occurs only when the selected event disappears or stops. That is, the status of the selected event transits from TRUE to FALSE.</li> <li>Both: action occurs both when the event occurs (asserts) and when the event stops/disappears (deasserts).</li> </ul>
State sensor state change	<ul style="list-style-type: none"> <li>Alarmed/Open/On: action occurs only when the chosen sensor enters the alarmed, open or on state.</li> <li>No longer alarmed/Closed/Off: action occurs only when the chosen sensor returns to the normal, closed, or off state.</li> <li>Both: action occurs whenever the chosen sensor switches its state.</li> </ul>
Sensor availability	<ul style="list-style-type: none"> <li>Unavailable: action occurs only when the chosen sensor is NOT detected and becomes unavailable.</li> <li>Available: action occurs only when the chosen sensor is detected and becomes available.</li> <li>Both: action occurs both when the chosen sensor becomes unavailable or available.</li> </ul>

Event types	Radio buttons
Network interface link state	<ul style="list-style-type: none"> <li>• Link state is up: action occurs only when the network link state changes from down to up.</li> <li>• Link state is down: action occurs only when the network link state changes from up to down.</li> <li>• Both: action occurs whenever the network link state changes.</li> </ul>
Function enabled or disabled	<ul style="list-style-type: none"> <li>• Enabled: action occurs only when the chosen function is enabled.</li> <li>• Disabled: action occurs only when the chosen function is disabled.</li> <li>• Both: action occurs when the chosen function is either enabled or disabled.</li> </ul>
Restricted service agreement	<ul style="list-style-type: none"> <li>• Accepted: action occurs only when the specified user accepts the restricted service agreement.</li> <li>• Declined: action occurs only when the specified user rejects the restricted service agreement.</li> <li>• Both: action occurs both when the specified user accepts or rejects the restricted service agreement.</li> </ul>
Server monitoring event	<ul style="list-style-type: none"> <li>• Monitoring started: action occurs only when the monitoring of any specified server starts.</li> <li>• Monitoring stopped: action occurs only when the monitoring of any specified server stops.</li> <li>• Both: action occurs when the monitoring of any specified server starts or stops.</li> </ul>
Server reachability	<ul style="list-style-type: none"> <li>• Unreachable: action occurs only when any specified server becomes inaccessible.</li> <li>• Reachable: action occurs only when any specified server becomes accessible.</li> <li>• Both: action occurs when any specified server becomes either inaccessible or accessible.</li> </ul>
Device connection or disconnection, such as a USB-cascaded device	<ul style="list-style-type: none"> <li>• Connected: action occurs only when the selected device is physically connected to it.</li> <li>• Disconnected: action occurs only when the selected device is physically disconnected from it.</li> <li>• Both: action occurs both when the selected device is physically connected to it and when it is disconnected.</li> </ul>

Event types	Radio buttons
+12V Supply 1 Status	<p>Available radio buttons include "Fault," "OK" and "Both."</p> <ul style="list-style-type: none"> <li>• Fault: action occurs only when the selected 12V power supply to the controller enters the fault state.</li> <li>• OK: action occurs only when the selected 12V power supply to the controller enters the OK state.</li> <li>• Both: action occurs whenever the selected 12 power supply's status changes.</li> </ul>

## Xerus Default Log Messages for All Products

Listed here are all default messages for all Xerus events, including all supported products. Not all products support all events, and events are marked here with the supported model type.

Event/context	Default message on event assertion	Default message on event deassertion	Model Type
Asset Management > Blade Extension Overflow	Blade extension overflow occurred on strip [AMSNUMBER] ('[AMSNAME]').	Blade extension overflow cleared for strip [AMSNUMBER] ('[AMSNAME]').	
Asset Management > Composite Asset Strip Composition Changed	Composition changed on composite asset strip [AMSNUMBER] ('[AMSNAME]').		
Asset Management > Device Config Changed	Config parameter '[CONFIGPARAM]' of asset strip [AMSNUMBER] ('[AMSNAME]') changed to '[CONFIGVALUE]' by user '[USERNAME]'.		
Asset Management > Firmware Update	Firmware update for asset strip [AMSNUMBER] ('[AMSNAME]'): status changed to '[AMSSTATE]'.		
Asset Management > Rack Unit > Blade Extension Connected	Blade extension with ID '[AMSTAGID]' connected at rack unit [AMSRACKUNITPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').	Blade extension with ID '[AMSTAGID]' disconnected at rack unit [AMSRACKUNITPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').	
Asset Management > Rack Unit > Tag Connected	Asset tag with ID '[AMSTAGID]' connected at rack unit [AMSRACKUNITPOSITION], slot [AMSBLADESLOTPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').	Asset tag with ID '[AMSTAGID]' disconnected at rack unit [AMSRACKUNITPOSITION], slot [AMSBLADESLOTPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').	
Asset Management > Rack Unit Config Changed	Config of rack unit [AMSRACKUNITPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]') changed by user '[USERNAME]' to: Name '[AMSRACKUNITNAME]', LED Operation Mode '[AMSLEDOPMODE]', LED Color '[AMSLEDCOLOR]', LED Mode '[AMSLEDMODE]'		

Asset Management > State	State of asset strip [AMSNUMBER] ('[AMSNAME]') changed to '[AMSSTATE]'.		
Card Reader Management > Card Reader > Card inserted	Card of type '[SMARTCARDTYPE]' inserted at Card Reader '[FORMATTEDCARDREADERPATH]'.		
Card Reader Management > Card Reader > Card removed	Card of type '[SMARTCARDTYPE]' removed at Card Reader '[FORMATTEDCARDREADERPATH]'.		
Card Reader Management > Card Reader attached	Card Reader '[FORMATTEDCARDREADERPATH]' connected.		
Card Reader Management > Card Reader detached	Card Reader '[FORMATTEDCARDREADERPATH]' disconnected.		
Card Reader Management > Card Reader settings changed	Settings with name '[CARDREADERNAME]' and description '[CARDREADERDESCRIPTION]' set at Card Reader '[FORMATTEDCARDREADERPATH]' by user '[USERNAME]' from host '[USERIP]'.		
Device > Event log cleared	Event log cleared by user '[USERNAME]' from host '[USERIP]'.		
Device > Bulk configuration copied	[LINKIDTAG]Bulk configuration copied by user '[USERNAME]' from host '[USERIP]'.		
Device > Bulk configuration saved	[LINKIDTAG]Bulk configuration saved by user '[USERNAME]' from host '[USERIP]'.		
Device > Device clock changed	The device clock was changed from [OLDDATETIME] to [DATETIME].		
Device > Data push failed	Data push to URL [DATAPUSHURL] failed. [ERRORDESC]		
Device > Device settings restored	[LINKIDTAG]Device settings restored by user '[USERNAME]' from host '[USERIP]'.		
Device > Device settings saved	[LINKIDTAG]Device settings saved by user '[USERNAME]' from host '[USERIP]'.		
Device > Firmware update completed	[LINKIDTAG]Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.		
Device > Firmware update failed	[LINKIDTAG]Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.		

Device > Firmware update started	[LINKIDTAG]Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.		
Device > Firmware validation failed	[LINKIDTAG]Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.		
Device > Hardware failure present	[LINKIDTAG]Failure '[FAILURETYPESTR]' asserted for component '[COMPONENTID]'.	[LINKIDTAG]Failure '[FAILURETYPESTR]' deasserted for component '[COMPONENTID]'.	
Device > Device identification changed	Config parameter '[CONFIGPARAM]' changed to '[CONFIGVALUE]' by user '[USERNAME]' from host '[USERIP]'.		
Device > An LDAP error occurred	An LDAP error occurred: [ERRORDESC].		
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 > A Radius error occurred	A Radius error occurred: [ERRORDESC].		
Device > Raw configuration downloaded	[LINKIDTAG]Raw configuration downloaded by user '[USERNAME]' from host '[USERIP]'.		
Device > Raw configuration updated	[LINKIDTAG]Raw configuration updated by user '[USERNAME]' from host '[USERIP]'.		
Device > Sending SMS message failed	Sending SMS message to '[PHONENUMBER]' failed. [ERRORDESC]		
Device > Sending SMTP message failed	Sending SMTP message to '[SMTPRECIPIENTS]' using server '[SMTPSERVER]' failed. [ERRORDESC]		
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 > System reset	[LINKIDTAG]System reset performed by user '[USERNAME]' from host '[USERIP]'.		
Device > System started	[LINKIDTAG]System started.		

Device > A TACACS+ error occurred	A TACACS+ error occurred: [ERRORDESC].		
Device > Unknown peripheral device attached	An unknown peripheral device with rom code '[ROMCODE]' was attached at position '[PERIPHDEVPOSITION]'.		
Device > Expansion unit connected	Expansion unit connected.	Expansion unit disconnected.	
Device > Wired network authentication result	The network authentication on interface [IFNAME] [NETAUTHRESULTSTR].		
Door Access Control > Door access denied	Door access was denied: [DOORACCESSDENIALREASON]		
Door Access Control > Door access granted	Door access was granted, rule '[DOORACCESSRULENAME]' ([DOORACCESSRULEID])		
Door Access Control > Door access rule added	Door access rule '[DOORACCESSRULENAME]' ([DOORACCESSRULEID]) was added by user '[USERNAME]' from host '[USERIP]'		
Door Access Control > Door access rule changed	Door access rule '[DOORACCESSRULENAME]' ([DOORACCESSRULEID]) was changed by user '[USERNAME]' from host '[USERIP]'		
Door Access Control > Door access deleted	Door access rule '[DOORACCESSRULENAME]' ([DOORACCESSRULEID]) was deleted by user '[USERNAME]' from host '[USERIP]'		
Door Access Control > Door Handle > (handle name) > Door Forced Open	[LINKIDTAG]Door '[DOORSTATENAME]' was opened without unlocking the door handle.		
Door Access Control > Door Handle > (handle name) > Mechanically Unlocked	[LINKIDTAG]Door handle '[DOORHANDLENAME]' was opened without being electronically unlocked.		
Peripheral Device Slot > Numeric Sensor > Above upper critical threshold	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Peripheral Device Slot > Numeric Sensor > Above upper warning threshold	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	

Peripheral Device Slot > Numeric Sensor > Below lower critical threshold	Peripheral device '[EXTSENSORNAME]' in [FORMATEDEXTSENSORSLLOT] asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in [FORMATEDEXTSENSORSLLOT] deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Peripheral Device Slot > Numeric Sensor > Below lower warning threshold	Peripheral device '[EXTSENSORNAME]' in [FORMATEDEXTSENSORSLLOT] asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in [FORMATEDEXTSENSORSLLOT] deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Peripheral Device Slot > Numeric Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in [FORMATEDEXTSENSORSLLOT] has become unavailable.	Peripheral device '[EXTSENSORNAME]' in [FORMATEDEXTSENSORSLLOT] is no longer unavailable; it is now [SENSORSTATENAME].	
Peripheral Device Slot > State Sensor / Actuator > Alarmed	Peripheral device '[EXTSENSORNAME]' in [FORMATEDEXTSENSORSLLOT] is [SENSORSTATENAME].	Peripheral device '[EXTSENSORNAME]' in [FORMATEDEXTSENSORSLLOT] is [SENSORSTATENAME].	
Peripheral Device Slot > State Sensor / Actuator > Switched by user	Peripheral device '[EXTSENSORNAME]' in [FORMATEDEXTSENSORSLLOT] has been switched to [SENSORSTATENAME] by user '[USERNAME]' from host '[USERIP]'.		
Peripheral Device Slot > State Sensor / Actuator > Unavailable	Peripheral device '[EXTSENSORNAME]' in [FORMATEDEXTSENSORSLLOT] has become unavailable.	Peripheral device '[EXTSENSORNAME]' in [FORMATEDEXTSENSORSLLOT] is no longer unavailable; it is now [SENSORSTATENAME].	
Keypad Management > Keypad > PIN entered	PIN entered at Keypad '[FORMATTEDKEYPADPATH]'.		
Keypad Management > Keypad attached	Keypad '[FORMATTEDKEYPADPATH]' connected.		
Keypad Management > Keypad detached	Keypad '[FORMATTEDKEYPADPATH]' disconnected.		
Keypad Management > Keypad settings changed	Settings with name '[KEYPADNAME]' and description '[KEYPADDESCRIPTION]' set at Keypad '[FORMATTEDKEYPADPATH]' by user '[USERNAME]' from host '[USERIP]'.		
Linking > Link unit added	Link unit [LINKID] ([LINKUNITHOST]) has been added by user '[USERNAME]' from '[USERIP]'.		
Linking > Link unit communication failed	Communication with link unit [LINKID] ([LINKUNITHOST]) failed.	Communication with link unit [LINKID] ([LINKUNITHOST]) is OK.	



Linking > Link unit released	Link unit [LINKID] ([LINKUNITHOST]) has been released by user '[USERNAME]' from '[USERIP]'.		
Outlet Grouping > Outlet Group > Outlet Group Modified	Outlet group '[OUTLETGROUPID]' was modified.		
Outlet Grouping > Outlet Group > Power control > Power cycled	Outlet group '[OUTLETGROUPID]' power cycle initiated by user '[USERNAME]' from host '[USERIP]'.		
Outlet Grouping > Outlet Group > Power control > Powered off	Outlet group '[OUTLETGROUPID]' has been powered off by user '[USERNAME]' from host '[USERIP]'.		
Outlet Grouping > Outlet Group > Power control > Powered on	Outlet group '[OUTLETGROUPID]' has been powered on by user '[USERNAME]' from host '[USERIP]'.		
Outlet Grouping > Outlet Group > Sensor > Above upper critical threshold	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Outlet Grouping > Outlet Group > Sensor > Above upper warning threshold	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Outlet Grouping > Outlet Group > Sensor > Below lower critical threshold	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Outlet Grouping > Outlet Group > Sensor > Below lower warning threshold	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Outlet Grouping > Outlet Group > Sensor > Reset	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' has been reset by user '[USERNAME]' from host '[USERIP]'.		
Outlet Grouping > Outlet Group > Sensor > Unavailable	Sensor '[OUTLETGROUPSENSOR]' of outlet group '[OUTLETGROUPID]' has become unavailable.	Sensor '[OUTLETGROUPSENSOR]' on outlet group '[OUTLETGROUPID]' is no longer unavailable; it is now [SENSORSTATENAME].	

Outlet Grouping > Outlet Group Created	Outlet group '[OUTLETGROUPID]' was created.		
Outlet Grouping > Outlet Group Deleted	Outlet group '[OUTLETGROUPID]' was deleted.		
PDU > Controller > Communication failed	Communication with PDU [PDUNUMBER] controller '[CONTROLLER]' (board ID [BOARDID]) failed	Communication with PDU [PDUNUMBER] controller '[CONTROLLER]' (board ID [BOARDID]) restored	
PDU > Controller > Firmware update	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] has started firmware update	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] has completed firmware update	
PDU > Controller > Incompatible	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] is incompatible	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] is no longer incompatible	
PDU > Controller > OK	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] is OK	PDU [PDUNUMBER] controller '[CONTROLLER]' with board ID [BOARDID] is no longer OK	
PDU > Inlet > Dip	A dip event occurred on PDU [PDUNUMBER] inlet '[INLET]' for [DIPSWELLDURATION] s with a minimum voltage of [DIPSWELLVOLTAGE] V.		PX4 or PRO4X
PDU > Inlet > Dip/swell event list cleared	The dip/swell event list for PDU [PDUNUMBER] inlet '[INLET]' was cleared by user '[USERNAME]' from host '[USERIP]'.		PX4 or PRO4X
PDU > Inlet > Enabled	PDU [PDUNUMBER] inlet '[INLET]' has been enabled by user '[USERNAME]' from host '[USERIP]'.	PDU [PDUNUMBER] inlet '[INLET]' has been disabled by user '[USERNAME]' from host '[USERIP]'.	
PDU > Inlet > Line Pair > Sensor > Above upper critical threshold	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Line Pair > Sensor > Above upper warning threshold	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	

PDU > Inlet > Line Pair > Sensor > Below lower critical threshold	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Line Pair > Sensor > Below lower warning threshold	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Line Pair > Sensor > Unavailable	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' has become unavailable.	Sensor '[PDULINEPAIRSENSOR]' on line '[INLETLINEPAIR]' of PDU [PDUNUMBER] inlet '[INLET]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Dip	A dip event occurred on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' for [DIPSWELLDURATION] s with a minimum voltage of [DIPSWELLVOLTAGE] V.		PX4 or PRO4X
PDU > Inlet > Pole > Dip/swell event list cleared	The dip/swell event list for pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' was cleared by user '[USERNAME]' from host '[USERIP]'.		PX4 or PRO4X
PDU > Inlet > Pole > Sensor > Above upper critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Above upper warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Below lower critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	

PDU > Inlet > Pole > Sensor > Below lower warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Critical	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' entered critical state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' exited critical state; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Failed	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' entered failed state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' exited failed state; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Normal	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' entered normal state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' exited normal state; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Self-Test	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' started self test.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' finished self test; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Unavailable	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' has become unavailable.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Sensor > Warning	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' entered warning state.	Sensor '[PDUPOLESENSOR]' on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' exited warning state; it is now [SENSORSTATENAME].	
PDU > Inlet > Pole > Swell	A swell event occurred on pole '[INLETPOLE]' of PDU [PDUNUMBER] inlet '[INLET]' for [DIPSWELLDURATION] s with a maximum voltage of [DIPSWELLVOLTAGE] V.		PX4 or PRO4X
PDU > Inlet > Sensor > Above upper critical threshold	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Above upper warning threshold	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSENSOR]' on PDU [PDUNUMBER] inlet '[INLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	

PDU > Inlet > Sensor > Below lower critical threshold	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Below lower warning threshold	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Critical	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' entered critical state.	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' exited critical state; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Failed	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' entered failed state.	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' exited failed state; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Fault	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' entered fault state.	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' exited fault state; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Normal	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' entered normal state.	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' exited normal state; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > OK	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' entered OK state.	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' exited OK state; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Reset	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.		
PDU > Inlet > Sensor > Self-Test	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' started self test.	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' finished self test; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Unavailable	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' has become unavailable.	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Inlet > Sensor > Warning	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' entered warning state.	Sensor '[INLETSensor]' on PDU [PDUNUMBER] inlet '[INLET]' exited warning state; it is now [SENSORSTATENAME].	

PDU > Inlet > Swell	A swell event occurred on PDU [PDUNUMBER] inlet '[INLET]' for [DIPSWELLDURATION] s with a maximum voltage of [DIPSWELLVOLTAGE] V.		PX4 or PRO4X
PDU > Load Shedding > Started	PDU [PDUNUMBER] placed in Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.	PDU [PDUNUMBER] removed from Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.	
PDU > Outlet > Pole > Sensor > Above upper critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Pole > Sensor > Above upper warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Pole > Sensor > Below lower critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Pole > Sensor > Below lower warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Pole > Sensor > Unavailable	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' has become unavailable.	Sensor '[PDUPOLESENSOR]' on pole '[OUTLETPOLE]' of PDU [PDUNUMBER] outlet '[OUTLET]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Outlet > Power control > Power cycled	PDU [PDUNUMBER] outlet '[OUTLET]' power cycle initiated by user '[USERNAME]' from host '[USERIP]'.		
PDU > Outlet > Power control > Powered off	PDU [PDUNUMBER] outlet '[OUTLET]' has been powered off by user '[USERNAME]' from host '[USERIP]'.		
PDU > Outlet > Power control > Powered on	PDU [PDUNUMBER] outlet '[OUTLET]' has been powered on by user '[USERNAME]' from host '[USERIP]'.		

PDU > Outlet > Sensor > Above upper critical threshold	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Sensor > Above upper warning threshold	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Sensor > Below lower critical threshold	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Sensor > Below lower warning threshold	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Outlet > Sensor > On	PDU [PDUNUMBER] outlet '[OUTLET]' state sensor changed to on.	PDU [PDUNUMBER] outlet '[OUTLET]' state sensor is no longer on; it is now [SENSORSTATENAME].	
PDU > Outlet > Sensor > Reset	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.		
PDU > Outlet > Sensor > Unavailable	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' has become unavailable.	Sensor '[OUTLETSENSOR]' on PDU [PDUNUMBER] outlet '[OUTLET]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Outlet > Suspended	PDU [PDUNUMBER] outlet '[OUTLET]' was suspended after being suspected of having caused an OCP trip event.		
PDU > Overcurrent Protector > Sensor > Above upper critical threshold	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	

PDU > Overcurrent Protector > Sensor > Above upper warning threshold	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Below lower critical threshold	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Below lower warning threshold	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Critical	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' entered critical state.	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' exited critical state; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Failed	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' entered failed state.	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' exited failed state; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Normal	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' entered normal state.	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' exited normal state; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Open	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' is open. [OCPTRIPCAUSEINFO]	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' is no longer open; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Self-Test	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' started self test.	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' finished self test; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Unavailable	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' has become unavailable.	Sensor '[OCSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' is no longer unavailable; it is now [SENSORSTATENAME].	



PDU > Overcurrent Protector > Sensor > Warning	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' entered warning state.	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' exited warning state; it is now [SENSORSTATENAME].	
PDU > Sensor > Above upper critical threshold	PDU [PDUNUMBER] sensor '[PDUSENSOR]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	PDU [PDUNUMBER] sensor '[PDUSENSOR]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Sensor > Above upper warning threshold	PDU [PDUNUMBER] sensor '[PDUSENSOR]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	PDU [PDUNUMBER] sensor '[PDUSENSOR]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Sensor > Below lower critical threshold	PDU [PDUNUMBER] sensor '[PDUSENSOR]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	PDU [PDUNUMBER] sensor '[PDUSENSOR]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Sensor > Below lower warning threshold	PDU [PDUNUMBER] sensor '[PDUSENSOR]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	PDU [PDUNUMBER] sensor '[PDUSENSOR]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Sensor > Fault	PDU [PDUNUMBER] sensor '[PDUSENSOR]' entered fault state.	PDU [PDUNUMBER] sensor '[PDUSENSOR]' exited fault state; it is now [SENSORSTATENAME].	
PDU > Sensor > Reset	PDU [PDUNUMBER] sensor '[PDUSENSOR]' has been reset by user '[USERNAME]' from host '[USERIP]'.		
PDU > Sensor > Unavailable	PDU [PDUNUMBER] sensor '[PDUSENSOR]' has become unavailable.	PDU [PDUNUMBER] sensor '[PDUSENSOR]' is no longer unavailable; it is now [SENSORSTATENAME].	
PDU > Transfer Switch > Active inlet changed	Active inlet on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' changed to '[ACTIVEINLET]' due to [TRANSFERSWITCHREASON].		Transfer switch
PDU > Transfer Switch > Sensor > Above upper critical threshold	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	Transfer switch

PDU > Transfer Switch > Sensor > Above upper warning threshold	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Below lower critical threshold	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Below lower warning threshold	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Fault	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is [SENSORSTATENAME].	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Non-redundant	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is now non-redundant.	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer non-redundant; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Normal	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is now normal.	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer normal; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Off	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is now off.	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer off; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Out of sync	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is out of sync.	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer out of sync; it is now [SENSORSTATENAME].	Transfer switch
PDU > Transfer Switch > Sensor > Standby	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is now standby.	Operational state of PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer standby; it is now [SENSORSTATENAME].	Transfer switch

PDU > Transfer Switch > Sensor > Unavailable	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' has become unavailable.	Sensor '[TRANSFERSWITCHSENSOR]' on PDU [PDUNUMBER] transfer switch '[TRANSFERSWITCH]' is no longer unavailable; it is now [SENSORSTATENAME].	Transfer switch
Port Fuse > Tripped	Fuse of [FORMATEDEXTPORT] is [FUSESTATENAME].	Fuse of [FORMATEDEXTPORT] is [FUSESTATENAME].	
Power Metering Controller > Power Meter > Circuit > Pole > Sensor > Above upper critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Pole > Sensor > Above upper warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Pole > Sensor > Below lower critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Pole > Sensor > Below lower warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Pole > Sensor > Unavailable	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' has become unavailable.	Sensor '[PDUPOLESENSOR]' on pole '[CIRCUITPOLE]' of panel '[POWERMETER]' circuit '[CIRCUIT]' is no longer unavailable; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Sensor > Above upper critical threshold	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC

Power Metering Controller > Power Meter > Circuit > Sensor > Above upper warning threshold	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Sensor > Below lower critical threshold	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Sensor > Below lower warning threshold	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Sensor > Reset	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' has been reset by user '[USERNAME]' from host '[USERIP]'.		BCM2 / PMC
Power Metering Controller > Power Meter > Circuit > Sensor > Unavailable	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' has become unavailable.	Sensor '[CIRCUITSENSOR]' on panel '[POWERMETER]' circuit '[CIRCUIT]' is no longer unavailable; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Circuit Created	Circuit '[CIRCUIT]' on panel '[POWERMETER]' was created.		BCM2 / PMC
Power Metering Controller > Power Meter > Circuit Deleted	Circuit '[CIRCUIT]' on panel '[POWERMETER]' was deleted.		BCM2 / PMC
Power Metering Controller > Power Meter > Circuit Modified	Circuit '[CIRCUIT]' on panel '[POWERMETER]' was modified.		BCM2 / PMC
Power Metering Controller > Power Meter > Pole > Sensor > Above upper critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC

Power Metering Controller > Power Meter > Pole > Sensor > Above upper warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Pole > Sensor > Below lower critical threshold	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Pole > Sensor > Below lower warning threshold	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Pole > Sensor > Unavailable	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' has become unavailable.	Sensor '[PDUPOLESENSOR]' on pole '[POWERMETERPOLE]' of power meter '[POWERMETER]' is no longer unavailable; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Sensor > Above upper critical threshold	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Sensor > Above upper warning threshold	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Sensor > Below lower critical threshold	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter > Sensor > Below lower warning threshold	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	BCM2 / PMC

Power Metering Controller > Power Meter > Sensor > Reset	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' has been reset by user '[USERNAME]' from host '[USERIP]'.		BCM2 / PMC
Power Metering Controller > Power Meter > Sensor > Unavailable	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' has become unavailable.	Sensor '[POWERMETERSENSOR]' on power meter '[POWERMETER]' is no longer unavailable; it is now [SENSORSTATENAME].	BCM2 / PMC
Power Metering Controller > Power Meter Created	Power meter '[POWERMETER]' was created.		BCM2 / PMC
Power Metering Controller > Power Meter Deleted	Power meter '[POWERMETER]' was deleted.		BCM2 / PMC
Power Metering Controller > Power Meter Modified	Power meter '[POWERMETER]' was modified.		BCM2 / PMC
Server Monitoring > Error	Error monitoring server '[MONITOREDHOST]': [ERRORDESC]		BCM2 / PMC
Server Monitoring > Monitored	Server '[MONITOREDHOST]' is now being monitored.	Server '[MONITOREDHOST]' is no longer being monitored.	BCM2 / PMC
Server Monitoring > Power control completed	Power control operation for '[MONITOREDHOST]' finished with result: [SERVERPOWERRESULT]		BCM2 / PMC
Server Monitoring > Power control initiated	User '[USERNAME]' initiated a power control operation for '[MONITOREDHOST]': [SERVERPOWEROPERATION]		BCM2 / PMC
Server Monitoring > Unreachable	Server '[MONITOREDHOST]' is unreachable.	Server '[MONITOREDHOST]' is reachable.	BCM2 / PMC
Server Monitoring > Unrecoverable	Connection to server '[MONITOREDHOST]' could not be restored.		BCM2 / PMC
Test > Test Event	A test event was triggered by user '[USERNAME]'.		
Timer Event > Occurred	Timer event '[EVENTRULENAME]' occurred.		
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 > Authentication failure	Authentication failed for user '[USERNAME]' from host '[USERIP]'.		
User Activity > User logon state	User '[USERNAME]' from host '[USERIP]' logged in.	User '[USERNAME]' from host '[USERIP]' logged out.	

User Activity > Session timeout	Session of user '[USERNAME]' from host '[USERIP]' timed out.		
User Activity > User blocked	User '[USERNAME]' from host '[USERIP]' was blocked.		
User Administration > Password changed	Password of user '[UMTARGETUSER]' 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 '[UMTARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'.		
User Administration > Role deleted	Role '[UMTARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.		
User Administration > Role modified	Role '[UMTARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'.		
User Administration > User added	User '[UMTARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'.		
User Administration > User deleted	User '[UMTARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'.		
User Administration > User modified	User '[UMTARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'.		
User Administration > User renamed	User '[UMTARGETUSER]' renamed to '[NEWUMTARGETUSER]' by user '[USERNAME]' from host '[USERIP]'.		
Webcam Management > Image upload started	A snapshot upload of webcam '[WEBCAMNAME]' to folder '[WEBCAMSNAPSHOTFOLDERURL]' was started.		
Webcam Management > Webcam attached	Webcam '[WEBCAMNAME]' ('[WEBCAMMODEL]') added to port '[WEBCAMUSBPORT]'.		
Webcam Management > Webcam detached	Webcam '[WEBCAMNAME]' ('[WEBCAMMODEL]') removed from port '[WEBCAMUSBPORT]'.		
Webcam Management > Webcam settings changed	Webcam '[WEBCAMNAME]' settings changed by user '[USERNAME]'		

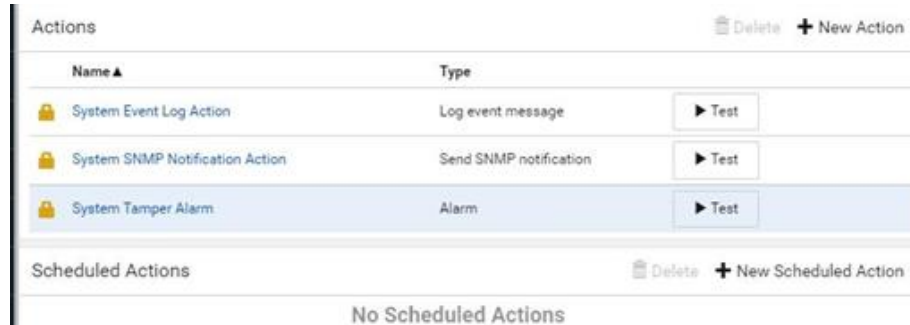
## Available Actions

There are several built-in actions, which cannot be deleted. You can create additional actions for responding to different events.

Some actions have messages that you can customize using placeholders that will populate with specific information when the message is generated. Custom messages with placeholders can be used in these actions: Log event message, Send SMS, Send email (subject+body), Send webcam image (subject+body).

► *To test an action:*

- Click the Test button next to the Action. The action is triggered and you can verify it.



► *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.

---

*Note: No IP addresses are specified for this notification action by default so you must enter IP addresses before applying this action to any event rule. Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa.*

---

- *System Tamper Alarm:*  
This action causes the BCM2 to show the alarm for the tamper sensor, if any, on the Dashboard page until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules.

► *Actions you can create:*

1. Choose Device Settings > Event Rules > New Action.
2. Click the Action field to select an action type from the list.



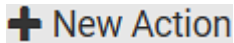
3. Available actions depend on your model. See next sections for details on each action you can configure.
4. Click Create to save an action, then you can include it in an event rule.

## Alarm


The Alarm is an action that requires users to acknowledge an alert. This helps ensure that the user is aware of the alert.


If the Alarm action has been included in a specific event rule and no one acknowledges that alert after it occurs, the BCM2 resends or regenerates an alert notification regularly until the alert is acknowledged or the maximum number of alert notifications is sent. You can acknowledge an alert in the Dashboard.

### ► Operation:

1. Choose Device Settings > Event Rules >  .
2. Select Alarm from the Action list.
3. In the Alarm Notifications list box, specify one or multiple ways to issue the 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, create them first.

  - a. To select any methods, select them one by one in the Available field.  
To add all available methods, simply click Select All.
  - b. To delete any methods, click a method's  in the Selected field.  
To remove all methods, simply click Deselect All.
4. To enable the notification-resending feature, select the 'Enable re-scheduling of alarm notifications' checkbox.


5. In the 'Re-scheduling period' field, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly.
6. In the 'Re-scheduling limit' field, specify the maximum number of times the alert notification is resent. Values range from 1 to infinite.
7. (Optional) You can instruct the BCM2 to send the acknowledgment notification after the alarm is acknowledged in the 'Acknowledgment notifications' field. Available methods are identical to those for generating alarm notifications.
  - a. In the Available field, select desired methods, or click Select All.
  - b. In the Selected field, click any method's  to remove unnecessary ones, or click Deselect All.

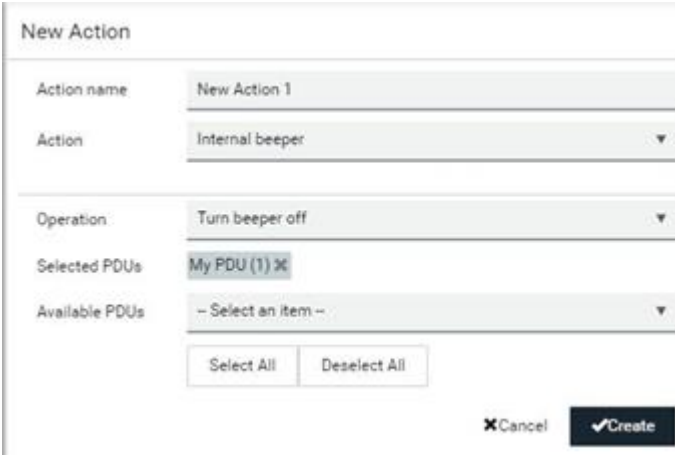
## Action Group

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 any event rule rather than selecting all needed actions one by one per rule.

If the needed action is not available yet, create it first.

### ► Operation:


1. Choose Device Settings > Event Rules >  .
2. Select 'Execute an action group' from the Action list.
3. Select the actions to include in group from the 'Available actions' list, or click Select All.
4. To remove any action(s) from the 'Selected actions' field, click its X.
5. Click Create to save the action.



## Change Load Shedding State

The "Change load shedding state" action is available only when your BCM2 is able to control outlet power. Use this action to activate or deactivate the load shedding mode for responding to a specific event.


► *Operation:*

1. Choose Device Settings > Event Rules >  .
2. Select 'Change load shedding state' from the Action list.
3. In the Operation field, select either one below:
  - Start load shedding: Enters the load shedding mode when the specified event occurs.
  - Stop load shedding: Quits the load shedding mode when the specified event occurs.

### External Beeper

If an external beeper is connected, you can change the beeper's behavior or status to respond to a certain event.

► *To control the connected external beeper:*

1. Choose Device Settings > Event Rules >  .
2. Select 'External beeper' from the Action list.
3. In the 'Beeper port' field, select the port where the external beeper is connected.
4. In the 'Beeper action' field, 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.

---


Warning: 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.

---

### Internal Beeper

You can have the built-in beeper of the BCM2 turned on or off when a certain event occurs.

► *Operation:*

1. Choose Device Settings > Event Rules >  .
2. Select 'Internal beeper' from the Action list.
3. 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.

### Log an Event Message

The option 'Log event message' records the selected events in the internal log.

A default log message will be generated for each type of event, or you can create a custom log message.

► *Operation:*

1. Choose Device Settings > Event Rules > New Action.
2. Select 'Log an event message' from the Action list.
3. Select the 'Use custom log message' checkbox, and then create a custom message in the provided text box.
  - To automatically insert message placeholders, open the Custom Log Message Help section. Search for placeholders and click to include them in your message.
4. Click Create.

### Shut down a Server and Control its Power

The "Power control server" action is available only when your BCM2 is outlet-switching capable.

You can configure the BCM2 to shut down a specific server and then turn off its outlet(s), or turn on that server's outlet(s) after a certain event occurs.


The server must be one of the servers being monitored by your BCM2 and the same BCM2 supplies power to it. See [Monitoring Server Accessibility](#) (on page 234) .

---

Tip: If the server has multiple power cords, make sure all of its power cords are connected to the same BCM2 and you have created an outlet group for controlling all outlets simultaneously.

---

► *Operation:*

1. Choose Device Settings > Event Rules >  .
2. Select 'Power control server' from the Action list.
3. In the Operation field, select an action for the server.
  - Power up: Turns on the outlet or outlet group associated with the selected server.
  - Graceful shutdown: Shuts down the selected server first and then turn off its associated outlet or outlet group.
4. Select the server you want in the Server field.
  - If BCM2 cannot power control any server, a message 'Power control not configured' is shown in the end of the server's host name or IP address.

### Push Out Sensor Readings

You can configure the BCM2 to push sensor log to a remote server after a certain event occurs, including logs of internal sensors, environmental sensors and actuators.

If you have connected asset strips, you can also configure the BCM2 to push the data to a server.


Before creating this action, make sure that you have properly defined the destination servers and the data to be sent on the Data Push page.

---

Tip: To send the data at a regular interval, schedule this action. Note that the "Asset management log" is generated only when there are changes made to any asset strips or asset tags, such as connection or disconnection events.

---

► *Operation:*


1. Choose Device Settings > Event Rules >  .
2. Select 'Push out sensor readings' from the Action list.
3. Select a server or host which receives the data in the Destination field.
  - If the desired destination is not available yet, go to the Data Push page to specify it.

### Record Snapshots to Webcam Storage

This option allows you to define an action that starts or stops a specific webcam from taking snapshots.

Per default the snapshots are stored on the BCM2. It is recommended to specify a remote server to store as many snapshots as possible.

► *Operation:*

1. Choose Device Settings > Event Rules >  .
2. Select 'Record snapshots to webcam storage' from the Action list.
3. Select a webcam in the Webcam field.
4. Select the action to perform - 'Start recording' or 'Stop recording.'

If 'Start recording' is selected, adjust the values of the following:

- Number of snapshots - the number of snapshots to be taken when the event occurs.

The maximum amount of snapshots that can be stored on the BCM2 is 10. If you set it for a number greater than 10 and the storage location is on the BCM2, after the 10th snapshot is taken and stored, the oldest snapshots are overwritten. Storing snapshots on a remote server does not have such a limitation.
- Time before first snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.
- Time between snapshots - the amount of time in seconds between when each snapshot is taken.
- Folder - names of the folders that will be automatically created to store webcam snapshots after the recording action is triggered by the rule you will configure.

Note that the Folder field is available only when the selected webcam has been configured to store its snapshots on an "FTP" server.

Folder name options	Definition
Serial number / Webcam name	Two folders will be created. <ul style="list-style-type: none"><li>• The parent folder's name is the serial number of BCM2.</li><li>• The subfolder's name is the selected webcam's name.</li></ul>
Serial number / Webcam name / Rule name	Three folders will be created. <ul style="list-style-type: none"><li>• Definitions of the parent folder and first subfolder are the same as the first row.</li><li>• The final subfolder's name is the name of event rule that triggers this recording action.</li></ul>

Folder name options	Definition
Serial number / Webcam name / Timestamp	<p>Three folders will be created.</p> <ul style="list-style-type: none"> <li>• Definitions of the parent folder and first subfolder are the same as the first row.</li> <li>• The final subfolder's name is the time when the recording event occurs, which is the accumulated time in seconds since 1970/1/1.</li> </ul>
Serial number / Webcam name / Rule name / Timestamp	<p>Four folders will be created.</p> <ul style="list-style-type: none"> <li>• Definitions of the parent folder and first subfolder are the same as the first row.</li> <li>• The second subfolder's name is the name of event rule that triggers this recording action.</li> <li>• The final subfolder's name is the time when the recording event occurs, which is the accumulated time in seconds since 1970/1/1.</li> </ul>
Serial number / Webcam name / Formatted timestamp	<p>Three folders will be created.</p> <ul style="list-style-type: none"> <li>• Definitions of the parent folder and first subfolder are the same as the first row.</li> <li>• The final subfolder's name is the time when the recording event occurs, which is a format comprising year, month, date, hour, minute, second and timezone.</li> </ul>
Serial number / Webcam name / Rule name / Formatted timestamp	<p>Four folders will be created.</p> <ul style="list-style-type: none"> <li>• Definitions of the parent folder and first subfolder are the same as the first row.</li> <li>• The second subfolder's name is the name of event rule that triggers this recording action.</li> <li>• The final subfolder's name is the time when the recording event occurs, which is a format comprising year, month, date, hour, minute, second and timezone.</li> </ul>

The timestamp is based on the time you have configured on the BCM2.

To find the serial number of your BCM2, go to Maintenance > *Device Information*.

## 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 placeholders. The placeholders represent information which is pulled from the BCM2 and inserted into the message.


For example:

```
[USERNAME] logged into the device on [DATETIME]
```

translates to

```
Mary logged into the device on 2022-January-30 21:00
```

### ► Operation:

1. Choose Device Settings > Event Rules >  .
2. Select 'Send email' from the Action list.
3. In the 'Recipient email addresses' field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.

4. By default, the SMTP server specified on the SMTP Server page will be the SMTP server for performing this action.

To use a different SMTP server, select the 'Use custom settings' radio button.

Default messages are sent based on the event.

5. If needed, you can customize the subject and messages sent via this email.
  - Select the 'Custom subject' checkbox, and enter the text you prefer as this email's subject.
  - Select the 'Use custom log message' checkbox, and then create a custom message up to 1024 characters in the provided field.
  - To automatically insert message placeholders, open the Custom Log Message Help section. Search for placeholders and click to include them in your message.
6. Click Create.


## Send Sensor Report

You may set the BCM2 so that it automatically reports the latest readings or states of one or multiple sensors by sending a message or email or simply recording the report in a log. These sensors can be either internal or environmental sensors 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 environmental sensor packages connected to the BCM2, such as temperature or humidity sensors.


See [Send Sensor Report Example](#) (on page 214).

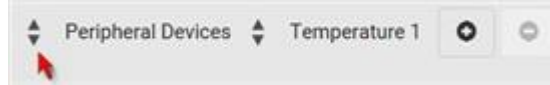
### ► Operation:


1. Choose Device Settings > Event Rules >  .
2. Select 'Send sensor report' from the Action list.
3. In the 'Destination actions' section, select the method(s) to report sensor readings or states. The number of available methods varies, depending on how many messaging actions have been created.

The messaging action types include:


- Log event message
  - Syslog message
  - Send email
  - Send SMS message
4. If no messaging actions are available, create them now.
  5. In the 'Available sensors' field, select the desired target's sensor.

- a. Click the first  to select a target component from the list.




b. Click the second  to select the specific sensor for the target from the list.

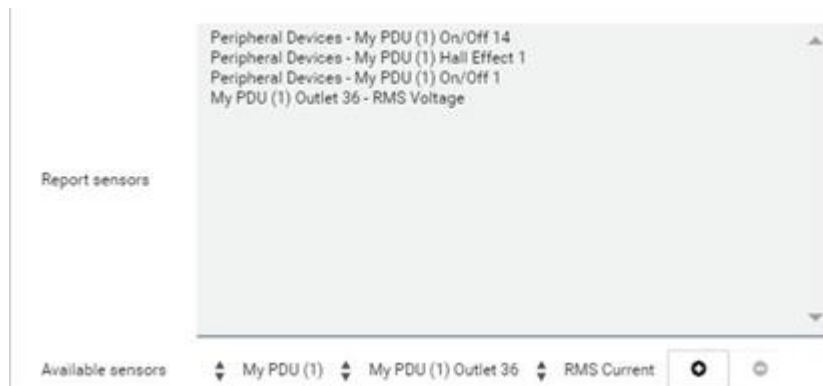


c. Click  to add the selected sensor to the Report Sensors list box.

For example, to monitor the current reading of the Inlet 1, select Inlet 1 from the left field, and then select RMS Current from the right field.

6. To report additional sensors simultaneously, repeat the above step to add more sensors.

- To remove any sensor from the 'Report sensors' list box, select it and click . To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.



7. To immediately send out the sensor report, click Send Report Now.

---

Tip: When intending to send a sensor report using custom messages, use the placeholder [SENSORREPORT] to report sensor readings.

---

### Send SMS Message

You can configure SMS messages to be sent when an event occurs and can customize the message.

A supported modem, such as the Cinterion<sup>®</sup> GSM MC52i modem, must be plugged into the BCM2 in order to send SMS messages.

---

Note: The BCM2 cannot receive SMS messages.


---



Only the 7-bit ASCII charset is supported for SMS messages. Messages consist of a combination of free text and placeholders. The placeholders represent information retrieved from the device and inserted into the message. For example:

```
[USERNAME] logged into the device on [TIMESTAMP]
translates to
Mary logged into the device on 2012-January-30 21:00
```


► *Operation:*

1. Choose Device Settings > Event Rules >  .
2. Select 'Send SMS message' from the Action list.
3. In the 'Recipient phone number' field, specify the phone number of the recipient.
4. Select the 'Use custom log message' checkbox, and then create a custom message in the provided text box.
  - To automatically insert message placeholders, open the Custom Log Message Help section. Search for placeholders and click to include them in your message.
5. Click Create.

### Send Snapshots via Email

This option notifies one or multiple persons for the selected events by emailing snapshots or videos captured by a connected Logitech® webcam.

► *Operation:*

1. Choose Device Settings > Event Rules >  .
2. Select 'Send snapshots via email' from the Action list.
3. In the 'Recipient email addresses' field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
4. By default, the SMTP server specified on the SMTP Server page will be the SMTP server for performing this action.

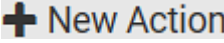
To use a different SMTP server, select the 'Use custom SMTP server' checkbox. The fields for customized SMTP settings appear.
5. Select the webcam that is capturing the images you want sent in the email.
6. Adjust the values of the following:
  - Number of snapshots - the number of snapshots to be taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action.
  - Snapshots per mail - the number of snapshots to be sent at one time in the email.
  - Time before first snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.
  - Time between snapshots - the amount of time in seconds between when each snapshot is taken.
7. If needed, you can customize the subject and messages sent via this email.

- Select the 'Custom subject' checkbox, and enter the text you prefer as this email's subject.
  - Select the 'Use custom log message' checkbox, and then create a custom message up to 1024 characters in the provided field.
  - To automatically insert message placeholders, open the Custom Log Message Help section. Search for placeholders and click to include them in your message.
8. Click Create.

## Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

### ► *Operation:*

1. Choose Device Settings > Event Rules >  .
2. Select 'Send SNMP notification' from the Action list.
3. Select the type of SNMP notification. See either procedure below according to your selection.

### ► *To send SNMP v2c notifications:*

1. In the 'Notification type' field, select 'SNMPv2c trap' or 'SNMPv2c inform.'
2. For SNMP INFORM communications, leave the resend settings at their default or do the following:
  - a. In the Timeout field, specify 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, specify the number of times you want to re-send the inform communication if it fails. For example, inform communications are re-sent up to 5 times when the initial communication fails.
3. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.
4. In the Port fields, enter the port number used to access the device(s).
5. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the BCM2 and all SNMP management stations.

---

Tip: An SNMP v2c notification action permits only 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. In the 'Notification type' field, 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 do the following:
  - a. In the Timeout field, specify 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, specify the number of times you want to re-send the inform communication if it fails. For example, inform communications are re-sent 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 for accessing the host -- make sure the User ID has the SNMPv3 permission.
  - 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"> <li>• Select the authentication protocol - MD5 or SHA</li> <li>• Enter the authentication passphrase and then confirm the authentication passphrase</li> </ul>
"authPriv"	Select this if authentication and privacy protocols are required. <ul style="list-style-type: none"> <li>• Select the authentication protocol - MD5 or SHA</li> <li>• Enter the authentication passphrase and confirm the authentication passphrase</li> <li>• Select the Privacy Protocol - DES or AES</li> <li>• Enter the privacy passphrase and then confirm the privacy passphrase</li> </ul>

### Start or Stop a Lua Script

If you have created or loaded a Lua script file into the BCM2, you can have that script automatically run or stop in response to a specific event.

See [Lua Scripts](#) (on page 243).

► *To automatically start or stop a Lua script:*


1. Choose Device Settings > Event Rules >  .
2. Select 'Start/stop Lua script' from the Action list.
3. In the Operation field, select 'Start script' or 'Stop script.'
4. In the Script field, select the script that you want it to be started or stopped when an event occurs. Scripts must be pre-loaded.
5. To apply different arguments than the default, do the following. Note that the newly-added arguments will override this script's default arguments.
  - a. Click Add Argument.
  - b. Type the key and value.

- To remove any existing argument, click  adjacent to it.

### Switch Outlet Group

The "Switch outlet group" action is available only when your BCM2 is outlet-switching capable. This action turns on, off or power cycles a specific outlet group.


► *Operation:*


1. Choose Device Settings > Event Rules >  .
2. Select 'Switch outlet group' from the Action list.
3. To specify the outlet group where this action will be applied, select it from the 'Group to switch' list.
4. In the Operation field, select an operation for the selected outlet group.
  - Turn on all outlets in group: Turns on the selected outlet group.
  - Turn off all outlets in group: Turns off the selected outlet group.
  - Cycle all outlets in group: Cycles power to the selected outlet group.

### Switch Outlets

The "Switch outlets" action is available only when your BCM2 is outlet-switching capable. This action turns on, off or power cycles a specific outlet.

► *Operation:*

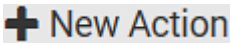

1. Choose Device Settings > Event Rules >  .
2. Select 'Switch outlets' from the Action list.
3. In the Operation field, select an operation for the selected outlet(s).
  - Turn outlet on: Turns on the selected outlet(s).
  - Turn outlet off: Turns off the selected outlet(s).
  - Cycle outlet: Cycles power to the selected outlet(s).

4. To specify the outlet(s) where this action will be applied, select them one by one from the 'Available outlets' list.
  - To add all outlets, click Select All.
5. To remove any outlets from the 'Selected outlets' field, click that outlet's .
6. If 'Turn outlet on' or 'Cycle outlet' is selected, choose to select the 'Use sequence order and delays' checkbox so that all selected outlets will follow the power-on sequence defined on the Outlets page.

### Switch Peripheral Actuator

If you have any actuator connected to the BCM2, you can set up the BCM2 so it automatically turns on or off the system controlled by the actuator when a specific event occurs.

► *Operation:*

1. Choose Device Settings > Event Rules > .
2. Select 'Switch peripheral actuator' from the Action list.
3. In the Operation field, select an operation for the selected actuator(s).
  - Turn on: Turns on the selected actuator(s).
  - Turn off: Turns off the selected actuator(s).
4. To select the actuator(s) where this action will be applied, select them one by one from the 'Available actuators' list.
  - To add all actuators, click Select All.
5. To remove any selected actuator from the 'Selected actuators' field, click that actuator's .

### 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.

BCM2 may or may not detect the syslog message transmission failure. If yes, it will log this syslog failure as well as the failure reason in the event log.

► *Operation:*

1. Choose Device Settings > Event Rules > New Action.
2. Select 'Syslog message' from the Action list.
3. In the 'Syslog server' field, specify the IP address to which the syslog is forwarded.
4. In the 'Transport protocol' field, select one of the syslog protocols: TCP, UDP or TCP+TLS. The default is UDP.

Transport protocols	Next steps
UDP	<ul style="list-style-type: none"> <li>• In the 'UDP port' field, type an appropriate port number. Default is 514.</li> <li>• Select the 'Legacy BSD syslog protocol' checkbox if applicable.</li> </ul>
TCP	NO TLS certificate is required. Type an appropriate port number in the 'TCP port' field.



Transport protocols	Next steps
TCP+TLS	<p>A TLS certificate is required. Do the following:</p> <ol style="list-style-type: none"> <li>a. Type an appropriate port number in the 'TCP port' field. Default is 6514.</li> <li>b. In the 'CA certificate' field, click Browse to select a TLS certificate. After importing the certificate, you may: <ul style="list-style-type: none"> <li>• Click Show to view its contents.</li> <li>• Click Remove to delete it if it is inappropriate.</li> </ul> </li> <li>c. Determine whether to select the 'Allow expired and not yet valid certificates' checkbox. <ul style="list-style-type: none"> <li>• To always send the event message to the specified syslog server as long as a TLS certificate is available, select this checkbox.</li> <li>• 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.</li> </ul> </li> </ol>

## Scheduling an Action

An action can be regularly performed at a preset time interval instead of being triggered by a specific event. For example, you can make the BCM2 report the reading or state of a specific sensor regularly by scheduling the "Send sensor report" action.

When scheduling an action, make sure you have a minimum of 1-minute buffer between this action's creation and first execution time. Otherwise, the scheduled action will NOT be performed at the specified time when the buffer time is too short. For example, if you want an action to be performed at 11:00 am, you should finish scheduling it at 10:59 am or earlier.

### ► Operation:

1. Choose Device Settings > Event Rules >  **New Scheduled Action** .
2. To select any action(s), select them one by one from the 'Available actions' list.
  - To select all available actions, click Select All.
3. To remove any action(s) from the 'Selected actions' field, click that action's  .
  - To remove all actions, click Deselect All.
4. Select the desired frequency in the 'Execution time' field, and then specify the time interval or a specific date and time in the field(s) that appear. Use the clock and calendar tools to choose the schedule. Use the AM/PM button to toggle time settings.

### Send Sensor Report Example

To create a scheduled action for emailing a temperature sensor report hourly, it requires:

- A 'Send email' action
- A 'Send sensor report' action
- A timer - that is, the scheduled action

► Steps:

1. Click **+ New Action** to create a 'Send email' action that sends an email to the desired recipient(s).
  - In this example, this action is named *Email a Sensor Report*.
  - The subject and content of this email can be customized.

The screenshot shows a 'New Action' configuration window. The 'Action name' is 'Email a Sensor Report' and the 'Action' is 'Send email'. The 'Recipient email addresses' field contains 'user@raritan.c'. Under 'SMTP server', 'Use default settings' is selected, with a note that server and sender email addresses are not configured. 'Use custom settings' is unselected. The 'Custom subject' dropdown is set to 'Custom Log Message Help'. The 'Use custom log message' checkbox is checked. The 'Custom log message' text area contains 'The following is the complete sensor report.' followed by '[SENSORREPORT]'. A character count shows '954 characters remaining'. A second 'Custom Log Message Help' dropdown is visible below the text area. At the bottom right are 'Cancel' and 'Create' buttons.

- Click **+ New Action** to create a 'Send sensor report' action that includes the 'Email a Sensor Report' action as its destination action.

- In this example, this action is named *Send Temperature Sensor Readings*.
- You can specify more than one temperature sensor as needed in this action.

**New Action**

Action name: Send Temperature Sensor Readings

Action: Send sensor report

Destination actions: Selected: System Event Log Action X; Available: -- Select an item --

Report sensors: Peripheral Devices - My PDU (1) Temperature 1, Peripheral Devices - My PDU (1) Hall Effect 1, Peripheral Devices - My PDU (1) On/Off 1

Available sensors: My PDU (1), Peripheral Devices, My PDU (1) On/Off 2

Buttons: Send Report Now, Cancel, Create

Note: Reported sensor units can be changed in the Default Preferences

1. Click **+ New Scheduled Action** to create a timer for performing the 'Send Temperature Sensor Readings' action hourly.
  - In this example, the timer is named *Hourly Temperature Sensor Reports*.
  - To perform the specified action at 12:30 pm, 01:30 pm, 02:30 pm, and so on, select Hourly, and set the Minute to 30.



- An email containing the specified temperature sensor readings will be sent hourly every day. If you no longer need the report, you can disable the timer by clearing the Enabled checkbox.

## Placeholders for Custom Messages

Actions that include messages allow you to customize text and include placeholders that retrieve system information and include it in the message.

Supported actions:

- Send email
- Send snapshots via email
- Send SMS
- Log event message

The following are placeholders that can be used in custom messages. Because the placeholders employ square brackets, you must precede with a backslash any other square brackets that must be included in your message. For example, \[ \].

If a placeholder is used in a situation where the information cannot be retrieved, it will be shown as "unknown" in the message.

Placeholder	Definition
[AMSBLADESLOTPOSITION]	The (horizontal) slot position inside a blade extension
[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

<b>Placeholder</b>	<b>Definition</b>
[AMSRACKUNITPOSITION]	The (vertical) rack unit position
[AMSSTATE]	The human-readable state of an asset strip
[AMSTAGID]	The asset tag ID
[CARDREADERCHANNEL]	The channel number of a card reader
[CARDREADERDESCRIPTION]	The custom description of a card reader
[CARDREADERID]	The id of a card reader
[CARDREADERMANUFACTURER]	The manufacturer of a card reader
[CARDREADERNAME]	The custom name of a card reader
[CARDREADERPRODUCT]	The product name of a card reader
[CARDREADERSERIALNUMBER]	The serial number of a card reader
[COMPONENTID]	The ID of a hardware component
[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
[DEVICESERIAL]	The unit serial number of the device the event occurred on
[DIPSWELLDURATION]	The formatted duration of the dip/swell event in seconds
[DIPSWELLVOLTAGE]	The formatted minimum/maximum voltage during the dip/swell event in volts
[DOORACCESSDENIALREASON]	The reason for the door access being denied
[DOORACCESSRULEID]	The id of a door access rule
[DOORACCESSRULENAME]	The name of a door access rule
[ERRORDESC]	The error message
[EVENTRULENAME]	The name of the matching event rule
[EXTPORTNAME]	The name of an external port
[EXTSENSOR]	The peripheral device identifier
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSORSLOT]	The ID of a peripheral device slot

Placeholder	Definition
[FAILURETYPE]	The numeric hardware failure type
[FAILURETYPESTR]	The textual hardware failure type
[FUSESTATENAME]	The human readable state of a fuse
[IFNAME]	The human readable name of a network interface
[INLET]	The inlet label
[INLETLINEPAIR]	The inlet line pair identifier
[INLETPOLE]	The inlet power line identifier
[INLETSENSOR]	The inlet sensor name
[ISASSERTED]	Boolean flag whether an event condition became true (1) or false (0)
[KEYPADCHANNEL]	The channel number of a keypad
[KEYPADDESCRIPTION]	The custom description of a keypad
[KEYPADID]	The id of a keypad
[KEYPADMANUFACTURER]	The manufacturer of a keypad
[KEYPADNAME]	The custom name of a keypad
[KEYPADPIN]	The PIN entered at a keypad
[KEYPADPRODUCT]	The product name of a keypad
[KEYPADSERIALNUMBER]	The serial number of a keypad
[LINKIDTAG]	Link ID prefix for link unit events, empty otherwise
[LINKID]	The link ID of a link unit
[LINKUNITHOST]	The host name or IP address of a link unit
[LOGMESSAGE]	The original log message
[MONITOREDHOST]	The name or IP address of a monitored host
[NETAUTHRESULTSTR]	The network authentication result string ('succeeded' or 'failed')
[NEWUMTARGETUSER]	The new target user of a user rename operation
[OCP]	The overcurrent protector label
[OCPSENSOR]	The overcurrent protector sensor name
[OCPTRIPCAUSELABEL]	The label of the outlet that likely caused the OCP trip
[OCPTRIPCURRENT]	The current flow before the trip event

Placeholder	Definition
[OLDDATETIME]	The device date and time before a clock change
[OLDVERSION]	The firmware version the device is being upgraded from
[OUTLET]	The outlet label
[OUTLETGROUPID]	The outlet group ID
[OUTLETGROUPNAME]	The outlet group name
[OUTLETGROUPSENSOR]	The outlet group sensor name
[OUTLETNAME]	The outlet name <hr/> <b>Note:</b> If any outlet does not have a name, neither an outlet name nor an outlet number will be shown in the custom message for it. Therefore, it is recommended to check the availability of all outlet names if intending to use this placeholder. <hr/>
[OUTLETPOLE]	The outlet power line identifier
[OUTLETSENSOR]	The outlet sensor name
[PDULINEPAIRSENSOR]	The sensor name for a certain line pair
[PDUNUMBER]	The PDU number in a cascade
[PDUPOLESENSOR]	The sensor name for a certain power line
[PDUSENSOR]	The PDU sensor name
[PERIPHDEVPOSITION]	The position of an attached peripheral device
[PHONENUMBER]	The destination phone number of an outgoing SMS message
[PORTID]	The label of the external port the event-triggering device is connected to
[PORTTYPE]	The type of the external port (e.g. 'feature' or 'auxiliary') the event-triggering device is connected to
[RADIUSERRORDESC]	The Radius error message
[ROMCODE]	The romcode of an attached peripheral device
[SENSORREADING]	The value of a sensor reading
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREPORT]	The formatted sensor report contents
[SENSORSTATENAME]	The human readable state of a sensor
[SENSORTHRESHOLDNAME]	The name of the threshold being crossed

Placeholder	Definition
[SENSORTHRESHOLDVALUE]	The value of the threshold being crossed
[SERVERPOWEROPERATION]	The power control operation that was initiated on a server (on/off)
[SERVERPOWERRESULT]	The result of a power control operation
[SMARTCARDID]	The id of a smart card
[SMARTCARDTYPE]	The type of a smart card
[SMTPRECIPIENTS]	The list of recipients of an outgoing mail
[SMTPSERVER]	The name or IP address of an SMTP server
[SYSCONTACT]	SNMP MIB-II sysContact field
[SYSLOCATION]	SNMP MIB-II sysLocation field
[SYSNAME]	SNMP MIB-II sysName field
[TIMEREVENTID]	The id of a timer event
[TIMESTAMP]	The timestamp of the event occurrence
[UMTARGETROLE]	The target role of a user management operation
[UMTARGETUSER]	The target user of a user management operation
[USERIP]	The IP address a user connected from
[USERNAME]	The user who performed an operation
[VERSION]	The firmware version the device is upgrading to

## Editing or Deleting a Rule/Action

You can change the settings of an event rule, action or scheduled action, or delete them.

---

Exception: Some settings of the built-in event rules or actions are not user-configurable. You cannot delete built-in rules and actions.

---

► *To edit or delete an event rule, action or scheduled action:*

1. Choose Device Settings > Event Rules.
2. Click an item in the list of rules, actions or scheduled actions to open its page.
  - To modify settings, make changes and then click Save.
  - To delete it, click the Delete icon then confirm.

## Sample Event Rules

### Sample PDU-Level Event Rule

In this example, we want the BCM2 to record the firmware upgrade failure in the internal log when it happens.

The event rule involves:

- Event: Device > Firmware update failed
- Action: System Event Log Action

► *To create this PDU-level event rule:*

1. For an event at the PDU level, select "Device" in the Event field.
2. Select "Firmware update failed" so that the BCM2 responds to the event related to firmware upgrade failure.
3. To make BCM2 record the firmware update failure event in the internal log, select "System Event Log Action" in the 'Available actions' field.

The screenshot shows a 'New Rule' configuration form. The 'Rule name' field contains 'New Rule 1'. The 'Enabled' checkbox is checked. The 'Event' field is a dropdown menu with 'Device' selected (marked with a circled 1) and 'Firmware update failed' selected (marked with a circled 2). The 'Selected actions' field contains 'System Event Log Action X' (marked with a circled 3). The 'Available actions' field is a dropdown menu with '- Select an item -'. Below the dropdowns are 'Select All' and 'Deselect All' buttons. At the bottom right are 'Cancel' and 'Create' buttons.

### Sample Outlet-Level Event Rule

In this example, we want the BCM2 to send SNMP notifications to the SNMP manager for any sensor change event of outlet 3.

The event rule involves:

- Event: Outlet > Outlet 3 > Sensor > Any sub-event
- Action: System SNMP Notification Action

► *To create this outlet-level event rule:*

1. For an event at the outlet level, select "Outlet" in the Event field.
2. Select "Outlet 3" because that is the desired outlet.
3. Select "Sensor" to refer to sensor-related events.
4. Select "Any sub-event" to include all events related to all sensors of this outlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
5. To make BCM2 send SNMP notifications, select "System SNMP Notification Action" in the 'Available actions' field.

---

*Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action. See Enabling and Configuring SNMP.*

---

The screenshot shows a configuration window for an event rule. On the left, there are labels for 'Event', 'Selected actions', and 'Available actions'. On the right, there are four dropdown menus for the event hierarchy, each with a red number next to it: 'Outlet' (1), 'Outlet 3' (2), 'Sensor' (3), and '<Any sub-event>' (4). Below these is a 'Selected actions' section with a red number 5 next to 'System SNMP Notification Action X'. Underneath is an 'Available actions' dropdown menu with the text '-- Select an item --'. At the bottom, there are buttons for 'Select All', 'Deselect All', 'Cancel', and 'Create'.

Then the SNMP notifications are sent when:

- Any numeric sensor's reading enters the warning or critical range.
- Any sensor reading or state returns to normal.
- Any sensor becomes unavailable.
- The active energy sensor is reset.
- Any state sensor changes its state.

For example, when the outlet 3's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

## Sample Inlet-Level Event Rule

In this example, we want the BCM2 to send SNMP notifications to the SNMP manager for any sensor change event of the Inlet I1.

The event rule involves:

- Event: Inlet > Sensor > Any sub-event
- Action: System SNMP Notification Action

► *To create the above event rule:*

1. For an event at the inlet level, select "Inlet" in the Event field.
2. Select "Sensor" to refer to sensor-related events.
3. Select "Any sub-event" to include all events related to all sensors of this inlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
4. To make the BCM2 send SNMP notifications, select "System SNMP Notification Action" in the 'Available actions' box.

---

*Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action. See [Enabling and Configuring SNMP](#).*

---

The screenshot shows a configuration window for an event rule. On the left, there are labels for 'Event', 'Selected actions', and 'Available actions'. On the right, there are dropdown menus and buttons. The 'Event' dropdown is set to 'Inlet' (marked with a red '1'), 'Sensor' (marked with a red '2'), and '<Any sub-event>' (marked with a red '3'). The 'Selected actions' dropdown is set to 'System SNMP Notification Action X' (marked with a red '4'). The 'Available actions' dropdown is set to '- Select an item -'. Below the dropdowns are 'Select All' and 'Deselect All' buttons. At the bottom right are 'Cancel' and 'Create' buttons.

Then the SNMP notifications are sent when:

- Any numeric sensor's reading enters 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 Inlet I1's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.



## Sample Environmental-Sensor-Level Event Rule

---

---

This section applies to outlet-switching capable models only.

---

---

In this example, we want BCM2 to activate the load shedding function when a contact closure sensor enters the alarmed state. This event rule requires creating a new action before creating the rule.

► *Step 1: create a new action for activating the load shedding*

1. Choose Device Settings > Event Rules > **+ New Action**.
2. In this illustration, assign the name "Activate Load Shedding" to the new action.
3. In the Action field, select "Change load shedding state."
4. In the Operation field, select "Start load shedding."

The screenshot shows a 'New Action' form with the following configuration:

- Action name: Activate Load Shedding (2)
- Action: Change load shedding state (3)
- Operation: Start load shedding (4)
- Selected PDUs: My PDU (1) X
- Available PDUs: -- Select an item --

Buttons: Select All, Deselect All, Cancel, Create

5. Click Create.

After the new action is created, follow the procedure below to create an event rule that triggers the load shedding mode when the contact closure sensor enters the alarmed state. This event rule involves the following:

- Event: Peripheral Device Slot > Slot 1 > State Sensor/Actuator > Alarmed/Open/On
- Trigger condition: Alarmed
- Action: Activate Load Shedding

► *Step 2: create the contact closure-triggered load shedding event rule*

1. Click **+ New Rule** on the Event Rules page.
2. In this illustration, assign the name "Contact Closure Triggered Load Shedding" to the new rule.
3. In the Event field, select "Peripheral Device Slot" to indicate we are specifying an event related to the environmental sensor package.
4. Select the ID number of the desired contact closure sensor. In this illustration, the ID number of the desired contact closure sensor is 1, so select Slot 1.

---

*Note: ID numbers of all sensors/actuators are available on the Peripherals page.*

---

5. Select "State Sensor/Actuator" because the contact closure sensor is a state sensor.
6. Select "Alarmed" since we want the BCM2 to respond when the selected contact closure sensor changes its state related to the "alarmed" state.
7. In the 'Trigger condition' field, select the Alarmed/Open/On radio button so that the action is taken only when the contact closure sensor enters the alarmed state.
8. Select "System Event log Action" from the 'Available actions' list.

**New Rule**

Rule name	New Rule 1
Enabled	<input checked="" type="checkbox"/>
Event	Peripheral Device Slot <b>3</b>
	My PDU (1) On/Off 1 <b>4</b>
	State Sensor / Actuator <b>5</b>
	Alarmed / Open / On <b>6</b>
Trigger condition	<b>7</b> <input checked="" type="radio"/> Alarmed / open / on <input type="radio"/> No longer alarmed / closed / off <input type="radio"/> Both
Selected actions	<b>8</b> System Event Log Action X
Available actions	-- Select an item --

Select All   Deselect All

## A Note about Infinite Loop

You should avoid building an infinite loop when creating event rules.

The infinite loop refers to a condition where the BCM2 keeps busy because the action or one of the actions taken for a certain event triggers an identical or similar event which will result in an action triggering one more event.

► *Example 1*

This example illustrates an event rule which continuously causes the BCM2 to send out email messages.

Event selected	Action included
Device > Sending SMTP message failed	Send email

► *Example 2*

This example illustrates an event rule which continuously causes the BCM2 to send out SMTP messages when one of the selected events listed on the Device menu occurs. Note that <Any sub-event> under the Device menu includes the event "Sending SMTP message failed."

Event selected	Action included
Device > Any sub-event	Send email

► *Example 3*

This example illustrates a situation where two event rules combined regarding the outlet state changes causes the BCM2 to continuously power cycle outlets 1 and 2 in turn.

Event selected	Action included
Outlet > Outlet 1 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 2 (Switch outlets --> Cycle Outlet --> Outlet 2)
Outlet > Outlet 2 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 1 (Switch outlets --> Cycle Outlet --> Outlet 1)

## A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing an alert. The measurement then returns to a value within the threshold, but the BCM2 does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the BCM2 uses. See "To De-assert" and Deassertion Hysteresis.

## Setting Data Logging

The data log stores records of each internal sensor's readings. You can configure the log capacity and the frequency that measurements are taken and stored. The total size of the data log is limited due to memory constraints. For example, for a PDU with 500 sensors, the effective log size cannot be more than 200 records. A log capacity warning appears if the desired log capacity is higher than the effective log capacity.

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field. Since the 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. 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.

The device's SNMP agent must be enabled. In addition, using an NTP time server ensures accurately time-stamped measurements.

By default, data logging is enabled. You must have the "Administrator Privileges" or "Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration" permissions to change the setting.

---

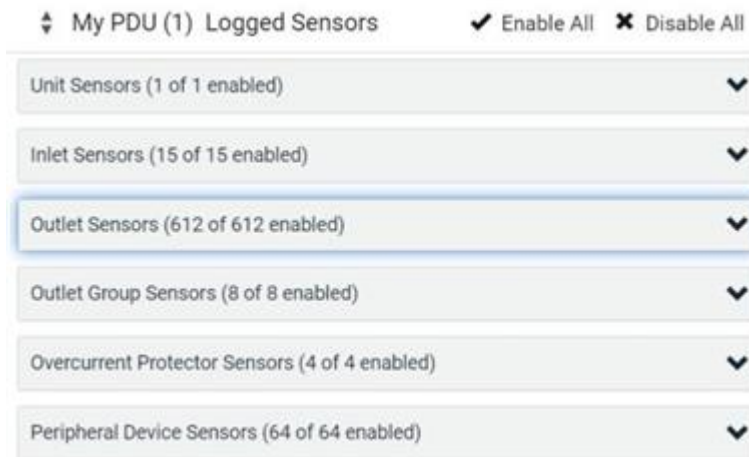
Important: The third-party management solutions like PowerIQ rely on the data logging feature, and the settings should be changed only in accordance with those systems' requirements.

---

► *To configure the data logging feature:*

1. Choose Device Settings > Data Logging.
2. To enable the data logging feature, select the "Enable" checkbox in the General Settings section.
3. Measurements Per Log Entry: Valid range is from 1 to 600. The default is 60.
4. Log capacity: Valid range varies, from 60 to 20,000.
5. Enable data log backup: Select this checkbox to enable an automatic USB backup of your data log. USB stick with specially configured file required, see procedure below.
6. Verify that all sensor logging is enabled. If not, click Enable All at the bottom of the page to have all sensors selected.
7. Click Save.

Data Logging	
Enable data logging	<input checked="" type="checkbox"/>
Measurements per log entry	<input type="text" value="60"/>
Desired log capacity	<input type="text" value="120"/>
Enable data log backup	<input checked="" type="checkbox"/>



► **Enable Data Log Backup:**

This feature allows backup of the data log on a USB drive. When the BCM2 reboots, e.g because of a power outage, it will repopulate the data log from the backup on the USB Stick.

**To Prepare USB:**

Before connecting a USB drive to the BCM2, configure a file with these details:

1. Create a text file containing:
  - user=<admin\_username>
  - password=<admin\_user\_password>
  - destroy\_and\_format\_for\_storage=true
2. Save the file as "fwupdate.cfg" on the USB drive.
3. Make sure the Enable Data log backup checkbox is selected in Device Settings > Data Logging.
4. Connect the USB drive to the device.

On the console of the BCM2, you will see the USB drive is reformatted and existing contents are removed. Once formatting is done, data is started to be backed up on the USB.

---

Note: Backed up data on the USB is in encrypted form.

---

## Configuring Data Push Settings

You can push the sensor or asset strip data to a remote server for data synchronization. The destination and authentication for data push have to be configured properly on the BCM2.


HTTP/HTTPS Destinations: The data will be sent in JSON format using HTTP POST when you select HTTP or HTTPS as the destination URL. Each push message contains exactly one JSON object. The data format is formally defined in IDL files, sharing several definitions from the JSON-RPC data model. IDL files are available by launching *JSON-RPC online help*, which is available on the Support site for your product.

MQTT Destinations: If MQTT is selected as the protocol, only data of the latest log row will be sent. The records of this log row are published under multiple topic names, one for each logged sensor.

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

- To perform the data push after the occurrence of a certain event, create the data push action and assign it to an event rule.
- To push the data at a regular interval, schedule the data push action.

► *To configure data push settings:*

1. Choose Device Settings > Data Push.
2. To specify a destination, click New Destination.
3. Set up the URL field.
  - a. Select *http*, *https*, or *MQTT*.
  - b. Type the URL or host name in the accompanying text box.
4. If selecting *https*, a CA certificate is required for making the connection. Click Browse to install it. Then you can:
  - Click Show to view the certificate's content.
  - Click Remove to delete the installed certificate if it is inappropriate.
5. If the destination server requires authentication, select the 'Use authentication' checkbox, and enter the following data.
  - User name comprising up to 64 characters
  - Password comprising up to 128 characters
6. In the 'Entry type' field, determine the data that will be transmitted.
  - *Asset management tag list*: Transmit the information of the specified asset strip(s), including the general status of the specified strip(s) and a list of asset tags. The asset tags list also includes the tags on blade extension strips, if any.
  - *Asset management tag log*: Transmit the log of all asset strips, which is generated when there are changes made to asset tags and asset strips, including asset tag connection or disconnection events.
  - *Sensor log*: Transmit the record of all logged sensors, including their sensor readings and/or status. Logged sensors refer to all internal and/or environmental sensors/actuators that you have selected on the Data Logging page.
7. If 'Asset management tag list' is selected in the above step, specify the asset strip(s) whose information to send. Depending on your PDU model, only one strip may be available.
  - To specify the asset strip(s), select them one by one from the Available AMS Ports list. Or click Select All to add all.
  - To remove the asset strip(s), click that asset strip's  in the Selected AMS Ports field. Or click Deselect All to remove all.
8. Click Create.
9. Repeat the same steps for additional destinations. Up to 64 destinations are supported.

► *To immediately push out the data:*

1. On the Data Push page, choose the data source you want to push out.
2. Click the Push Now button.

► *To cancel a data push:*

- You can cancel the push in progress: Click Cancel.

► *To modify or delete data push settings:*

1. On the Data Push page, click the one you want in the list.
2. Perform either action below.
  - To modify settings, make necessary changes and then click Save.
  - To delete it, click Delete, and then confirm it on the confirmation message.

## Data Push Format Examples

### Sensor Log

The root object of the message is a `SensorLogPushMessage` structure. It comprises a list of sensor descriptors and a list of log rows.

► *Sensor descriptors:*

The sensor descriptor vector contains static information of all logged sensors, including:

- The electrical component a sensor is associated with. For example, an inlet pole or an overcurrent protector.
- The sensor's type. For example, RMS current or active energy.
- Unit and range of the sensor's readings.

► *Log rows:*

Each log row consists of a time stamp (accumulated seconds since 1/1/1970) and a list of log records -- one for each logged sensor.

The length and order of the record list is the same as the sensor descriptor vector.

### Sensor Descriptors for Inlet Active Power

The following illustrates a descriptor for an inlet active power sensor.

The `metadata` field is relevant only to numeric sensors so the `readingtype` field is displayed twice in the illustration.

The comment beginning with `//` in each line, is added to the following illustration to help explain it.

```

{
  "device": {
    "type": 0,           // Inlet sensor (see DeviceType enumeration)
    "label": "I1",      // Inlet label: I1
    "line": 0           // Power line; not applicable for inlet sensors
  },
  "id": "activePower", // Sensor identification
  "readingtype": 0,    // Reading type: numeric
  "metadata": {
    "type": {
      "readingtype": 0, // Reading type: numeric
      "type": 5,        // Sensor type: Active power
      "unit": 3         // Reading unit: Watt
    },
    "decdigits": 0,    // No decimal digits
    "accuracy": 1.0,   // Accuracy: 1 percent
    "resolution": 1.0, // Reading resolution: 1 W
    "tolerance": 1.5,  // Reading tolerance: +/- 1.5 W
    "range": {
      "lower": 0.0,    // Minimum reading: 0 W
      "upper": 30000.0 // Maximum reading: 30 kW
    }
  }
}

```

## Log Rows

The following illustrates log rows with only one sensor record shown.

The actual length and order of log rows will be the same as those of sensors descriptors.

The comment beginning with // in each line, is added to the following illustration to help explain it.

```

{
  "timestamp": 1334052852, // Time stamp (seconds since 1/1/1970)
  "records": [
    {
      "available": true,    // This record is available
      "takenValidSamples": 60, // Number of valid samples in this log period
      "state": 5,          // Sensor was in normal range
      "minValue": 5800.0,  // Minimum sensor value: 5.8 kW
      "avgValue": 5900.0,  // Average sensor value: 5.9 kW
      "maxValue": 6100.0   // Maximum sensor value: 6.1 kW
    },
    {
      // [...] record for next sensor
    }
  ]
}

```

## Asset Management Tag List

The root object of the asset management tag list message is an `AssetStripsMessage` structure. It contains current data about all connected asset management strips and tags, which is similar to the illustration below.



```

{
  "assetStrips": [
    {
      "stripInfo": {
        "bladeOverflow": false,
        "bladeTagCount": 0,
        "cascadeState": 0,
        "componentCount": 1,
        "mainTagCount": 2,
        "maxBladeTagCount": 128,
        "maxMainTagCount": 64,
        "rackUnitCount": 48
      },
      "deviceInfo": {
        "appVersion": 24,
        "bootVersion": 6,
        "deviceId": 48,
        "hardwareId": 2,
        "isCascadable": false,
        "orientationSensAvailable": true,
        "protocolVersion": 257,
        "rackUnitCountConfigurable": true
      },
      "settings": {
        "rackUnitCount": 48,
        "name": "Asset Strip 1",
        "scanMode": 0,
        "defaultColorConnected": { "r": 0, "g": 255, "b": 0 },
        "defaultColorDisconnected": { "r": 255, "g": 0, "b": 0 },
        "numberingMode": 1,
        "numberingOffset": 1,
        "orientation": 0
      }
    },
  ],
}

```

*(Continued)*

```

    "tags": [
      {
        "rackUnitNumber": 4,
        "slotNumber": 0,
        "familyDesc": "Unknown",
        "rawId": "DEADBEEF0000",
        "programmable": 0
      },
      {
        "rackUnitNumber": 5,
        "slotNumber": 0,
        "familyDesc": "Unknown",
        "rawId": "DEADBEEF0500",
        "programmable": 0
      }
    ]
  }
}

```

## Asset Management Tag Log

The root object of the asset management log message is an `AssetLogPushMessage` structure. It contains a list of tag or strip events since the last successful push.

The comment beginning with `//` in each line, is added to the following illustration to help explain it.

```
{
  "records": [
    {
      "timestamp": 1334052852, // Time stamp (seconds since 1/1/1970)
      "type": 1, // 0: empty, 1: tag connected, 2: tag disconnected,
                // 3: asset strip state changed
      "assetStripNumber": 0, // Asset strip number
      "rackUnitNumber": 10, // Rack unit number
      "rackUnitPosition": 12, // Rack unit position
      "slotNumber", // Blade extension slot number
      "tagId", // The ID of the asset management tag
      "state": 5, // Sensor was in normal range
      "parentBladeId", // ID of the parent blade extension tag
      "state": 0 // 0: disconnected, 1: firmware update,
                // 2: unsupported, 3: available
    },
    {
      // [...] next record
    }
  ]
}
```

## Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the BCM2 continuously ping them. An IT device's successful response to the ping commands indicates that the IT device is still alive and can be remotely accessed.

This function is especially useful when you are not located in an area with Internet connectivity.

BCM2 can monitor any IT device, such as database servers, remote authentication servers, power distribution units (PDUs), and so on. It supports monitoring a maximum of 64 IT devices.

To perform this feature, you need the Administrator Privileges.

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 for optimal results.

In addition, if your BCM2 is outlet switching capable, you can even connect a monitored IT device to one or multiple outlets of BCM2 and then have BCM2 perform the following two actions as needed, in addition to monitoring its status:


- First shut down the monitored IT device.
- After the IT device is shut down, power off the outlet(s) where that device is connected.

---

**Important: Not every IT device can be shut down by BCM2 so it is suggested to verify whether the device can be shut down using a shutdown command. For example, BCM2 cannot shut down a PDU with a shutdown command.**

---

► *To add IT equipment for ping monitoring:*

1. Choose Device Settings > Server Reachability.
2. Click  **Monitor New Server**.
3. By default, the "Enable ping monitoring for this server" checkbox is selected. If not, select it to enable this feature.
4. Configure the following.

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.
Wait time 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 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 before resuming pinging after failure	The wait time before the BCM2 resumes pinging after the monitored equipment is declared "Unreachable." Valid range is 1 to 1200 (seconds).
Number of consecutive failures before disabling feature (0 = unlimited)	The number of times the monitored equipment is declared "Unreachable" consecutively before the BCM2 disables the ping monitoring feature for it and shows "Waiting for reliable connection." Valid range is 0 to 100.

5. On a PDU with outlet switching capability, there is one more checkbox available -- *Power control enabled*.

To be able to shut down and power control the monitored IT device via the Server Reachability page, enable this checkbox and configure related settings, which are explained in the following table.

6. Click Create.
7. To add more IT devices, repeat the same steps.

► *To configure the shutdown and power control settings:*

---



---

Restriction: To make the power control feature work properly, the power cord(s) of the monitored IT device must be connected to the same PDU which is monitoring the IT device.

---



---

Field	Description
Shutdown command	<p>This is the command which is sent to the monitored IT device via SSH for shutting it down after you press the Shutdown button on BCM2.</p> <ul style="list-style-type: none"> <li>• <i>GNU/Linux:</i> This option sends the GNU/Linux shutdown command.</li> <li>• <i>Windows:</i> This option sends the Windows shutdown command.</li> <li>• <i>Custom:</i> If the monitored device's system is neither GNU/Linux nor Windows, choose this option to specify a proper shutdown command, which can comprise a maximum of 1024 ASCII characters.</li> </ul>
User name, Password	<p>Specify user credentials for logging in to the monitored device via SSH.</p> <ul style="list-style-type: none"> <li>• <i>User name:</i> The name comprises up to 128 non-empty ASCII characters.</li> <li>• <i>Password:</i> The password comprises up to 128 ASCII characters.</li> </ul>
SSH port	<p>The monitored device's SSH port.</p> <ul style="list-style-type: none"> <li>• Default is 22.</li> </ul>
Power target to switch	<p>Select the outlet or outlet group that is powering the monitored device.</p>
Method of checking successful shutdown	<p>This field determines when BCM2 will power off the outlet(s) that supplies power to the monitored device, after BCM2 issues the shutdown command to that device.</p> <ul style="list-style-type: none"> <li>• <i>Timer:</i></li> <li>• BCM2 will power off the selected outlet or outlet group after the time specified in the 'Timer delay' field expires. <i>Active power drop:</i> BCM2 will power off the selected outlet(s) after the active power value of the selected outlet or outlet group drops below the value specified in the 'Active power threshold' field.</li> </ul> <hr/> <p>Note: Number of available methods is model dependent. The 'Active power drop' method is available only on models with outlet metering capability.</p> <hr/>

Field	Description
Timer delay	<p>This field appears for the 'Timer' method.</p> <p>Valid values range between 5 and 10,000 seconds.</p>
Active power threshold	<p>The field appears for the 'Active power drop' method.</p> <p>Valid values range between 0 and 21,000 W.</p>
Timeout for shutdown check	<p>This field appears for the 'Active power drop' method.</p> <p>Valid values range between 5 and 10,000 seconds.</p> <p>The power-off operation is performed only when the active power value of the selected outlet or outlet group drops below the 'Active power threshold' within the period of time specified in this field.</p> <p>If the active power value drops below the 'Active power threshold' after the specified time expires, the power-off operation will NOT be performed.</p>

## Server Status Checking or Power Control

Not all models supports the shutdown and power control features via the Server Reachability page.

After adding IT equipment for monitoring, all IT devices are listed on the Server Reachability page.

IP Address/Hostname	Ping Enabled	Status	Power Control
192.168.3.55	yes	Waiting for reliable connection	(disabled)
www.legrand.com	yes	Error	Server power is off

In the beginning, the status of the added IT equipment shows "Waiting for reliable connection," which means the requested number of consecutive successful or unsuccessful pings has not reached before BCM2 can declare that the monitored device is reachable or unreachable.

► *To check the server monitoring states and results:*

1. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.
2. The column labeled "Status" indicates the accessibility of monitored equipment.

Status	Description
Reachable	The monitored equipment is accessible.
Unreachable	The monitored equipment is inaccessible.
Waiting for reliable connection	The connection between the device and the monitored equipment is not reliably established yet.

3. If your model supports outlet switching, one more column displays -- *Power Control*.

Power control status	Description
(disabled)	Power control is not enabled for the monitored equipment.
Server power is on	The outlet or outlet group associated with the monitored equipment is being powered on. <ul style="list-style-type: none"> <li>In the scenario where an 'outlet group' is associated with the equipment, the message 'Server power is on' is shown as long as one of the outlets in the outlet group remains powered on.</li> </ul>
Server power is off	The outlet or all outlets of the outlet group associated with the monitored equipment are being powered off.
Server is shutting down	The shutdown command was sent to the monitored equipment, but the shutdown operation has not completed or succeeded yet.
Power state unknown	Cannot determine the power state of the outlet(s) associated with the monitored device.  For example, maybe the outlet group associated with the monitored device has been deleted.

► *To shut down a monitored device:*

1. Select the IT device that you want to shut down.
2. Click Shutdown.
3. Confirm the operation when prompted.
4. Observe the Power Control status of the monitored device to make sure the shutdown operation succeeds.

► *To power on a monitored device:*

1. Select the IT device that you want to turn on.
2. Click Power Up.
3. Confirm the operation when prompted.
4. Observe the Power Control status of the monitored device to make sure the power-on operation succeeds.

## Editing or Deleting Ping Monitoring Settings

You can edit the ping monitoring settings of any IT device or simply delete it if no longer needed.

► *To modify or delete any monitored IT device:*

1. Choose Device Settings > Server Reachability.
2. Click the desired one in the list.
3. Perform the desired action.

- To modify settings, make necessary changes and then click Save. To delete it, click on the top-right corner.



## Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your BCM2 to make sure that PDU is properly operating all the time, and the BCM2 must send out SNMP notifications (trap or inform) if that PDU is declared unreachable due to power or network failure. The prerequisite for this example is that the power sources are different between your BCM2 and the monitored PDU.

This requires the following two steps.

► *Step 1: Set up the ping monitoring for the target PDU*

1. Choose Device Settings > Server Reachability.
2. Click .
3. Ensure the "Enable ping monitoring for this server" checkbox is selected.
4. Enter the data shown below.

- Enter the server's data.

Field	Data entered
IP address/hostname	192.168.84.95

- To make the BCM2 declare the accessibility of the monitored PDU every 15 seconds (3 pings \* 5 seconds) when that PDU is accessible, enter the following data.

Field	Data entered
Number of successful pings to enable feature	3
Wait time after successful ping	5

- To make the BCM2 declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 seconds \* 3 pings), enter the following data.

Field	Data entered
Wait time after unsuccessful ping	4

Field	Data entered
Number of consecutive unsuccessful pings for failure	3

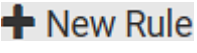
- To make the BCM2 stop pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared, enter the following data. After 60 seconds, the BCM2 will re-ping the target PDU,

Field	Data entered
Wait time before resuming pinging after failure	60

- The "Number of consecutive failures before disabling feature (0 = unlimited)" can be set to any value you want.

5. Click Create.

► *Step 2: Create an event rule to send SNMP notifications for the target PDU*

1. Choose Device Settings > Event Rules.
2. Click  .
3. Select the Enabled checkbox to enable this new rule.
4. Configure the following.

Field/setting	Data specified
Rule name	Send SNMP notifications for PDU (192.168.84.95) inaccessibility
Event	Choose Server Monitoring > 192.168.84.95 > Unreachable
Trigger condition	Select the Unreachable radio button

This will make the BCM2 react only when the target PDU becomes inaccessible.

5. Select the System SNMP Notification Action.

## Front Panel Settings

You can set up the default mode of the front panel display, and front panel functions for outlet switching, actuator control, beeper mute or RCM self-test.

Note that available front panel settings are model dependent.

- Outlet switching -- available on outlet-switching capable models only.
- Actuator control -- available on all models.
- Internal beeper's mute function -- available on all models
- Default front panel mode setup -- available on all models, except for the PX3-3000 series, which does NOT provide inlet sensor information.
- RCM self-test -- available on those models which support residual current monitoring.



► *To configure the front panel settings:*

1. Choose Device Settings > Front Panel.
2. Configure the following:
  - To configure the default view of the LCD display, select one mode below.

---

*Note: The default view is shown in the automatic mode.*

---

Mode	Data entered
Automatic mode	The LCD display cycles through both the inlet and overcurrent protector information. This is the default.  Overcurrent protector information is available only when your BCM2 has overcurrent protectors.
Inlet overview	The LCD display cycles through the inlet information only.

- To enable the front panel outlet-switching function, select the 'Outlet switching' checkbox.
  - To enable the front panel actuator-control function, select the 'Peripheral actuator control' checkbox.
  - The built-in beeper's mute control function is enabled per default. To disable it, deselect the 'Mute beeper' checkbox.
  - By default the front panel RCM self-test function, if available, is enabled.
3. Click Save.

If the 'Mute beeper' feature is enabled, you can operate the front panel to mute it whenever it beeps.

Or you can turn on or off outlets/actuators by operating the front panel.

## Configuring the Serial Port

You can change the bit rate of the serial port labeled CONSOLE / MODEM that is present on some models. The default bit rate for console and modem operation is 115200 bps.

The following devices are supported via the serial interface:

- A computer for console management.
- A Raritan KVM product.
- An analog modem for remote dial-in and access to the CLI.
- A GSM modem for sending out SMS messages to a cellular phone.

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

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

The BCM2 will indicate the detected device in the Port State section of the Serial Port page.

To configure serial port and modem settings, choose Device Settings > Serial Port.

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

1. Click the 'Connected device' field to make the serial port enter an appropriate state.

Options	Description
Automatic detection	The BCM2 automatically detects the type of the device connected to the serial port. Select this option unless your BCM2 cannot correctly detect the device type.
Force console	The BCM2 attempts to recognize that the connected device is set for the console mode.
Force analog modem	The BCM2 attempts to recognize that the connected device is an analog modem.
Force GSM modem	The BCM2 attempts to recognize that the connected device is a GSM modem.

2. Click the 'Console baud rate' field to select the baud rate intended for console management.

---

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

---

3. Click the 'Modem baud rate' field to select the baud rate for the modem connected to the BCM2.

The following modem settings/fields appear in the web interface after the BCM2 detects the connection of an analog or GSM modem.

► *To configure the analog modem:*

1. Select the 'Answer incoming calls' checkbox to enable the remote access via a modem. Otherwise, deselect it.
2. Type a value in the 'Number of rings before answering' field to determine the number of rings the BCM2 must wait before answering the call.

► *To configure the GSM modem:*

1. Enter the SIM PIN code.
2. Select the 'Use custom SMS center number' checkbox if a custom SMS center will be used.
  - Enter the SMS center number in the 'SMS center' field.
3. If needed, click Advanced Information to view detailed information about the modem, SIM and mobile network.
4. To test whether the BCM2 can successfully send out SMS messages with the modem settings:
  - a. Enter the number of the recipient's phone in the Recipient Phone field.
  - b. Click Send SMS Test to send a test SMS message.

## Lua Scripts

If you can write or obtain any Lua scripts, you can create or load them into the BCM2 to control its behaviors.

Some Lua scripts examples are provided, which you can load as needed.

---

Note: Not all Lua script examples can apply to your BCM2 model. You should read each example's introduction before applying them.


---

You must have the Administrator Privileges to manage Lua scripts.

## Writing or Loading a Lua Script

You can enter or load up to 4 scripts.

► *To write or load a Lua script:*

1. Choose Device Settings > Lua Scripts >  .
2. Type a name for this script. Its length ranges between 1 to 63 characters.

The name must contain the following characters only.

- Alphanumeric characters
- Underscore (\_)
- Minus (-)

---

*Note: Spaces are NOT permitted.*

---

3. Determine whether and when to automatically execute the loaded script.

Checkbox	Behavior when selected
Start automatically at system boot	Whenever the BCM2 reboots, the script is automatically executed.
Restart after termination	The script is automatically executed each time after 10 seconds since the script execution finishes.

4. (Optional) Determine the arguments that will be executed by default.



- a. Click
- b. Type the key and value.
- c. Repeat the same steps to enter more arguments as needed.

- To remove any existing argument, click  adjacent to it.

---

*Note: The above default arguments will be overridden by new arguments specified with the "Start with Arguments" command or with any Lua-script-related event rule.*

---

5. In the Source Code section, do one of the following. It is recommended to leave the Enable Syntax Highlighting checkbox selected unless you do not need different text colors to identify diverse code syntaxes.

- To write a Lua script, type the codes in the Source Code section.



- To load an existing Lua script file, click Load Local File.
- To use one of the default Lua script examples, click Load Example.

---

*Warning: The newly-loaded script will overwrite all existing codes in the Source Code section. Therefore, do not load a new script if the current script meets your needs.*

---

6. If you chose to load a script or the example in the previous step, its codes are then displayed in the Source Code section. Double check the codes. If needed, modify the codes to meet your needs.
7. Click Create.

## Manually Starting or Stopping a Script

You can manually start or stop an existing Lua script at any time.

When starting a script, you can choose to start it either with its default arguments or with new arguments.

---

Tip: To have the BCM2 automatically start or stop a script in response to an event, create an event rule.

---

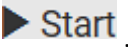
### ► To manually start a script:

1. Choose Device Settings > Lua Scripts. The Lua scripts list displays.



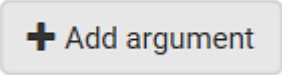
<input type="checkbox"/>	Name	State	Autostart	Restart
<input type="checkbox"/>	script-1	New	yes	no
<input type="checkbox"/>	script-2	New	no	yes
<input type="checkbox"/>	test	New	no	no

2. Click the desired script whose state is either 'Terminated' or 'New.'

3. To start with default arguments, click .

To start with new arguments, click  > Start With Arguments. Newly-assigned arguments will override default ones.

4. If you chose "Start With Arguments" in the above step, enter the key and value in the Start Lua Script dialog.

- Click  if needing additional arguments.

← Lua Scripts | New Script

**Settings**

Name


Start options  
 Start automatically at system boot  
 Restart after termination

Default arguments


Key	Value	
required	required	-

[+ Add Argument](#)

5. Click Start.
6. The script output will be shown in the Script Output section.

- If needed, click  **Clear** to delete the existing output data.

► *To manually stop a script:*

1. Choose Device Settings > Lua Scripts.
2. Click the desired script whose state is either 'Running' or 'Restarting.'
3. Click  **Stop** on the top-right corner.
4. Click Stop on the confirmation message.

## Checking Lua Scripts States

Choose Device Settings > Lua Scripts to show the scripts list, which indicates the current state and settings of each script.

Lua Scripts				<a href="#">Delete</a>	<a href="#">+ Create New Script</a>
<input type="checkbox"/>	Name	State	Autostart	Restart	
<input type="checkbox"/>	script-1	Terminated	yes	no	
<input type="checkbox"/>	script-2	Terminated	no	yes	
<input type="checkbox"/>	test	New	no	no	

► *State:*

State	Description
New	The script is never executed since the device boot.
Running	The script is currently being executed.

State	Description
Terminated	The script was once executed, but stops now.
Restarting	The script will be executed. Only the scripts with the "Restart" column set to "yes" will show this state.

► *Autostart:*


This column indicates whether the checkbox labeled "Start automatically at system boot" is enabled. .

► *Restart:*


This column indicates whether the checkbox labeled "Restart after termination" is enabled.

## Modifying or Deleting a Script

► *To modify or replace a script:*

1. Choose Device Settings > Lua Scripts.
2. Click the desired one in the scripts list.
3. Click  > Edit Script.
4. Make changes to the information shown, except for the script's name, which cannot be revised.
  - To replace the current script, click Load Local File or Load Example to select a new script.

► *To delete a script:*

1. Choose Device Settings > Lua Scripts.
2. Click the desired one in the scripts list.
3. Click  > Delete.
4. Click Delete on the confirmation message.

## Miscellaneous

The Miscellaneous page contains some assorted settings.

► *Enable USB Host Ports:*

- If you want to enable/disable your BCM2 USB host ports, use this checkbox.

When disabled, the following features are unavailable:

- Wireless networking
- USB cascading
- USB configuration and firmware update
- Webcam support
- USB card reader support
- PDView mobile app for iOS

► *Enable Crestron XiO Connection:*

- If the Crestron XiO connection is part of your configuration, you can enable/disable it here.



## Using Prometheus and Grafana

You can use the open-source tools Prometheus and Grafana to collect sensor data and visualize it. In Prometheus, the sensor readings are stored locally as time series data, which can be visualized in graphs created by Grafana or similar tools. This information is displayed on dashboards, and you can create multiple dashboards as needed.

## Requirements for Prometheus and Grafana

► *Prometheus Requirements:*

- Prometheus v2.0 or higher
- Install on a computer in the BCM2 network.
- Reference: [https://prometheus.io/docs/introduction/first\\_steps/](https://prometheus.io/docs/introduction/first_steps/)



► *Grafana requirements:*

- Grafana v8.1.5 or higher
- Install on a computer in the network of the Prometheus instance.
- Reference: <https://grafana.com/grafana/download?pg=get&plcmt=selfmanaged-box1-cta1>

## Collected Data

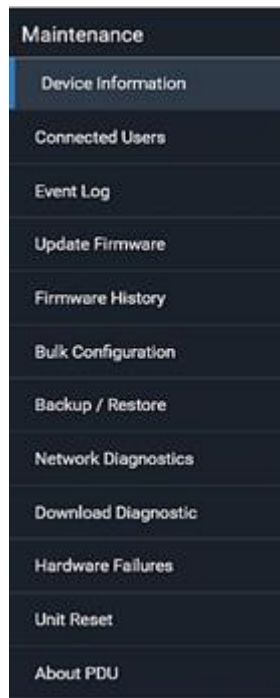
For integration into a Prometheus system, the PDU can output all measurements in a Prometheus-compatible format that can be queried from the URL: 'https://<PDU\_IP>/cgi-bin/dump\_prometheus.cgi'. The URL has one optional parameter, "include\_names=1", to include PDU, names for Inlet, Outlet, OCP, TransferSwitch, and Sensors as metric labels.

You can use cURL as follows to retrieve the data:

1. `curl -k https://username:password@[PDU_IP]/cgi-bin/dump_prometheus.cgi`
2. `curl -k https://username:password@[PDU_IP]/cgi-bin/dump_prometheus.cgi?include_names=1`

## Maintenance

Click 'Maintenance' in the *Menu* to view the options.



## Device Information

The Device Information page displays hardware and software information of components or connected peripheral devices.

---

Tip: If the information shown on this page does not match the latest status, press F5 to reload it.

---

► *To display device information:*

1. Choose Maintenance > Device Information. Click any header to expand the information. Available sections depend on your model.

Section title	Information shown
Information	General device information, such as model name, serial number, firmware version, board ID and revision, MIB download link(s) and so on.  iX7-G1 hardware or newer shows both Board ID and revision.
Network	The network information, such as the current networking mode, IPv4 and/or IPv6 addresses and so on.  Information on cascading configurations also shows here.
Port Forwarding	If the port forwarding mode is activated, this section shows a list of port numbers for all cascaded devices.
Outlets	Each outlet's receptacle type, operating voltage and rated current.
Overcurrent Protectors	Each overcurrent protector's type, rated current and the outlets that it protects.
Controllers	Each inlet or outlet controller's serial number, Device ID, Hardware ID, Firmware Version and Status.
Peripheral Devices	Serial numbers, model names, position and firmware-related information of connected environmental sensor packages. <hr/> <i>Note: Serial number when clicked provides the detail information of the peripheral device.</i> <hr/>
Asset Management	Each asset strip's ID, boot version, application version and protocol version.
Security	SSH host keys.

## Viewing Connected Users

You can check which users are logged in and their status. If you have administrator privileges, you can terminate any user's connection.

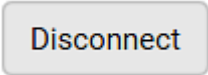
► *To view and manage connected users:*

1. Choose Maintenance > Connected Users. A list of logged-in users displays.

Connected Users Disconnect

<input type="checkbox"/> User Name ▲	IP Address	Client Type	Idle Time
admin	192.168.49.50	Web GUI	0 min

Column	Description
User Name	The login name of each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (serial RS-232 or USB), <local> is displayed instead of an IP address.
Client Type	The interface through which the user is being connected to the BCM2. <ul style="list-style-type: none"> <li>• Web GUI: Refers to the web interface.</li> <li>• 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"> <li>- Serial: The local connection, such as the serial RS-232 or USB connection.</li> <li>- SSH: The SSH connection.</li> <li>- Telnet: The Telnet connection.</li> </ul> </li> <li>• Webcam Live Preview: Refers to the live webcam image sessions. See below.</li> </ul>
Idle Time	The length of time for which a user remains idle.



2. To disconnect any user, click the corresponding
  - a. Click Disconnect on the confirmation message.
  - b. The disconnected user is forced to log out.

► *If there are live webcam sessions:*

All Live Preview window sessions sharing the same URL, including one Primary Standalone Live Preview window and multiple Secondary Standalone Live Preview windows, are identified as one single "<webcam>" user in the Connected Users list. You can disconnect a "<webcam>" user to terminate all sessions sharing the same URL.

User Name ▲	IP Address	Client Type	Idle Time	
<webcam>	192.168.84.22	Webcam Live Preview	0 min	Disconnect

The IP address refers to the IP address of the host where the Primary Standalone Live Preview window exists, NOT the IP address of the other two associated sessions.

## Viewing, Pausing, Resuming or Clearing the Local Event Log

By default, certain system events are captured and saved in a local event log.

You can view over 2000 historical events in the local event log. When the log size exceeds 256KB, each new entry overwrites the oldest one.

### ► To display the local event log:

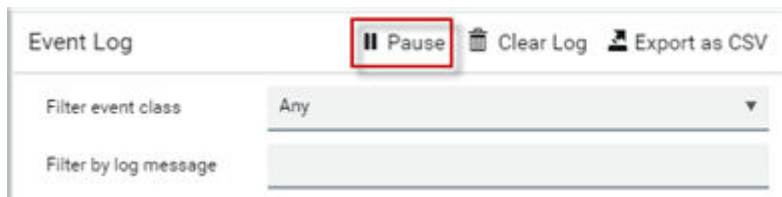
1. Choose Maintenance > Event Log.

Each event entry consists of:

- ID number of the event
  - Date and time of the event
  - Event type
  - A description of the event
2. To filter the list, select the desired event type in the 'Filter event class' field, or enter keywords in the 'Filter by log message' field.
  3. The log is refreshed automatically at a regular interval of five seconds. To avoid any new events' interruption during data browsing, you can suspend the automatic update by clicking Pause.
    - To restore automatic update, click Resume. Those new events that have not been listed yet due to suspension will be displayed in the log now.

### ► To Pause & Resume the local log:

1. Click Pause on the top right corner.



GUI temporarily stops displaying Event Log updates and button label shows 'Resume'.

2. Click Resume on the top right corner.

GUI continues displaying Event Log updates and shows also messages which were skipped when paused. The Button label shows 'Pause'.

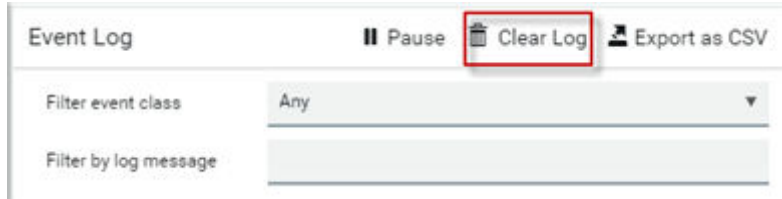
---

Note: After page change, Event Log list is automatically in 'Resumed' state again.

---

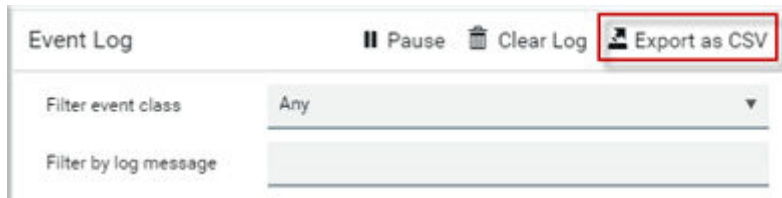
### ► To clear the local log:

1. Click Clear Log on the top-right corner.
2. Click Clear Log on the confirmation message.



► *To export the log:*

1. Click Export as CSV on top right corner.
2. CSV file gets downloaded to local machine.



## Updating the Firmware

When performing the firmware update, the BCM2 keeps each outlet's power status unchanged so no server operation is interrupted. During and after the firmware update, outlets that have been powered on prior to the update remain powered ON and outlets that have been powered off remain powered OFF.

You must be the administrator or a user with the Firmware Update permission to update the firmware.

Before starting, read the release notes. If you have any questions or concerns, contact Technical Support BEFORE updating.

On a multi-inlet PDU, all inlets must be connected to power for the PDU to successfully update its firmware.

Note that firmware update via iOS mobile devices, such as iPad, requires the use of iCloud Drive or a file manager app.

Firmware update can also be completed using methods other than the web interface. See [Special Configuration and Upgrade Methods](#) (on page 417).

---

---

Warning: Do NOT perform the firmware update over a wireless network connection.

---

---

► *To update the firmware:*

1. Choose Maintenance > Update Firmware.
2. Click Browse to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload process.
4. Select Free memory before upload to clear up the memory.

5. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.
  - The expected firmware platform and product category is displayed in case the uploaded file is incorrect.
  - If anything is incorrect, click Discard Upload.
6. To proceed with the update, click Update Firmware.

---

*Warning: Do NOT power off the BCM2 during the update.*

---

7. During the firmware update:
  - A progress bar appears on the web interface, indicating the update status.
  - The front panel display shows the firmware upgrade message.
  - The outlet LEDs flash if the relay boards are being updated. If the firmware update does not include the update of the relay board firmware, outlet LEDs do NOT flash.
  - No users can log in.
  - Other users' operation, if any, is forced to suspend.
8. When the update is complete, the unit resets, and the Login page re-appears.

---

**Important: If you are using the BCM2 with an SNMP manager, download its MIB again after the firmware update to ensure your SNMP manager has the correct MIB for the latest release you are using.**

---

## Upgrade Matrix

In Xerus 4.0.x, the following upgrade paths must be followed

Firmware Version	Upgrade Steps
3.0.x, 3.1.x, 3.2.x	>> 3.4.0 >> 3.5.0 >> 4.2.10
3.3.x, 3.4.x	>> 3.5.0 >> 4.2.10
3.5.x, 3.6.x	>> 4.2.10
4.0.x	>> 4.2.10
4.1.x, 4.2.x	>> 4.2.10
4.2.x	>>4.3.x

---

Note: Due to file system changes in Xerus 4.0.x, the upgrade paths must be followed, or the Xerus-based device may become inoperable and require manual recovery.

---

## Upgrade Guidelines for Existing Cascading Chains

There are additional concerns when upgrading devices in a cascading chain. See Firmware Upgrade for Cascading Chains

## A Note about Firmware Upgrade Time

The PDU firmware upgrade time varies from unit to unit, depending on various external and internal factors.

External factors include, but are not limited to: network throughput, firmware file size, and speed at which the firmware is retrieved from the storage location. Internal factors include: the necessity of upgrading the firmware on the microcontroller and the number of microcontrollers that require upgrade (which depends on the number of outlets). The microcontroller is upgraded only when required. Therefore, the length of firmware upgrade time ranges from approximately 3 minutes (without any microcontroller updated) to almost 7 minutes (with all microcontrollers for 48 outlets updated). Take the above factors into account when estimating the PDU's firmware upgrade time.

The time indicated in this note is for BCM2 web-interface-based upgrades. Upgrades through other management systems, such as Sunbird's Power IQ, may take additional time beyond the control of the PDU itself. This note does not address the upgrades using other management systems.

## Full Disaster Recovery

If the firmware upgrade fails, causing the BCM2 to stop working, you can recover it by using a special utility rather than returning the device.

Contact Raritan Technical Support for the recovery utility. You will also need an appropriate firmware file in the recovery procedure.

## Viewing Firmware Update History

The firmware upgrade history is permanently stored. It remains available even though you perform a device reboot or any firmware update.

► *To view the firmware update history:*

1. Choose Maintenance > Firmware History.

Each firmware update event consists of:

- Update date and time
- Previous firmware version
- Update firmware version
- Update result

## Bulk Configuration

The Bulk Configuration feature lets you save generic settings of a configured BCM2 device to your computer. You can use this configuration file to copy settings to other devices of the same model and firmware version.

A source device is the BCM2 device where the configuration file is downloaded/saved. A target device is the BCM2 device that loads the configuration file.

By default the configuration file downloaded from the source device contains settings based on the built-in bulk profile. The built-in bulk profile defines that all settings should be saved except for device-specific settings, such as IP address or environmental sensor settings. If you need to load these device-specific settings, you should use the Backup/Restore feature instead.

You can decide which settings are downloaded by creating your own bulk configuration profile.

When the date and time settings are included in the bulk configuration file, exercise caution when distributing that file to target devices located in a different time zone than the source device.

This bulk configuration method can be employed through the web interface, USB, or SCP. See [Special Configuration and Upgrade Methods](#) (on page 417).

► *Bulk configuration overview:*

1. A built-in configuration profile is available, or you can customize your own bulk configuration profile.
2. Select and download the file from the source device.
3. Upload the file to perform the configuration on the target device.

## Bulk Configuration Restrictions

Before performing bulk configuration, make sure your source and target devices are compatible devices for sharing general settings.

► *Restrictions for bulk configuration:*

- The target device must be running the same firmware version as the source device.
- The target device must be of the same model type as the source device.
- Bulk configuration is permitted if the differences between the target and source devices are only "mechanical" designs which are indicated in the model name's suffix.

For example, you can perform bulk configuration between PX3-4724-E2N1K2 and PX3-4724-E2N1K9 since the only difference between the two models is their chassis colors represented by K2 (blue) and K9 (gray).

► *Mechanical design codes in model numbers:*

These mechanical designs are represented by suffixes added to the model name. In the table, x represents a number. For example, Ax can be A1, A2, A3, and so on.



Suffix	Mechanical design	Example
Ax	The line cord's length in meters <hr/> Note: For an inline monitor, it is likely two Ax's are added to the model name for indicating the lengths of its inlets' and outlets' line cords. <hr/>	A20 = 3.3 meters
Bx	The line cord's color	B501 = bright red orange
Cx	Cord types or options	C4 = power cord with the standard gauge
Dx	Plug types or options	D1 = IP67 watertight plug
Ex	Outlet types or options	E2 = <i>Locking C13</i> or <i>Locking C19</i>
Gx	Controller options	G0 = no controller
Kx	Chassis colors	K6 = yellow
Lx	The line cord's length in centimeters	
Nx	Chassis dimensions or other mechanical changes	
Ox	OCP brand options	
Px	Special requests for device painting or printing	
Qx	Special requests for physical placement arrangements	
Rx	Custom logo	
Ux	Different power plug brands	

## Customizing Bulk Configuration Profiles

A bulk profile defines which settings are downloaded/saved from the source device and which are not. The default is to apply the built-in bulk profile, which downloads all settings from the source device except for device-specific data.


If the built-in profile does not meet your needs, you can create your own profiles.

### ► To create new bulk configurations profiles:

1. Log in to the source device whose settings you want to download.
2. Choose Maintenance > Bulk Configuration.
3. Click New Profile, then enter a Profile name and Description.

4. To make this new profile the default one for future bulk configuration operations, select the 'Select as default profile' checkbox.
5. Now decide which settings to include or exclude.



- a. Click  of the setting which you want to configure.
- b. When the pop-up menu appears, select one of the options.

Note that the two options 'Inherited' and 'Built-in' are mutually exclusive.

Option	Description
Excluded	The setting will <i>not</i> be downloaded.
Included	The setting will be downloaded.
Inherited	<p>The setting will follow its parent setting (that is, the upper-level setting).</p> <ul style="list-style-type: none"> <li>• If you select 'Excluded' for its upper-level setting, this setting will be also excluded.</li> <li>• If you select 'Included' for its upper-level setting, this setting will be also included.</li> </ul> <p>The option inherited from its parent setting will be enclosed in parentheses.</p>
Built-in	<p>The setting will follow the same setting of Raritan's built-in profile.</p> <ul style="list-style-type: none"> <li>• If 'Excluded' is selected in the built-in profile, this setting will be also excluded.</li> <li>• If 'Included' is selected in the built-in profile, this setting will be also included.</li> </ul> <p>The option inherited from the built-in profile will be enclosed in parentheses.</p> <hr/> <p><i>Note: The option 'Built-in' is available in those settings whose corresponding settings in the built in profile have been set to a non-inherited option -- Excluded or Included.</i></p> <hr/>

6. Click Save.

## Performing Bulk Configuration

To perform the bulk configuration using the web interface, first select and download the bulk configuration file, then upload it to the target device to configure it.

### ► Step 1: Save a bulk configuration file

---



---

You must have the Administrator Privileges or "Unrestricted View Privileges" to download the configuration.

---



---

1. Log in to the source device.
2. Choose Maintenance > Bulk Configuration.
3. Select the profile of the configuration you want to use in the Bulk Profile field.
4. In the 'Bulk format' field select Encrypted or Cleartext, to specify the security of the file.

Option	Description
Encrypted	<ul style="list-style-type: none"> <li>• Partial content is base64 encoded.</li> <li>• Its content is encrypted using the AES-128 encryption algorithm.</li> <li>• The file is saved to the TXT format</li> </ul>
Cleartext	<ul style="list-style-type: none"> <li>• Content is displayed in clear text.</li> <li>• The file is saved to the TXT format.</li> </ul>

5. In Encrypted mode, you can password protect the file. Select the Use Password checkbox, then enter a password. A password will be required when the file is uploaded on the target device.
6. Click Download Bulk Configuration. The file is named "bulk\_config" with the source device serial number and a creation date/time stamp, such as "bulk\_config\_1BZ31B603C\_20210927". Your browser's file download method determines download location. Save the file so that it's available to be uploaded to the target device.

► *Step 2: Upload the file to configure the target*

---



---

You must have the Administrator Privileges to upload the configuration.

---



---

1. Log in to the target device, which is of the same model and runs the same firmware as the source device.
2. Choose Maintenance > Bulk Configuration.
3. In the Restore Bulk Configuration section, click Browse to select the configuration file.
4. Click 'Upload & Restore Bulk Configuration'.
5. Confirm the operation and enter the administrator password, then click Restore.
6. Wait until the login page reappears.

## Modifying or Deleting Bulk Configuration Profiles

You can modify or delete any bulk profile except for the built-in one.


Note that a profile that has been set as the default cannot be deleted. To remove it, you have to remove its default setting first.

Choose Maintenance > Bulk Configuration. A list of profiles displays and then do one of the following.

► *To modify an existing profile:*

1. Click on the row of the wanted profile in the list.
2. Change the settings you want.
3. Click Save.

► *To delete profiles*

1. Select one or multiple profiles, then click the Delete icon  .
2. Click Delete in the confirmation message.

## Backup and Restore of Device Settings

Unlike the bulk configuration file, the backup file contains ALL device settings, including device-specific data like device names and all network settings. To back up or restore the device settings, you should use the Backup/Restore feature. To perform bulk configuration among multiple BCM2 devices, use the Bulk Configuration feature instead.

All BCM2 information is captured in the plain-TEXT-formatted backup file except for the device logs and TLS certificate.

Backup/Restore can also be completed using other methods. See [Special Configuration and Upgrade Methods](#) (on page 417).

► *To download a backup file:*

---

---

You must have the Administrator Privileges or "Unrestricted View Privileges" to download a backup file.

---

---

1. Choose Maintenance > Backup/Restore.
2. Check the 'Backup format' field. If the chosen value does not match your need, change it.

Option	Description
Encrypted	<ul style="list-style-type: none"><li>• Partial content is base64 encoded.</li><li>• Its content is encrypted using the AES-128 encryption algorithm.</li><li>• The file is saved to the TXT format</li></ul>
Cleartext	<ul style="list-style-type: none"><li>• Content is displayed in clear text.</li><li>• The file is saved to the TXT format.</li></ul>

3. Click Download Device Settings. Save the file onto your computer.

► *To restore using a backup file:*

---

---

You must have the Administrator Privileges to restore the device settings.

---

---

1. Choose Maintenance > Backup/Restore.
2. Click Browse to select the backup file.
3. Click 'Upload & Restore Device Settings' to upload the file.
  - A message appears, prompting you to confirm the operation and enter an administrator password.
4. Enter the password, then click Restore.
5. Wait until the BCM2 resets and the Login page re-appears, indicating that the restore is complete.

## Network Diagnostics

BCM2 provides the following tools in the web interface for diagnosing potential networking issues.

- Ping: The tool is useful for checking whether a host is accessible through the network or Internet.
- Trace Route: The tool lets you find out the route over the network between two hosts or systems.
- List TCP Connections: You can use this function to display a list of TCP connections.

---

Tip: These network diagnostic tools are also available through the CLI.

---

Choose Maintenance > Network Diagnostics, and then perform any function below.

### ► *Ping:*

1. Type values in the following fields.

Field	Description
Network host	The name or IP address of the host that you want to check.
Number of requests	A number up to 20. This determines how many packets are sent for pinging the host.

2. Click Run Ping to ping the host. The Ping results are then displayed.

### ► *Trace Route:*

1. Type values in the following fields.

Field/setting	Description
Hostname	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation.
Use ICMP packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this checkbox.

2. Click Run. The Trace Route results are then displayed.

### ► *List TCP Connections:*

1. Click the List TCP Connections title bar to show the list.

## Downloading Diagnostic Information

---

**Important: Use this function only when you are directed by Technical Support.**

---

You can download the diagnostic file to a client machine. The file is compressed into a .tgz file and should be sent to Technical Support.

This feature is accessible only by users with Administrative Privileges or Unrestricted View Privileges.

► *To retrieve a diagnostic file:*

1. Choose Maintenance > Download Diagnostic > Download Diagnostic.
2. The system prompts you to save or open the file. Save the file.

## Hardware Issue Detection

This page lists any internal hardware issues BCM2 has detected, including current events and historical records.

Choose Maintenance > Hardware Failures, and the page similar to either of the following diagrams opens.

*Current* hardware failure events, if any, will also display on the Dashboard.

► *NO hardware failures detected:*



► *Hardware failure(s) detected:*

Hardware Failures			
Current Hardware Failures			
Failure Message	Last Asserted ▲	Last Deasserted	Number of Occurrences
I2C bus 0 is stuck.	1/1/2018, 1:18:24 AM UTC+0100	1/1/2018, 1:00:00 AM UTC+0100	17
Past Hardware Failures			
Failure Message	Last Asserted ▲	Last Deasserted	Number of Occurrences
Network device ETH2 was not detected.	8/3/2018, 3:56:46 PM UTC+0200	8/3/2018, 3:13:10 PM UTC+0200	7

► *Hardware failure types:*

Hardware issues	Description
<b>Network device not detected</b>	A specific networking interface is NOT detected.
<b>I2C Bus stuck</b>	A specific I2C bus is stuck, which affects the communication with sensors.
<b>Sub controller not reachable</b>	Communication with a specific sub unit controller fails.
<b>Sub controller malfunction</b>	A specific sub unit controller does not work properly.
<b>Outlet power state inconsistent</b>	The physical power state of a specific outlet is different from the chosen power state set by the software.
<b>Sub controller incompatible</b>	A specific sub unit controller is incompatible with the firmware.

## Rebooting

You can remotely reboot the BCM2 via the web interface.

Resetting/rebooting does not interrupt the operation of connected servers because there is no loss of power to outlets. During and after the reboot, outlets that have been powered on prior to the reboot remain powered on, and outlets that have been powered off remain powered off.

---



---

Warning: Rebooting deletes all webcam snapshots that are saved locally. If needed, download important snapshots before rebooting the device.

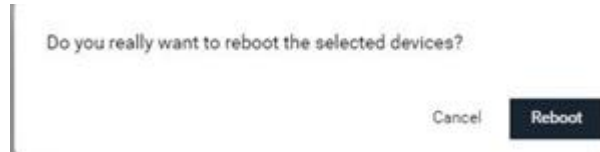
---



---

► *To reboot the device:*

1. Choose Maintenance > Unit Reset > Reboot Unit.



2. Click Reboot.
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 restart is complete, the login page opens.

---

Tip: If you are not redirected to the login page after the restart is complete, click the text "this link" in the countdown message.

---

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

---

## Resetting All Settings to Factory Defaults

You must have the Administrator Privileges to reset all settings to factory defaults.

Resetting to factory default can also be completed in the CLI or with a Reset button on the unit. See [Resetting to Factory Defaults](#)

---

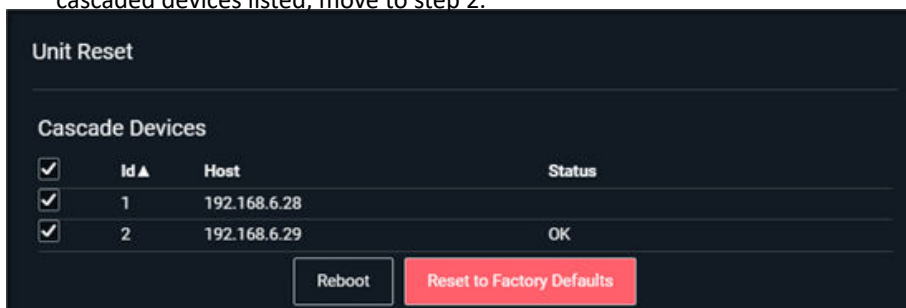
**Important: Exercise caution before resetting to factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only active energy data and firmware upgrade history are retained.**

---

If your PDU is in a Linking configuration, you can reset expansion units through the primary unit.

► *To reset the device to factory defaults:*

1. Choose Maintenance > Unit Reset
  - If your PDU is in a cascaded configuration, select the units you want to reset. If you do not have cascaded devices listed, move to step 2.



2. Click Reset to Factory Defaults.



## Reset to Factory Defaults

Do you really want to reset the selected devices to factory defaults?

Saying yes will clear all settings, including the network setup.

Please confirm with your password:

**Password:**

Enter password

Cancel

Factory Reset

3. Type your password and then click Factory Reset.
4. A message appears, with a countdown timer showing the remaining time of the operation. It takes about two minutes to complete.
5. When the reset is complete, the login page opens.

---

Tip: If you are not redirected to the login page after the reset is complete, click the text "this link" in the countdown message.

---

---

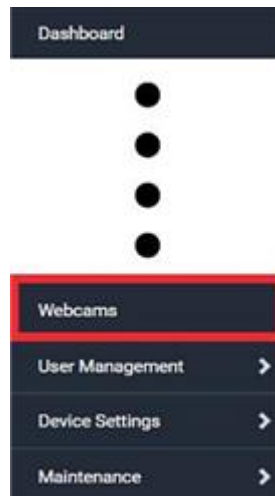
Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

---

## Webcam Management

With a Logitech® webcam connected, you can visually monitor the environment around the BCM2 via snapshots or videos captured by the webcam.

The 'Webcams' menu item appears when there is any webcam connected to the BCM2, or when there are snapshots saved onto already.



► *Permissions required:*

To do...	Permission(s) required
View snapshots and videos	Either permission below: <ul style="list-style-type: none"> <li>• Change Webcam Configuration</li> <li>• View Webcam Snapshots and Configuration</li> </ul>
Configure webcam settings	Change Webcam Configuration

## Configuring Webcams and Viewing Live Images

To configure a webcam or view live snapshot/video sessions, choose *Webcams* in the *Menu*. Then click the desired webcam to open that webcam's page.

Note that default webcam names are determined by the detection order. The one that is detected first is named *Webcam*, and a second webcam detected later is named *Webcam 2*.

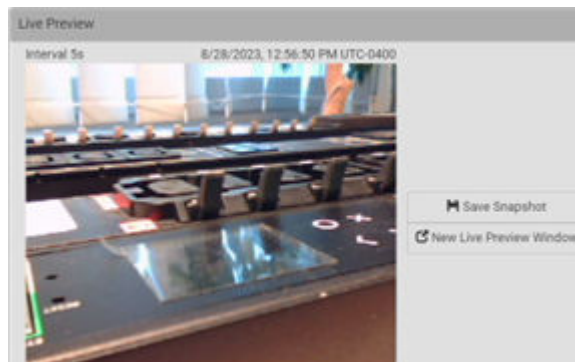


Name ▲	Location	Resolution	Mode
Webcam		352x288	Snapshot

The Webcam page consists of three sections -- *Live Preview*, *Image Controls* and *Settings*.

► *Live Preview:*

1. By default the Live Preview section is opened, displaying the live snapshot/video session captured by the webcam.
  - The default is to show live snapshots. Interval time and capture date/time of the image are displayed on the top of the image. In video mode, the number of frames per second (fps) and the video capture date/time are displayed.



---

*Tip: The date and time shown on the BCM2 web interface are automatically converted to your computer's time zone.*

---

2. To save the current image onto BCM2 or a remote server, click Save Snapshot.
  - The default storage location for snapshots is the BCM2 device. To save them onto a remote server, you can change the storage settings.
  - To download an image onto your computer, you can right-click it and save.
3. To have the same live session displayed in a separate window, click New Live Preview Window.
  - A separate window appears, which is called the Primary Standalone Live Preview window in this User Guide.
  - You can send out this window's URL to share the live image with others.
  - Note that your browser may block the pop-up window

► **Image Controls:**



1. Adjust the brightness, contrast, saturation and gain by modifying their values or adjusting the corresponding slide bar.
  - To customize the gain value, you must deselect the Auto Gain checkbox first.
  - To restore all settings to this webcam's factory defaults, click Set to Webcam Defaults.

► **Settings:**

1. Click Edit Settings.
2. Enter a name for the webcam. Up to 64 ASCII printable characters are supported.
  - If configured to store snapshots on a *remote* server, the webcam's name determines the name of the folder where snapshots are stored.
  - It is suggested to customize a webcam's name before saving snapshots on the remote server. In case you change the webcam's name after saving any snapshots, BCM2 will create a new folder with the new webcam name while keeping the old folder with the old name.
3. Type the location information in each location field as needed. Up to 63 ASCII printable characters are supported.
  - Note that the location data you enter is not available in those snapshots stored on remote servers.

---

*Tip: If the webcam's location is important, you can customize the webcam's name based on its location.*

---

4. 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.
5. Select the webcam mode.

Mode	Description
------	-------------

<b>Video</b>	The webcam enters the video mode. <ul style="list-style-type: none"> <li>• Set the 'Framerate' (frames per second) as needed.</li> </ul>
<b>Snapshot</b>	The webcam shows static images captured by the webcam at a regular interval. <ul style="list-style-type: none"> <li>• To determine the interval, set the 'Time Between Snapshots' (seconds).</li> </ul>

6. Click Save. The changes made to the settings are applied to the live session in the above *Live Preview* section immediately.

## Sending Links to Snapshots or Videos

When opening a Primary Standalone Live Preview window, a unique URL is generated for this window session. You can email or instant message this URL to as many people as possible as long as your system resources permit. Recipients can then click on the provided link and view live snapshots or videos simultaneously in the Secondary Standalone Live Preview window(s).

---

**Tip:** All Live Preview window sessions sharing the same URL, including one Primary Standalone Live Preview window and multiple Secondary Standalone Live Preview windows, are identified as one single "<webcam>" user in the Connected Users list. You can disconnect a "<webcam>" user to terminate all sessions sharing the same URL.

---

► **Best practice:**

1. The sender opens the Primary Standalone Live Preview window, and sends the link to one or multiple recipients.
2. The sender must wait until at least one recipient opens the Secondary Standalone Live Preview window.
3. The recipient(s) should inform the sender that the link has been opened.
4. Now the sender can close the Primary Standalone Live Preview window.

► **To send a snapshot or video link via email or instant message:**

1. Choose Webcams in the *Menu*.
2. Click the desired webcam to open the Webcam page.
3. Click New Live Preview Window in the Live Preview section. The live snapshot or video in a standalone window opens.
4. Copy the URL from that live preview window.
  - a. Select the URL shown on the top of the image.



- b. Right click to copy the URL, or press CTRL+ C.
5. Send the URL link through an email or instant message application to one or multiple persons.
6. Leave the live preview window open until the recipient(s) opens the snapshot or video via the link.

## How Long a Link Remains Accessible

For documentation purposes, the one who opens and sends the URL of the Primary Standalone Live Preview window is called *User A* and the two recipients of the same URL link are called *User B* and *C*.

User C is able to access the snapshot or video image via the link when the URL link remains valid, which can be one of these scenarios:

- The Primary Standalone Live Preview window remains open on User A's computer. If so, even though User A logs out of the BCM2 or the login session times out, the link remains accessible.
- User B's Secondary Standalone Live Preview window remains open. If so, even though User A already closes the Primary Standalone Live Preview window, the link remains accessible.
- Neither User A's Primary Standalone Live Preview window nor User B's Secondary Standalone Live Preview window remains open, but it has not exceeded two minutes yet after the final live preview window session was closed.

---

Note: The link is no longer valid after two minutes since the final live preview window is closed.

---

## Viewing, Downloading, Deleting Locally-Saved Snapshots

This section describes the operation for snapshots saved onto the BCM2 device only.

When saving a snapshot, it is stored locally on the BCM2 device by default. Up to 10 snapshots can be stored locally. The oldest snapshot is automatically overridden by the newest one when the total of snapshots exceeds 10, if no snapshots are deleted manually.

When there is more than one webcam connected, then the oldest snapshot of the webcam with the most snapshots is overwritten.

Snapshots are saved as JPG files, and named with sequential numbers, such as *1.jpg, 2.jpg, 3.jpg*.

---

**Warning: Rebooting the BCM2 deletes all webcam snapshots that are saved locally. If needed, download important snapshots before rebooting the device.**

---

► *To view, refresh, download or delete saved snapshots:*

1. Choose Webcams > Browse Snapshots. The Snapshots page opens.
  - To view a snapshot, click the link in the list. The image, capture time and resolution is displayed on the same page.
  - To refresh the list, click the Refresh icon.
  - To download an image file, click the Download icon.
  - To delete an image, select the checkbox of the image and click the Delete icon.



## Changing Storage Settings

---

Important: The BCM2 web interface only lists the snapshots stored locally on the BCM2 device, but does NOT list those saved onto remote servers. You must launch appropriate third-party applications, such as an FTP client, to access and manage the snapshots stored on remote servers.

---

The default is to store snapshots locally on the device, which has a limitation of 10 snapshots. Note that any operation involving device reboot, such as firmware upgrade, will remove the locally saved snapshots.

If you need to keep more than 10 images or need to keep them permanently, configure the settings to move images onto a remote FTP server.

► *To configure the storage settings:*

1. Choose Webcams > Edit Settings.



2. Click the Storage Type field to select the desired storage location and configure as needed.

---

*Note: When entering user credentials for remote servers, make sure the user credentials you enter have the write permission, or NO snapshots can be successfully saved onto remote servers.*

---

Storage location	Description
Local	'Local' means the BCM2. This is the default. <ul style="list-style-type: none"><li>• It can store a maximum of 10 snapshots only.</li><li>• The web interface can list and display all snapshots stored on the BCM2.</li><li>• All snapshots are CLEARED when the BCM2 is rebooted.</li></ul>
FTP	Snapshots are saved onto a FTP server. <ul style="list-style-type: none"><li>• Total number of saved snapshots depends on the server's capacity.</li><li>• Saved snapshots are not affected by reboots of the BCM2.</li><li>• Configure the following fields:<ul style="list-style-type: none"><li>* <i>Server URL</i> - the FTP server's path</li><li>* <i>Username</i> - for server access</li><li>* <i>Password</i> - for server access</li></ul></li></ul>

1. Click Save.

---

**Warning: Before disconnecting or powering off any remote server where the webcam snapshots are being stored, you must first change the storage settings, or the connectivity issue of the remote server may degrade the performance of the BCM2 web interface. If this issue occurs, first restore the connectivity of the remote server and then change the storage settings of the webcam snapshots.**

---

► *Tip for notifications showing the snapshots path on FTP:*

If you are using SNMP to retrieve data, you can make BCM2 automatically send a notification containing the full path or URL to the snapshots saved onto FTP with this SNMP code:  
`webcamStorageUploadStarted.`

## Identifying Snapshots Folders on Remote Servers

If saving snapshots onto a remote server, you can access those snapshots via an appropriate third-party application, such as an FTP client.

All snapshots are saved as JPEG and named according to the date and time when saving the snapshots. Note that the date and time of the filename are based on the time zone of the BCM2 rather than that of the computer or mobile device you are operating.

---

Tip: To check the time zone, choose Device Settings > Date/Time.

---

The structure of a snapshots folder looks similar to the diagram below.



Number	Folder name description
①	User-defined parent directory, whose name depends your server settings, such as your FTP configuration.
②	Serial number of your BCM2 device where the webcam is connected. For example, <i>PH85350018</i> . <ul style="list-style-type: none"> <li>View your serial number in Device Information.</li> </ul>
③	The name of the webcam that your BCM2 detects first. This is the folder where the snapshots captured by the first webcam are stored. <ul style="list-style-type: none"> <li>The first webcam's default name is "Webcam".</li> <li>You can customize the webcam's name, which will change the snapshots folder's name.</li> <li>If the webcam's location is important, you can customize the webcam's name based on its location when configuring BCM2 to save snapshots onto a remote server.</li> </ul>
④	The name of the webcam that your BCM2 detects later, if an additional webcam is connected. This is the folder where the snapshots captured by the second webcam are stored. <ul style="list-style-type: none"> <li>The second webcam's default name is "Webcam 2".</li> <li>Changing this webcam's name also changes the second snapshots folder's name.</li> <li>If the webcam's location is important, you can customize the webcam's name based on its location when configuring BCM2 to save snapshots onto a remote server.</li> </ul>

---

Note: It is suggested to customize a webcam's name "prior to" saving snapshots on the remote server. In case you change the webcam's name after saving any snapshots, BCM2 will create a new folder with the new webcam name while keeping the old folder with the old name.

---

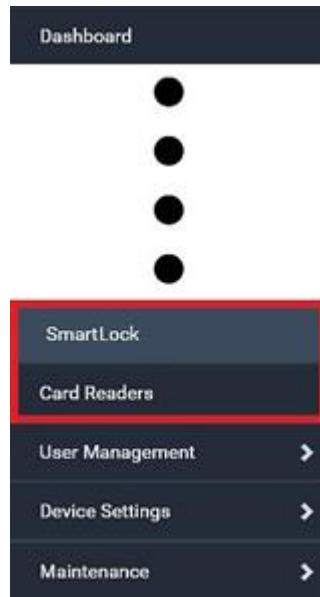
## SmartLock and Card Reader

Raritan's SmartLock kits provide several cabinet access control solutions.

If you have purchased a SmartLock kit with the door handle controller "DX2-DH2C2", both menu items "SmartLock" and "Card Readers" will appear in the menu after connecting and configuring properly DX2-DH2C2 and the door handles included in the kit.



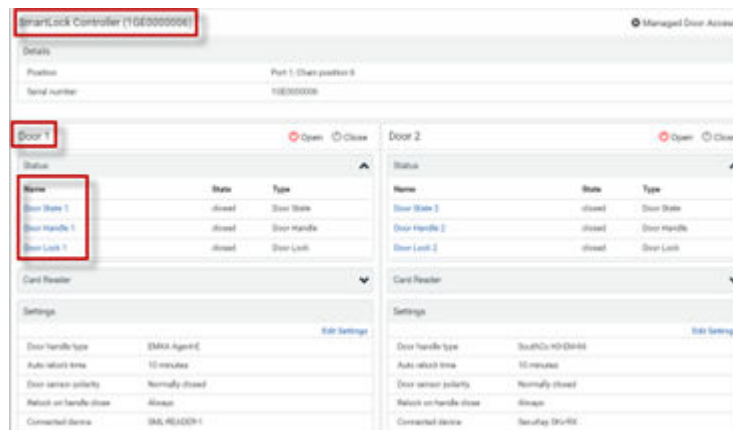
Note that "SmartLock" appears only when your door handles are connected via DX2-DH2C2, but "Card Readers" appears as long as any card reader is detected, whether standalone USB card reader or a card reader integrated with the door handles.



## SmartLock

To open the SmartLock page, choose SmartLock in the *Menu*.

The page shows information of all DX2-DH2C2 modules connected, including its serial number, position and its door configuration. When primary units and/or link units have SmartLock controllers connected, this page includes all door information for both.



On this page you can:

- View the status of the cabinet door and card reader.

---

*Note: Data of "external" USB card readers is shown on the Card Readers page.*

---

- Configure the doors connected to DX2-DH2C2. You must set this because the types of connected door handles are not automatically detected.
- Control the doors connected to DX2-DH2C2.
- Manage the door access.

► *To configure the doors:*

There are two door sections per DX2-DH2C2 because a DX2-DH2C2 has two door handle ports.

The screenshot displays two side-by-side configuration panels for 'Door 1' and 'Door 2'. Each panel includes a status table, a 'Card Reader' dropdown menu, and a 'Settings' section. In the 'Settings' section of both doors, a red arrow points to the 'Edit Settings' link.

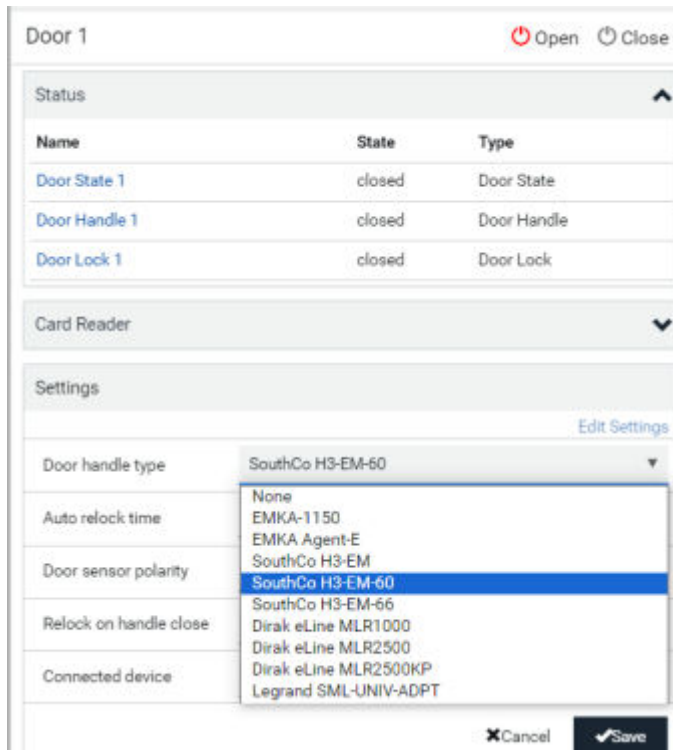
Name	State	Type
Door Contact Front	closed	Door State
Door Lock 1	closed	Door Handle
Door Handle Lock 1	closed	Door Lock

Name	State	Type
Door 2	closed	Door State
Door Lock 2	closed	Door Handle
Door Handle Lock 2	closed	Door Lock

Door handle type	SouthCo H3-EM
Auto relock time	30 s
Door sensor polarity	Normally closed
Relock on handle close	Only if door closed
Connected device	None

Door handle type	EMKA Agent-E
Auto relock time	10 minutes
Door sensor polarity	Normally closed
Relock on handle close	Always
Connected device	None

1. Click Edit Settings in the Settings section.
2. In the 'Door handle type' field, select the door handle type you are using.
  - If your specific Southco H3-EM model is listed, select it. For all other supported Southco H3-EM models, select "Southco H3-EM".



3. Make changes to the remaining fields as needed, then click Save.

Section	Description
<b>Auto Relock Time</b>	<ul style="list-style-type: none"> <li>Specify how long the lock can remain open after someone opens the door handle lock via smart card or remote control without the handle being opened during that period. When the timeout expires, the lock will be automatically closed. Default is 600 seconds (that is, 10 minutes).</li> </ul>
<b>Door sensor polarity</b>	<ul style="list-style-type: none"> <li>Choose the correct setting based on the type of contact closure sensors used to monitor the door:</li> <li>Normally closed: The contact is closed (conducting) when the door is closed and open (not conducting) when the door is open. Default.</li> <li>Normally open: The contact is not conducting when the door is closed and is conducting when the door is open.</li> <li>Note: For both normally closed and normally open sensors, the reported state is "open" when the door is open and "closed" when the door is closed.</li> </ul>
<b>Relock on Handle Close</b>	<ul style="list-style-type: none"> <li>This setting controls auto-locking. Select "Only if door closed" to delay auto-locking until "Door State" and "Door Handle State" are both verified as "Closed". Select "Always" to relock automatically.</li> </ul>
<b>Connected Device</b>	<ul style="list-style-type: none"> <li>If your door handle has a connected device, such as a keypad, select it from the list.</li> </ul>

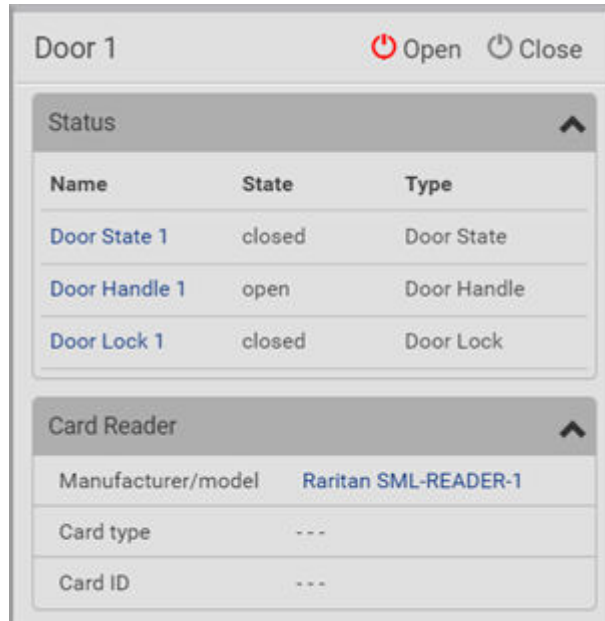
► To manage the door access:

"Managed Door Access" link provides access to "Door Access Rules" where you can create new rules.  
[Door Access](#) (on page 173)



## Door Status and Control

After configuring the door handle type properly, you can see the Status and Card Reader sections.



The screenshot shows the 'Door 1' control interface. At the top, there are 'Open' and 'Close' buttons. Below this is a 'Status' section with a table of door components. The table has three columns: Name, State, and Type. The rows are: Door State 1 (closed, Door State), Door Handle 1 (open, Door Handle), and Door Lock 1 (closed, Door Lock). Below the status section is a 'Card Reader' section with a table of reader details. The table has two columns: Manufacturer/model and Card type/ID. The rows are: Manufacturer/model (Raritan SML-READER-1), Card type (---), and Card ID (---).

Name	State	Type
Door State 1	closed	Door State
Door Handle 1	open	Door Handle
Door Lock 1	closed	Door Lock

Manufacturer/model	Card type/ID
Raritan SML-READER-1	---
	---

► *To view the status of the door and card reader:*

Section	Description
<b>Status</b>	<p>Shows all sensor states detected by DX2-DH2C2, including:</p> <ul style="list-style-type: none"><li>• <i>Door State</i>: States of contact closure sensors connected to DX2-DH2C2. Contact closure sensors detect whether the door is physically opened or closed.</li><li>• <i>Door Handle</i>: States of door locks integrated with the door handles.</li><li>• <i>Door Lock</i>: States of the door handle locks.</li></ul> <p>Door locks and door handle locks are interrelated so their states are changed one after another. The door handle lock is opened first and then the door lock.</p> <hr/> <p>Exception: If you manually open the door lock with the key shipped with your door handle, the Door Lock state will enter the open state while the Door Handle Lock state remains closed.</p> <hr/>
<b>Card Reader</b>	<p>Shows the data of the smart card scanned by the internal or external card reader accompanying each door handle connected to DX2-DH2C2.</p>

---

Tip: All sensors of the connected door handles are also listed on the Peripherals page. The same Card Reader information is also available on the Card Reader page.

---

► *To control the door:*

---

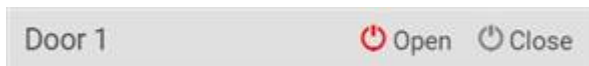
---

Per default, only one door handle can be opened at the same time so you must close one door before opening another. To increase the upper limit of concurrently opened doors, go to the Peripherals page.

---

---

1. Go to the proper door section, and click Open or Close.



2. Confirm the operation when prompted.
3. Now you can physically open or close the door.

► *Door Terms:*

The following terms and definitions are helpful when discussing doors, door handles, and locks. Note that all door sensors also display in the Peripherals page.

- SmartLock Controllers: DX2-DH2C2
- Door Handle Assembly: Door Handle and Door Lock which are connected to the SmartLock controller 8 pin connector, for example "door handle 1".
- Door: Door is the same as "Door Handle Assembly", but with optional contact closure sensor that is connected to the SmartLock controller connector. The contact closure sensor status describes whether the cabinet door is open or closed.
- Door Handle: The small grip on the front of the Door Handle Assembly, which is used to mechanically open the door by hand if it's unlocked. Sensor status describes if the Door Handle is pulled out (open) or closed.
- Door Lock: The small lock actuator inside of the Door Handle Assembly which locks or unlock the Door Handle. Sensor status describes if the Door Handle is unlocked or locked.

## Card Readers

To open the Card Readers page, choose Card Readers in the *Menu*.

This page lists all card readers connected, including:

- Standalone USB card readers
- Card readers integrated with door handles

Card Readers					
# ▲	Manufacturer/Model	Serial Number	Channel	Card Type	Card ID
1	EMKA Agent-E	1GE8200098	1	---	---
2	EMKA Agent-E	1GE8200098	2	---	---

When a user scans a smart card with the card reader, the card's type and ID are retrieved and shown in the corresponding Card Type and Card ID column. If no data is shown in the two columns, it means the scanned card may not be supported by the card reader.

---

Tip: You can use a third-party application, such as Power IQ, to retrieve the card's data to perform security features like cabinet access control. Refer to that application's user documentation for more information.

---

### ► *Door handle-integrated card readers:*

- This type of card reader is integrated in the door handle, which is any series below:
  - Emka Agent E
  - SouthCo H3-EM
  - Dirak eLine MLR 2500

---

*Note: Not every SouthCo H3-EM door handle has a card reader integrated.*

---

- It is connected via the DX2-DH2C2 module.
- The Channel column indicates which door handle port (channel) it is connected to.
- Note that the serial number displayed for this card reader is the same as DX2-DH2C2's serial number.

Each DX2-DH2C2 module can show two card readers because they have two ports for connecting two door handles with card readers integrated.

► *Standalone USB card readers:*

- It is directly connected to BCM2.
- The Channel column does not show any data.

# Using SNMP

This SNMP section helps you set up the BCM2 for use with an SNMP manager. The BCM2 can be configured to send traps or informs to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

## In This Chapter

Enabling and Configuring SNMP.....	280
SNMPv3 Notifications.....	280
SNMPv2c Notifications.....	282
Downloading SNMP MIB.....	283
SNMP Gets and Sets.....	284

### Enabling and Configuring SNMP

To communicate with an SNMP manager, you must enable SNMP protocols on the BCM2. By default, SNMP is disabled.

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, you must configure the users with the SNMP v3 access permission and set Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between SNMP and the BCM2.

---

**Important: You must download the SNMP MIB for your BCM2 to use with your SNMP manager.**

---

► *To enable SNMP v1/v2c and/or v3 protocols:*

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent section, enable SNMP v1/v2c or SNMP v3, and configure related fields, such as the community strings.
  - If SNMP v3 is enabled, you must determine which users shall have the SNMP v3 access permission.

► *To configure users for SNMP v3 access:*

1. Choose User Management > Users.
2. Create or modify users to enable their SNMP v3 access permission.
  - If authentication and privacy is enabled, configure the SNMP password(s) in the user settings.

### SNMPv3 Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the 'Enable SNMP notifications' checkbox is selected.



4. Select 'SNMPv3 trap' or 'SNMPv3 inform' as the notification type.
5. For SNMP TRAPs, the engine ID is prepopulated.
6. Type values in the following fields.

Field	Description
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent.
Port	The port number used to access the device(s).
User ID	User name for accessing the device. <ul style="list-style-type: none"> <li>• Make sure the user has the SNMP v3 access permission.</li> </ul>
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. <ul style="list-style-type: none"> <li>• For example, resend a new inform communication once every 3 seconds.</li> </ul>
Number of retries	Specify the number of times you want to resend the inform communication if it fails. <ul style="list-style-type: none"> <li>• For example, inform communications are resent up to 5 times when the initial communication fails.</li> </ul>

Field	Description
Security level	<p>Three types are available.</p> <ul style="list-style-type: none"> <li>• noAuthNoPriv - neither authentication nor privacy protocols are needed.</li> <li>• authNoPriv - only authentication is required.</li> <li>• authPriv - both authentication and privacy protocols are required.</li> </ul>
Authentication protocol, Authentication passphrase, Confirm authentication passphrase	<p>The three fields are available when the security level is set to AuthNoPriv or authPriv.</p> <ul style="list-style-type: none"> <li>• Select the authentication protocol - MD5 or SHA</li> <li>• Enter the authentication passphrase</li> </ul>
Privacy protocol, Privacy passphrase, Confirm privacy passphrase	<p>The three fields are available when the security level is set to authPriv.</p> <ul style="list-style-type: none"> <li>• Select the Privacy Protocol - DES or AES</li> <li>• Enter the privacy passphrase and then confirm the privacy passphrase</li> </ul>

7. Click Save.

## SNMPv2c Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the 'Enable SNMP notifications' checkbox is selected.

#	Host	Port	Community
1		162	
2		162	
3		162	

4. Select 'SNMPv2c trap' or 'SNMPv2c inform' as the notification type.
5. Type values in the following fields.

Field	Description
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. <ul style="list-style-type: none"> <li>For example, resend a new inform communication once every 3 seconds.</li> </ul>
Number of retries	The number of times you want to resend the inform communication if it fails. <ul style="list-style-type: none"> <li>For example, inform communications are resent up to 5 times when the initial communication fails.</li> </ul>
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent. You can specify up to 3 SNMP destinations.
Port	The port number used to access the device(s).
Community	The SNMP community string to access the device(s). The community is the group representing the BCM2 and all SNMP management stations.

6. Click Save.

## Downloading SNMP MIB

You must download an appropriate SNMP MIB file for successful SNMP communications. Always use the latest SNMP MIB downloaded from the current firmware of your BCM2.

You can download the MIBs from two different pages of the web interface.

### ► *MIB download via the SNMP page:*

1. Choose Device Settings > Network Services > SNMP.
2. Click the Download MIBs title bar.



3. Select the desired MIB file to download.
  - PDU2-MIB: The SNMP MIB file for BCM2 management.
  - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
4. Click Save to save the file onto your computer.

► *MIB download via the Device Information page:*

1. Choose Maintenance > Device Information.
2. In the Information section, click the desired download link:
  - PDU2-MIB
  - ASSETMANAGEMENT-MIB
3. Click Save to save the file onto your computer.

## SNMP Gets and Sets

In addition to sending notifications, the BCM2 is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the BCM2, such as the system location, and the current on a specific outlet.
- Set requests are used to configure a subset of the information, such as the SNMP system name.

---

*Note: The SNMP system name is the BCM2 device name. When you change the SNMP system name, the device name shown in the web interface is also changed.*

---

The BCM2 does NOT support configuring IPv6-related parameters using the SNMP set requests.

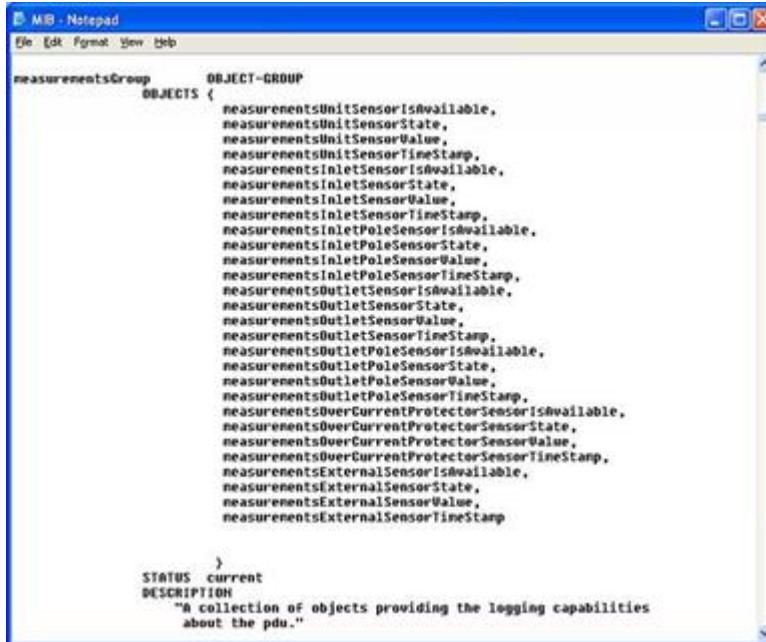
Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom BCM2 MIB.

## The MIB File

An SNMP MIB file describes the SNMP functions.

Opening the MIB reveals the custom objects that describe the BCM2 system at the unit level as well as at the individual-outlet 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.



```

MIB - Notepad
File Edit Format View Help

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 BCM2 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 PDU current rating.

## 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 cause the BCM2 to generate a warning and send an SNMP notification when certain parameters are exceeded. See Sensor Threshold Settings 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.

---

## Configuring NTP Server Settings

Using SNMP, you can change the following NTP server-related settings in the unitConfigurationTable:

- Enable or disable synchronization of the device's date and time with NTP servers (synchronizeWithNTPServer)
- Enable or disable the use of DHCP-assigned NTP servers if synchronization with NTP servers is enabled (useDHCPProvidedNTPServer)
- Manually assign the primary NTP server if the use of DHCP-assigned NTP servers is disabled (firstNTPServerAddressType and firstNTPServerAddress)
- Manually assign the secondary NTP server (optional) (secondNTPServerAddressType and secondNTPServerAddress)

---

Tip: To specify the time zone, use the CLI or web interface instead.

---

When using the SNMP SET command to specify or change NTP servers, it is required that both the NTP server's address type and address be set in the command line simultaneously.

For example, the SNMP command to change the primary NTP server's address from IPv4 (192.168.84.84) to host name looks similar to the following:

```
snmpset -v2c -c private 192.168.84.84 firstNTPServerAddressType = dns
firstNTPServerAddress = "angu.pep.com"
```

## Retrieving Energy Usage

You can discover how much energy an IT device consumes by retrieving the Active Energy for the outlet this IT device is plugged into. The Active Energy values are included in the `outletSensorMeasurementsTable`, along with other outlet sensor readings.

# Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer the BCM2.

Note that available CLI commands are model dependent.

CLI commands are case sensitive.

The CLI can be used to:

- Reset
- Display the device and network information, such as the device name, firmware version, IP address, and so on
- Configure the device 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. To enable Telnet, go to Device Settings > Network Services > Telnet.

---

## In This Chapter

Logging in to CLI. . . . .	287
Tips for Using the CLI. . . . .	290
Showing Information. . . . .	294
Clearing Information. . . . .	311
Configuring the Device and Network. . . . .	312
Network Troubleshooting in Diagnostic Mode. . . . .	410

### 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 product 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 "Device Serial Console" under the Ports group.*

---

3. In the communications program, press Enter to send a carriage return to the BCM2. The Username prompt appears.
4. Type a name and press Enter. The name is case sensitive. Then you are prompted to enter a password.
5. Type a password and press Enter. The password is case sensitive.

After properly entering the password, the BCM2 name appears at the prompt.

---

*Tip: The 'Last login' information, including the date and time, is also displayed if the same user account 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 using commands.

## With SSH or Telnet

You can remotely log in to the command line interface (CLI) using an SSH or Telnet client, such as PuTTY.

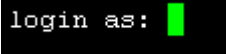
---

Note: PuTTY is a free program you can download from the Internet. Refer to PuTTY's documentation for details on configuration.

---

► *To log in using SSH or Telnet:*

1. Ensure SSH or Telnet has been enabled.
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 BCM2 name appears at the prompt.

---

*Tip: The 'Last login' information, including the date and time, is also displayed if the same user account 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 this product.

## With an Analog Modem

The BCM2 supports remote access to the CLI via a connected analog modem. This feature is especially useful when the LAN access is not available.

### ► To connect to the BCM2 via the modem:

1. Make sure the BCM2 has an analog modem connected. See [Connecting an Analog Modem](#).
2. Make sure the computer you are using has an appropriate modem connected.
3. Launch a terminal emulation program, and configure its baud rate settings according to the baud rate set for the analog modem connected to the BCM2. See [Configuring the Serial Port](#).
4. Type the following AT command to make a connection with the BCM2.

```
ATD<modem phone number>
```

5. The CLI login prompt appears after the connection is established successfully. Then type the user name and password to log in to the CLI.

### ► To disconnect from the BCM2:

1. Return to the modem's command mode using the escape code +++.
2. After the OK prompt appears, type the following AT command to disconnect from the BCM2.

```
ATH
```

## Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies. The device name appears with the prompt.

- **User Mode:** When you log in as a normal user, who may not have full permissions to configure the BCM2, the > prompt appears.
- **Administrator Mode:** When you log in as an administrator, who has full permissions to configure the BCM2, the # prompt appears.
- **Configuration Mode:** You can enter the configuration mode from the administrator or user mode. In this mode, the prompt changes to config:# or config:> and you can change BCM2 device and network configurations. See [Configuring the Device and Network](#) (on page 312).
- **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 [Network Troubleshooting in Diagnostic Mode](#) (on page 410).

## Closing a Local Connection

Close the window or terminal emulation program when you finish accessing the BCM2 over the local connection.

---



---

When accessing or upgrading multiple BCM2 devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

---



---

## 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.

### Tips for Using the CLI

## The ? Command for Showing Available Commands

When you are not familiar with CLI commands, you can press the ? key at anytime for one of the following purposes.

- Show a list of main CLI commands available in the current mode.
- Show a list of available commands or parameters for the command you type.

► *In the administrator mode:*

#

?

- ▶ *In the configuration mode:*

```
config:#                ?
```

- ▶ *In the diagnostic mode:*

```
diag:#                  ?
```

Press Enter after pressing the ? command, and a list of main commands for the current mode is displayed.

## 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 (?) or list command (ls) 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 role configuration parameters:*

```
config:#                role ?
```

- ▶ *To query available parameters for the "role create" command:*

```
config:#                role create ?
```

## 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 several times 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.
3. If there are more than one possible commands, a list of these commands is displayed. Then type the full command.

► *Examples:*

- Example 1 (only one possible command):
  - a. Type the first word and the first letter of the second word of the "reset factorydefaults" command -- that is, `reset f`.
  - b. Then press Tab or Ctrl+i to complete the second word.
- Example 2 (only one possible command):
  - a. Type the first word and initial letters of the second word of the "security strongPasswords" command -- that is, `security str`.
  - b. Then press Tab or Ctrl+i to complete the second word.
- Example 3 (more than one possible commands):
  - a. Type only the first two words of the "network ipv4 gateway xxx.xxx.xxx.xxx" command -- that is, `network ipv4`.
  - b. Then press Tab or Ctrl+i one or two times, a list of possible commands displays as shown below.

```
gateway          interface          staticRoutes
```
  - c. Type the full command "network ipv4 gateway xxx.xxx.xxx.xxx", according to the onscreen command list.

## Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command to perform all of them at a time. All combined commands must belong to the same configuration type, such as commands prefixed with *network*, *user modify*, *sensor externalsensor* and so on.

A multi-command syntax looks like this:

```
<configuration type> <setting 1> <value 1> <setting 2> <value 2>  
<setting 3> <value 3> ...
```

► *Example 1 - Combination of ETH1's Activation, Configuration Method and IP*

The following multi-command syntax configures IPv4 address, configuration method and activation status for ETH1's network connectivity simultaneously.

```
config:# network ipv4 interface eth1 enabled true configMethod static
        address 192.168.84.225/24
```

*Results:*

- The ETH1 interface is enabled.
- ETH1's configuration method is set to static IP address.
- ETH1's IPv4 address is set to 192.168.84.225/24.

► *Example 2 - Combination of Upper Critical and Upper Warning Settings*

The following multi-command syntax simultaneously configures Upper Critical and Upper Warning thresholds for the RMS current of the 2nd overcurrent protector.

```
config:# sensor ocp 2 current upperCritical disable upperWarning 15
```

*Results:*

- The Upper Critical threshold of the 2nd overcurrent protector's RMS current is disabled.
- The Upper Warning threshold of the 2nd overcurrent protector's RMS current is set to 15A and enabled at the same time.

► *Example 3 - 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.

► *Example 4 - Combination of Upper Critical, Upper Warning and Lower Warning Settings*

The following multi-command syntax configures Upper Critical, Upper Warning and Lower Warning thresholds for the outlet 5 RMS current simultaneously.

```
config:# sensor outlet 5 current upperCritical disable upperWarning enable
        lowerWarning 1.0
```

#### Results:

- The Upper Critical threshold of outlet 5 RMS current is disabled.
- The Upper Warning threshold of outlet 5 RMS current is enabled.
- The Lower Warning threshold of outlet 5 RMS current is set to 1.0A and enabled at the same time.

## Showing Information

You can use the show commands to view current settings or the status of the BCM2 device or part of it, such as the IP address, networking mode, firmware version, states or readings of internal or external sensors, user profiles, and so on.

Some "show" commands have two formats: one with the parameter "details" and the other without. The difference is that the command without the parameter "details" displays a shortened version of information while the other displays in-depth information.

After typing a "show" command, press Enter to execute it.

---

Note: Depending on your login name, the # prompt may be replaced by the > prompt.

---

## 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. <hr/> <b>Tip:</b> You can also type the command without adding this option "all" to get the same data. <hr/>
A specific actuator number*	Displays the information for the specified actuator only.

\* The actuator number is the ID number assigned to the actuator. The ID number can be found using the BCM2 web interface or CLI. It is an integer starting at 1.

*Displayed information:*

- Without the parameter "details," only the actuator ID, type and state are displayed.
- With the parameter "details," more information is displayed in addition to the ID number and actuator state, such as the serial number and X, Y, and Z coordinates.

## Asset Strip Settings

This command shows the asset strip settings, such as the total number of rack units (tag ports), asset strip 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 strip information. <hr/> <b>Tip:</b> You can also type the command without adding this option "all" to get the same data. <hr/>
A specific asset strip number	Displays the settings of the asset strip connected to the specified FEATURE port number. For the BCM2 device with only one FEATURE port, the valid number is always 1.

## Authentication Settings

### ► *General authentication settings:*

This command displays the authentication settings of the BCM2, including LDAP, Radius, and TACACS+ settings.

```
# show authentication
```

### ► *One LDAP server's settings:*

To show the configuration of a specific LDAP server, assign the desired LDAP server with its sequential number in the command. To get detailed information, add "details" to the end of the command.

```
# show authentication ldapServer <server_num>
```

-- OR --

```
# show authentication ldapServer <server_num> details
```

► *One Radius server's settings:*

To show the configuration of a specific Radius server, assign the desired Radius server with its sequential number in the command. To get detailed information, add "details" to the end of the command.

```
# show authentication radiusServer <server_num>
```

-- OR--

```
# show authentication radiusServer <server_num> details
```

► *One TACACS+ server's settings:*

To show the configuration of a specific TACACS+ server, assign the desired TACACS+ server with its sequential number in the command. To get detailed information, add "details" to the end of the command.

```
# show authentication tacplusServer <server_num>
```

-- OR--

```
# show authentication tacplusServer <server_num> details
```



*Variables:*

- <server\_num> is the sequential number of the specified authentication server on the LDAP or Radius or TACACS+ server list.

*Displayed information:*

- Without specifying any server, BCM2 shows the authentication type and a list of LDAP, Radius, and TACACS+ servers that have been configured.
- When specifying a server, only that server's configuration is displayed. For LDAP server IP address/hostname, server type, security, and port number are displayed, whereas Radius or TACACS+ servers show their IP address/host name Authentication type and Port/s.

With the parameter "details" added, detailed information of the specified server is displayed, such as an LDAP server's bind DN and the login name attribute. Whereas Radius and TACACS+ servers show accounting, timeout, retries, and shared secret values.

## Blade Slot

This command shows the blade extension information, such as number of blade extensions connected to the rack unit on the asset strip.

```
# show bladeSlot [<assetstrip>] [<rackunit>]
  [<bladeslot>]
```

- assetstrip Asset strip index (1..99) [1]
- rackunit Rack unit index (1..99) [1]
- bladeslot Blade slot index (1..99 or all) [all]

## Command History

This command 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.

## Device Configuration

This command shows the device configuration, such as the device name, firmware version, model type and upper limit of active powered dry contact actuators. The CLI is supported by various Xerus products.

```
# show pmc
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show pmc details
```

Variables:

- pmc is one of the options: pdu, src, pmc or ts.

---

Note: Your Xerus product may not support all commands.

---

## Date and Time Settings

This command shows the current date and time settings on the BCM2.

```
# show time
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show time details
```

---

Note: If details is not specified, only the deviceTime, timeZone and setupMethod will be displayed.

---

## Default Measurement Units

This command shows the default measurement units applied to the BCM2 web and CLI interfaces across all users, especially those users authenticated through remote authentication servers.

```
# show user defaultPreferences
```

---

Note: If a user has set their 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. See [Existing User Profiles](#) (on page 302) for the preferred measurement units for a specific user.

---

## 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.
sensor	Internal or external sensor events, such as state changes of any sensors.
serverMonitor	Server-monitoring records, such as a server being declared reachable or unreachable.
assetManagement	Raritan asset management events, such as asset tag connections or disconnections.
modem	Modem-related events.
timerEvent	Scheduled action events.

Event type	Description
webcam	Events for webcam management, if available.
cardReader	Events for card reader management, if available.

## Environmental Sensor Information

This command syntax shows the external sensor's information.

```
# show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show externalsensors <n> details
```

```
# show externalsensors 2 details
External sensor 2 ('Temperature 2')
Sensor type: Temperature
Reading:      24.0 deg C (normal)

Serial number:      QMSemu0004
Description:        Not configured
Location:           X Not configured
                   Y Not configured
                   Z Not configured
Position:           Port 1, Chain Position 4
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. <hr/> <b>Tip:</b> You can also type the command without adding this option "all" to get the same data. <hr/>
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 Peripherals page of the BCM2 web interface.

*Displayed information:*

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

---

*Note: A state sensor displays the sensor state instead of the 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.

## 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
	<hr/> <p>Tip: You can also type the command without adding this option "all" to get the same data.</p> <hr/>

*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.

## 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. <hr/> <b>Tip:</b> You can also type the command without adding this option "all" to get the same data. <hr/>
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.

## 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. <hr/> <b>Tip:</b> You can also type the command without adding this option "all" to get the same data. <hr/>
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.

## Front Panel Permissions

This command shows the front panel permissions applied to the BCM2.

```
# show frontPanelPermission
```

Switch Peripheral Actuator: no

Acknowledge Alarm: no

Factory Reset: no

Mute Beeper: yes

## Network Configuration

This command shows all network configuration and all network interfaces' information, such as the IP address, MAC address, the Ethernet interfaces' duplex mode, and the wireless interface's status/settings.

```
# show network
```

## Network Diagnostics

This command shows the network diagnostics (Wi-Fi/802.1x) log.

```
# show network diagLog limit <limit>
```

*Variable:*

- <limit> Number of log lines to display (1..10000 or all)

## IP Configuration

This command shows the IP settings shared by all network interfaces, such as DNS and routes. Information shown will include both IPv4 and IPv6 configuration.

```
# show network ip common
```

To show the IP settings of a specific network interface, use the following command.

```
# show network ip interface <ETH>
```

*Variables:*

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

---

*Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.*

---

Interface	Description
eth1	Show the IP-related configuration of the ETH1 interface.
eth2	Show the IP-related configuration of the ETH2 interface.
wireless	Show the IP-related configuration of the WIRELESS interface.
bridge	Show the IP-related configuration of the BRIDGE interface.
all	Show the IP-related configuration of all interfaces. <hr/> <p>Tip: You can also type the command without adding this option "all" to get the same data. That is, <i>show network ip interface</i>.</p> <hr/>

## IPv4-Only or IPv6-Only Configuration

To show IPv4-only or IPv6-only configuration, use any of the following commands.



- ▶ To show IPv4 settings shared by all network interfaces, such as DNS and routes:

```
# show network ipv4 common
```

- ▶ To show IPv6 settings shared by all network interfaces, such as DNS and routes:

```
# show network ipv6 common
```

- ▶ To show the IPv4 configuration of a specific network interface:

```
# show network ipv4 interface <ETH>
```

- ▶ To show the IPv6 configuration of a specific network interface:

```
# show network ipv6 interface <ETH>
```

*Variables:*

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

---

*Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.*

---

Interface	Description
eth1	Show the IPv4 or IPv6 configuration of the ETH1 interface.
eth2	Show the IPv4 or IPv6 configuration of the ETH2 interface.
wireless	Show the IPv4 or IPv6 configuration of the WIRELESS interface.
bridge	Show the IPv4 or IPv6 configuration of the BRIDGE interface.
all	Show the IPv4 or IPv6 configuration of all interfaces. <hr/> <p>Tip: You can also type the command without adding this option "all" to get the same data. That is, <i>show network ipv4 interface</i>.</p> <hr/>

## Network Interface Settings

This command shows the specified network interface's information which is NOT related to IP configuration. For example, the Ethernet port's LAN interface speed and duplex mode, or the wireless interface's SSID parameter and authentication protocol.

```
# show network interface <ETH>
```

### Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

---

*Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.*

---

Interface	Description
eth1	Show the ETH1 interface's non-IP settings.
eth2	Show the ETH2 interface's non-IP settings.
wireless	Show the WIRELESS interface's non-IP settings.
bridge	Show the BRIDGE interface's non-IP settings.
all	Show the non-IP settings of all interfaces.
	<hr/> <p>Tip: You can also type the command without adding this option "all" to get the same data. That is, <i>show network interface</i>.</p> <hr/>

## 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. <hr/> <b>Tip:</b> You can also type the command without adding this option "all" to get the same data. <hr/>
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.
redfish	Only displays the redfish service settings.
zeroconfig	Only displays the settings of the zero configuration advertising.

## Network Connections Diagnostic Log

This command shows the diagnostic log for both the EAP authentication and wireless LAN connection.

```
# show network diagLog
```

## Peripheral Devices Settings

This command shows peripheral devices settings, including Z coordinate format of external sensors, device altitude, peripheral device auto management, maximum number of concurrently active powered dry contacts, and muting of other door handle.

```
# show peripheralDevicesSetup
```

## 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. Peripheral Device Package refers to an environmental sensor package.

```
Peripheral Device Package 1
```

```
Serial Number: 1GE7A00022
```

```
Package Type: DX2-T1H1
```

```
Position: Port 1, Chain Position 1
```

```
Package State: operational
```

```
Firmware Version: 33.0
```

```
Peripheral Device Package 2
```

```
Serial Number: 1GE7A00021
```

```
Package Type: DX2-T3H1
```

```
Position: Port 1, Chain Position 2
```

```
Package State: operational
```

```
Firmware Version: 33.0
```

## 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. <hr/> <b>Tip:</b> You can also type the command without adding this option "0" to get all data. <hr/>
A specific integer number	Displays the specified number of last entries in the reliability error log.

## Rack Unit Settings of an Asset Strip

A rack unit refers to a tag port on the asset strips. This command shows the settings of a specific rack unit or all rack units on an asset strip, 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 strip is physically connected. For the BCM2 device with only one FEATURE port, the number is always 1.
- <rack\_unit> is one of the options: *all* or a specific rack unit's index number.

Option	Description
all	Displays the settings of all rack units on the specified asset strip. <hr/> <b>Tip:</b> You can also type the command without adding this option "all" to get the same data. <hr/>
A specific number	Displays the settings of the specified rack unit on the specified asset strip.  Use the index number to specify the rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.

## Reliability Hardware Failures

This command shows a list of detected hardware failures.

```
# show reliability hwfailures
```

For details, see Hardware Issue Detection.

## Security Settings

This command shows the security settings of the BCM2.

```
# show security
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show security details
```

### *Displayed information:*

- Without the parameter "details," the information including IP access control, role-based access control, password policy, and HTTPS encryption is displayed.
- With the parameter "details," more security information is displayed, such as user blocking time, user idle timeout and front panel permissions (if supported by your model).

## 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.

## Serial Port Settings

This command shows the baud rate setting of the serial port labeled CONSOLE / MODEM on the BCM2.

```
# show serial
```

## Clearing Information

You can use the clear commands to remove unnecessary data.

After typing a "clear" command, press Enter to execute it.

---

Note: Depending on your login name, the # prompt may be replaced by the > prompt.

---

## 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.

## Clearing Diagnostic Log for Network Connections

This command removes all data from the diagnostic log for both the EAP authentication and WLAN connection.

```
# clear networkDiagLog
```

-- OR --

```
# clear networkDiagLog /y
```

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type *y* to clear the log or *n* to abort the operation.

## Configuring the Device and Network

To configure the device or network settings through the CLI, it is highly recommended to log in as the administrator so that you have full permissions. If you enter configuration mode from user mode, you may have limited permissions to make configuration changes.

To configure any settings, enter the configuration mode. Configuration commands are case sensitive.

### ► To enter configuration mode:

1. Ensure you have entered administrator mode and the # prompt is displayed.
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.**

---

### ► To quit the configuration mode, use either "apply" or "cancel" command:

```
config:# apply
```

-- OR --

```
config:# cancel
```

The # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode.

## Device Configuration Commands

Device configuration command begins with `pmc`. You can use the `pmc` configuration commands to change the settings that apply to the whole device.



Configuration commands are case sensitive so ensure you capitalize them correctly.

## Changing the Device Name

```
config:#          pmc name "<name>"
```

Variables:

- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

## Enabling or Disabling Data Logging

This command enables or disables the data logging feature.

```
config:#          pmc 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.

## Setting Data Logging Measurements Per Entry

This command defines the number of measurements accumulated per log entry.

```
config:#          pmc measurementsPerLogEntry <number>
```

Variables:

- <number> is an integer between 1 and 600. The default is 60 samples per log entry.

## Setting Log Capacity

This command defines the size of data log (records per sensor).

```
config:#          pmc logCapacity <number>
```

Variables:

- <number> is an integer between 60 and 20,000. Desired default log capacity is 120.

## Enabling or Disabling data backup

This command enables or disables the data backup feature.

```
config:#      pmc dataBackup <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.

## 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.

### Configuring IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

### Setting the IPv4 Configuration Mode

This command determines the IP configuration mode.

```
config:#      network ipv4 interface <ETH> configMethod <mode>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

---

*Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.*

---

Interface	Description
eth1	Determine the IPv4 configuration mode of the ETH1 interface (wired networking).

Interface	Description
eth2	Determine the IPv4 configuration mode of the ETH2 interface (wired networking).
wireless	Determine the IPv4 configuration mode of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 configuration mode of the BRIDGE interface (that is, bridging mode).

- <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 interface <ETH> preferredHostName <name>
```

*Variables:*

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

---

*Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.*

---

Interface	Description
eth1	Determine the IPv4 preferred host name of the ETH1 interface (that is, wired networking).
eth2	Determine the IPv4 preferred host name of the ETH2 interface (that is, wired networking).
wireless	Determine the IPv4 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 preferred host name of the BRIDGE interface (that is, bridging mode).

- <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 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:# network ipv4 interface eth1 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.

Interface	Description
eth1	Determine the IPv4 address of the ETH1 interface (that is, wired networking).
eth2	Determine the IPv4 address of the ETH2 interface (that is, wired networking).
wireless	Determine the IPv4 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 address of the BRIDGE interface (that is, the bridging mode).

## Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the BCM2.

```
config:# network ipv4 interface <ETH> address <ip address>
```

*Variables:*

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

---

*Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.*

---

Interface	Description
eth1	Determine the IPv4 address of the ETH1 interface (that is, wired networking).
eth2	Determine the IPv4 address of the ETH2 interface (that is, wired networking).
wireless	Determine the IPv4 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 address of the BRIDGE interface (that is, the bridging mode).

- <ip address> is the IP address being assigned to your BCM2. Its format is "IP address/prefix". For example, *192.168.84.99/24*.

## Setting IPv4 Static Routes

If the IPv4 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the BCM2 and devices in the other subnet.

These commands are prefixed with *network ipv4 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route. For further information, see [Static Route Examples](#).

- ▶ *Method 1: add a static route when the other network is NOT directly reachable:*

```
config:# network ipv4 staticRoutes add <dest-1> nextHop <hop>
```

- ▶ *Method 2: add a static route when the other network is directly reachable:*

```
config:# network ipv4 staticRoutes add <dest-1> interface <ETH>
```

- ▶ *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 <dest-2> nextHop <hop>
```

-- OR --

```
config:# network ipv4 staticRoutes modify <route_ID> dest <dest-2>
        interface <ETH>
```

*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.
- <ETH> is one of the interfaces: *ETH1/ETH2*, *WIRELESS* and *BRIDGE*. Type "bridge" only when your BCM2 is in the bridging mode.
- <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*.

## Setting the IPv6 Configuration Mode

This command determines the IP configuration mode.

```
config:# network ipv6 interface <ETH> configMethod <mode>
```

*Variables:*

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

---

*Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.*

---

Interface	Description
eth1	Determine the IPv6 configuration mode of the ETH1 interface (wired networking).
eth2	Determine the IPv6 configuration mode of the ETH2 interface (wired networking).
wireless	Determine the IPv6 configuration mode of the WIRELESS interface (that is, wireless networking).

Interface	Description
bridge	Determine the IPv6 configuration mode of the BRIDGE interface (that is, bridging mode).

- <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.

---

\*You can configure the BCM2 to either "Manual" or "Automatic" IPv6 settings. In manual mode, you must specify the device's IP address, the default router, the DNS server etc. But when Automatic mode is selected, the behavior of the BCM2 depends on the configuration of the Router Advertisement (RA) in the network's router. If the RA contains a Prefix Information that has the "Autonomous address-configuration flag" set, the BCM2 will use SLAAC and use an IPv6 address based on that Prefix. The BCM2 will create a stable privacy address according to RFC 7217. If the RA has the "otherconf" flag set, the BCM2 will also use Stateless DHCP to retrieve information like a DNS server. If the "managed" flag is set in the RA, Stateful Address Auto configuration is used via DHCPv6. Both modes (SLAAC and DHCPv6) can be used at the same time.

---

## 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 interface <ETH> preferredHostName <name>
```

*Variables:*

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

---

*Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.*

---

Interface	Description
eth1	Determine the IPv6 preferred host name of the ETH1 interface (wired networking).
eth2	Determine the IPv6 preferred host name of the ETH2 interface (wired networking).
wireless	Determine the IPv6 preferred host name of the WIRELESS interface (that is, wireless networking).

Interface	Description
bridge	Determine the IPv6 preferred host name of the BRIDGE interface (that is, bridging mode).

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
- Cannot contain punctuation marks, spaces, and other symbols

## Setting the IPv6 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the BCM2.

```
config:# network ipv6 interface <ETH> address <ip
        address>
```

*Variables:*

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your BCM2 is set to the bridging mode.

---

*Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.*

---

Interface	Description
eth1	Determine the IPv6 address of the ETH1 interface (wired networking).
eth2	Determine the IPv6 address of the ETH2 interface (wired networking).
wireless	Determine the IPv6 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 address of the BRIDGE interface (that is, the bridging mode).

- <ip address> is the IP address being assigned to your BCM2. 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 interface gateway eth1 <ip
        address>
```

*Variables:*

- <ip address> is the IP address of the gateway. This value uses the IPv6 address format.

Interface	Description
eth1	Determine the IPv6 address of the ETH1 interface (that is, wired networking).
eth2	Determine the IPv6 address of the ETH2 interface (that is, wired networking).
wireless	Determine the IPv6 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 address of the BRIDGE interface (that is, the bridging mode).

## Setting IPv6 Static Routes

If the IPv6 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the BCM2 and devices in the other subnet.

These commands are prefixed with *network ipv6 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route. For further information, see [Static Route Examples](#).

- ▶ *Method 1: add a static route when the other network is NOT directly reachable:*

```
config:# network ipv6 staticRoutes add <dest-1> nextHop <hop>
```

- ▶ *Method 2: add a static route when the other network is directly reachable:*

```
config:# network ipv6 staticRoutes add <dest-1> interface <ETH>
```

- ▶ *Delete an existing static route:*

```
config:# network ipv6 staticRoutes delete <route_ID>
```

► **Modify an existing static route:**

```
config:# network ipv6 staticRoutes modify <route_ID> dest <dest-2>
        nextHop <hop>
```

-- OR --

```
config:# network ipv6 staticRoutes modify <route_ID> dest <dest-2>
        interface <ETH>
```

*Variables:*

- <dest-1> is the IP address and prefix length of the subnet where the BCM2 belongs. The format is *IP address/prefix length*.
- <hop> is the IP address of the next hop router.
- <ETH> is one of the interfaces: *ETH1/ETH2, WIRELESS* and *BRIDGE*. Type "bridge" only when your BCM2 is in the bridging mode.
- <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.

## Configuring DNS Parameters

Use the following commands to configure static DNS-related settings.

► **Specify the primary DNS server:**

```
config:# network dns firstServer <ip address>
```

► **Specify the secondary DNS server:**

```
config:# network dns secondServer <ip address>
```

► **Specify the third DNS server:**

```
config:# network dns thirdServer <ip address>
```

► **Specify one or multiple optional DNS search suffixes:**

```
config:# network dns searchSuffixes <suffix1>
```

-- OR --

```
config:# network dns searchSuffixes  
      <suffix1>,<suffix2>,<suffix3>,...,<suffix6>
```

- *Determine which IP address is used when the DNS server returns both IPv4 and IPv6 addresses:*

```
config:# network dns resolverPreference <resolver>
```

*Variables:*

- <ip address> is the IP address of the DNS server.
- <suffix1>, <suffix2>, and the like are the DNS suffixes that automatically apply when searching for any device via BCM2. For example, <suffix1> can be *raritan.com*, and <suffix2> can be *legrand.com*. You can specify up to 6 suffixes by separating them with commas.
- <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 LAN Interface Parameters

A LAN interface configuration command begins with *network ethernet*.

## Enabling or Disabling the LAN Interface

This command enables or disables the LAN interface.

```
config:# network ethernet <ETH> enabled <option>
```

*Variables:*

- <ETH> is one of the options -- *eth1* or *eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

- <option> is one of the options: *true* or *false*.

Option	Description
true	The specified network interface is enabled.
false	The specified network interface is disabled.

## Changing the LAN Interface Speed

This command determines the LAN interface speed.

```
config:# network ethernet <ETH> speed <option>
```

*Variables:*

- <ETH> is one of the options -- *eth1* or *eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

- <option> is one of the options: *auto*, *10Mbps*, *100Mbps* or *1000Mbps*.

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.
1000Mbps	The LAN speed is always 1000 Mbps.

## Changing the LAN Duplex Mode

This command determines the LAN interface duplex mode.

```
config:# network ethernet <ETH> duplexMode <mode>
```

*Variables:*

- <ETH> is one of the options -- *eth1* or *eth2*.

Option	Description
eth1	ETH1 port

Option	Description
eth2	ETH2 port

- <mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	The BCM2 selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the BCM2) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

## Setting the LAN MTU

This command sets the MTU for the ethernet interface.

```
config:#          network ethernet <ETH> mtu <mtu>
```

Variables:

- <ETH> is one of the options -- eth1 or eth2.
- <mtu> is the Maximum Transfer Unit. Enter a value from 1280-1500.

## Setting the Ethernet Authentication Method

BCM2 supports 802.1X (EAP) Network Authentication. Enable the ethernet interface, and then set the authentication method.

```
config:# network ethernet <interface> [enabled
      <enabled>]
```

The following command sets the authentication method for the selected Ethernet interface to either none or Extensible Authentication Protocol (EAP).

```
config:# network ethernet <ETH> authMethod <method>
```

Variables:

- <ETH> is one of the options -- *eth1* or *eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

- <method> is one of the authentication methods: *NONE* or *EAP*.

Method	Description
NONE	The authentication method is set to NONE.
EAP	The authentication method is set to EAP.

## Setting Ethernet EAP Parameters

When the selected Ethernet interface's authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, client certificate, client private key, password, CA certificate, and RADIUS authentication server. For more information, see Ethernet Interface Settings.

- ▶ *Determine the outer authentication protocol:*

```
config:# network ethernet <ETH> eapOuterAuthentication <outer_auth>
```

- ▶ *Determine the inner authentication protocol for authentication set to "EAP + PEAP":*

```
config:# network ethernet <ETH> eapInnerAuthentication <inner_auth>
```

- ▶ *Set the EAP identity:*

```
config:# network ethernet <ETH> eapIdentity <identity>
```

- ▶ *Set the EAP password:*

```
config:# network ethernet <ETH> eapPassword
```

After performing the above command, the BCM2 prompts you to enter the password. Then type the password and press Enter.

- ▶ *Provide a client certificate for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":*

```
config:#    network ethernet <ETH> eapClientCertificate
```

After performing any certificate or private key commands, including commands for the client certificate, client private key, and CA certificate, the system prompts you to enter the contents of the wanted certificate or key. For an example with detailed procedure, see [EAP CA Certificate Example](#) (on page 329).

- ▶ *Provide a client private key for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":*

```
config:#    network ethernet <ETH> eapClientPrivateKey
```

- ▶ *Provide a CA TLS certificate for EAP:*

```
config:#    network ethernet <ETH> eapCACertificate
```

- ▶ *Enable or disable verification of the TLS certificate chain:*

```
config:#    network ethernet <ETH> enableCertVerification <option1>
```

- ▶ *Allow expired and not yet valid TLS certificates:*

```
config:#    network ethernet <ETH> allowOffTimeRangeCerts <option2>
```

- ▶ *Allow network connection with incorrect system time:*

```
config:#    network ethernet <ETH> allowConnectionWithIncorrectClock  
           <option3>
```

- ▶ *Set the RADIUS authentication server for EAP:*

```
config:#    network ethernet <ETH> eapAuthServerName <FQDN>
```

*Variables:*

- <ETH> is one of the options -- *eth1* or *eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

- <outer\_auth> is one of the options: *PEAP* or *TLS*.

Option	Description
PEAP	Outer authentication is set to Protected Extensible Authentication Protocol (PEAP).
TLS	Outer authentication is set to TLS.

- <inner\_auth> is one of the options: *MS-CHAPv2* or *TLS*.

Option	Description
MSCHAPv2	Inner authentication is set to Microsoft's Challenge Authentication Protocol Version 2 (MS-CHAPv2).
TLS	Inner authentication is set to TLS.

- <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 network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.
false	The 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 network connection successful when the BCM2 system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.



Option	Description
false	The network connection is NOT successfully established when the BCM2 finds that the TLS certificate is not valid due to incorrect system time.

- <FQDN> is the name of the RADIUS server if it is present in the TLS certificate. The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

## EAP CA Certificate Example

This section provides a CA certificate example for the Ethernet interface "ETH1". Your CA certificate contents should be different from the contents displayed in this example.

In addition, the procedure of uploading the client certificate and client private key in CLI is similar to the following example, except for the CLI command.

### ► To provide a CA certificate:

1. Make sure you have entered the configuration mode.
2. Type the following command for ETH1 and press Enter.

```
config:# network ethernet eth1 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 ---
MIICJTCCAfigAwIBAgIEMaYgRzALBgqhkiG9w0BAQQwRTElMAkGA1UEBhMCVVMx
NjA0BgNVBAAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbWJmFjE5NjA1Mjg5MzQ5MDU5MDU5MDU5MDU5MDU5MDU5MDU5MDU5MDU5
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbWJmFjE5NjA1Mjg5MzQ5MDU5MDU5MDU5MDU5
ZSBTY2hvY2gwWDALBgqhkiG9w0BAQEDSQAwRgJBAwYydgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULa4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlyDTL2ftgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAiVTMTYwNAZDVQK
Ey1OYXRpb25hbCBBZXBmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBGGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFis2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLGItkCKp0F5EWIrVDwh54NNEvkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Select and copy the contents as illustrated below, including the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE."
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:#
```

## Removing the Uploaded Certificate or Private Key

The procedures of removing an existing client certificate, client private key or CA certificate in CLI are similar.

This section illustrates such a procedure for the Ethernet interface "ETH1."

### ► To remove a certificate or private key for ETH1:

1. Make sure you have entered the configuration mode.
2. Type the appropriate command, depending on which file you want to remove, and press Enter.

- *Client certificate:*

```
config:# network ethernet eth1 eapClientCertificate
```

- *Client private key:*

```
config:# network ethernet eth1 eapClientPrivateKey
```

- *CA certificate:*

```
config:# network ethernet eth1 eapCACertificate
```

3. The system prompts you to enter the contents of the chosen certificate or private key.
4. Press Enter without typing any data.
5. Verify whether the system shows the following command prompt, indicating the existing certificate or private key has been removed.

```
config:#
```

## 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 wireless networking mode is not enabled, the SSID, PSK and BSSID values are not applied until the wireless networking mode is enabled. 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

### Enabling or Disabling 802.11n High Throughput

This command enables or disables the 802.11n high throughput protocol.

```
config:# network wireless enableHT <option>
```

*Variables:*

- <option> is one of the options: *true* or *false*.

Option	Description
true	802.11n is enabled.
false	802.11n is disabled.

### Setting the Wireless Authentication Method

This command sets the wireless authentication method to None, 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 authentication method is set to PSK.
EAP	The authentication method is set to EAP.
None	The authentication method is set to None.

### 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 Wireless EAP Parameters

When the wireless authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, client certificate, client private key, password, CA certificate, and RADIUS authentication server. For more information, see [Wireless Network Settings](#).

- *Determine the outer authentication protocol:*

```
config:# network wireless eapOuterAuthentication <outer_auth>
```

- *Determine the inner authentication protocol for authentication set to "EAP + PEAP":*

```
config:# network wireless eapInnerAuthentication <inner_auth>
```

- *Set the EAP identity:*

```
config:# network wireless eapIdentity <identity>
```

- *Set the EAP password:*

```
config:# network wireless eapPassword
```

After performing the above command, the BCM2 prompts you to enter the password. Then type the password and press Enter.

- *Provide a Client Certificate for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":*

```
config:# network wireless eapClientCertificate
```

After performing any certificate or private key commands, including commands for the client certificate, client private key, and CA certificate, the system prompts you to enter the contents of the wanted certificate or key. For an example with detailed procedure, see [EAP CA Certificate Example](#) (on page 329).

- ▶ Provide a Client Private Key for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":

```
config:#      network wireless eapClientPrivateKey
```

- ▶ Provide a CA TLS certificate for EAP:

```
config:#      network wireless eapCACertificate
```

- ▶ 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>
```

- ▶ Set the RADIUS authentication server for EAP:

```
config:#      network wireless eapAuthServerName <FQDN>
```

*Variables:*

- <outer\_auth> is one of the options: *PEAP* or *TLS*.

Option	Description
PEAP	Outer authentication is set to Protected Extensible Authentication Protocol (PEAP).
TLS	Outer authentication is set to TLS.

- <inner\_auth> is one of the options: *MS-CHAPv2* or *TLS*.

Option	Description
MSCHAPv2	Inner authentication is set to Microsoft's Challenge Authentication Protocol Version 2 (MS-CHAPv2).
TLS	Inner authentication is set to TLS.

- <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 network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.
false	The 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 network connection successful when the BCM2 system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.
false	The network connection is NOT successfully established when the BCM2 finds that the TLS certificate is not valid due to incorrect system time.

- <FQDN> is the name of the RADIUS server if it is present in the TLS certificate. The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

## 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.

## Setting the Wireless MTU

This command sets the MTU for the wireless interface.

```
config:#          network wireless mtu<mtu>
```

Variables:

- <mtu> is the Maximum Transfer Unit. Enter a value from 1280-1500.

## Configuring the Cascading Mode

This command determines the cascading mode.

```
config:#      network <mode> enabled <option1>
```

Variables:

- <mode> is one of the following cascading modes.

Mode	Description
bridge	The 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.

---

**Important: When enabling either cascading mode, you must make sure the other cascading mode is disabled, or the preferred cascading mode may not be enabled successfully.**

---

- <option1> is one of the following options:

Option	Description
true	The selected cascading mode is enabled.
false	The selected cascading mode is disabled.

► *If Port Forwarding mode is enabled, you must configure two more settings to finish the configuration:*

On ALL cascaded devices, you must configure the 'role' setting one by one.

```
config:# network portForwarding role <option2>
```

On the primary device, you must configure the 'downstream interface' setting.

```
config:# network portForwarding
        primaryUnitDownstreamInterface <option3>
```

*Variables:*

- <option2> is one of the following cascading roles:

Role	Description
primary	The device is a primary device.
expansion	The device is an expansion device.

- <option3> is one of the following options:

Option	Description
ETH1/ETH2	ETH1/ETH2 port is the port where the 1st expansion device is connected.
Usb	USB port is the port where the 1st expansion device is connected.

## 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>
```

- ▶ *Enforce redirection from HTTP to HTTPS:*

```
config:# network services http enforceHttps <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	<ul style="list-style-type: none"><li>• The HTTP port is enabled.</li><li>- OR -</li><li>• HTTP redirection to HTTPS is enabled.</li></ul>
false	<ul style="list-style-type: none"><li>• The HTTP port is disabled.</li><li>- OR -</li><li>• HTTP redirection to HTTPS is disabled.</li></ul>

### Setting the HTTPS Port

The commands used to configure the HTTPS port settings begin with *network services https*.

► *Change the HTTPS port:*

```
config:# network services https port <n>
```

► *Enable or disable the HTTPS access:*

```
config:# network services https enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Forces any access to the BCM2 via HTTP to be redirected to HTTPS.
false	No HTTP access is redirected to HTTPS.

### Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

► *Enabling or Disabling Telnet*

This command enables or disables the Telnet service.

```
config:# network services telnet enabled <option>
```

*Variables:*

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.
false	The Telnet service is disabled.

### ► *Changing the Telnet Port*

This command changes the Telnet port.

```
config:# network services telnet port <n>
```

*Variables:*

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

### Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

### ► *Enabling or Disabling SSH*

This command enables or disables the SSH service.

```
config:# network services ssh enabled <option>
```

*Variables:*

- <option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.

Option	Description
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 enter a valid SSH public key for each user profile to log in over the SSH connection.

## 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.

### Setting Redfish Service

You can enable or disable the redfish service.

► *Enabling or Disabling Redfish service:*

```
config:# network services redfish enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The redfish service is enabled.
false	The redfish service is disabled.

## Enabling or Disabling Service Advertising

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services. See Enabling Service Advertising for details.

```
config:# network services zeroconfig <method> <option>
```

Variables:

- <method> is one of the options: *mdns* or *llmnr*.

Option	Description
mdns	Service advertisement via MDNS is enabled or disabled.
llmnr	Service advertisement via LLMNR is enabled or disabled.

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Service advertisement via the selected method (MDNS or LLMNR) is enabled.
disable	Service advertisement via the selected method (MDNS or LLMNR) is disabled.

## 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.
ntp	The date and time settings synchronize with a specified NTP server.

► *Setting NTP Parameters*

A time configuration command for NTP-related parameters begins with *time ntp*.

► *Specify the primary time server:*

```
config:#    time ntp firstServer <first_server>
```

► *Specify the secondary time server:*

```
config:#    time ntp secondServer <second_server>
```

► *To delete the primary time server:*

```
config:#          time ntp firstServer ""
```

► *To delete the secondary time server:*

```
config:#          time ntp secondServer ""
```

Variables:

- The <first\_server> is the IP address or host name of the primary NTP server.
- The <second\_server> is the IP address or host name of the secondary NTP server.

► *Customizing the Date and Time*

To manually configure the date and time, use the following CLI commands to specify them.

---

Note: You shall set the time configuration method to "manual" prior to customizing the date and time.

---



► *Assign the date:*

```
config:#    time set date <yyyy-mm-dd>
```

► *Assign the time:*

```
config:#    time set time <hh:mm:ss>
```

*Variables:*

Variable	Description
<yyyy-mm-dd>	Type the date in the format of yyyy-mm-dd. For example, type <i>2015-11-30</i> for November 30, 2015.
<hh:mm:ss>	Type the time in the format of hh:mm:ss in the 24-hour format. For example, type <i>13:50:20</i> for 1:50:20 pm.

## Setting the Time Zone

The CLI has a list of time zones to configure the date and time for BCM2.

```
config:#          time zone
```

After a list of time zones is displayed, type the index number of the time zone or press Enter to cancel.

► *To set the time zone:*

1. Type the time zone command as shown below and press Enter.

```
config:#          time zone
```

2. The system shows a list of time zones. Type the index number of the desired time zone and press Enter.
3. Type `apply` for the selected time zone to take effect.

## Setting the Automatic Daylight Savings Time

This command determines whether the daylight saving 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.

## Checking the Accessibility of NTP Servers

This command verifies the accessibility of NTP servers specified manually and then shows the result.

To perform this command successfully, you must:

- Own the "Change Date/Time Settings" permission.
- Customize NTP servers.

This command is available either in the administrator/user mode or in the configuration mode.

### ► *In the administrator/user mode:*

```
#          check ntp
```

### ► *In the configuration mode:*

```
config#          check ntp
```

## Example -Time Configuration

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
```

## Security Configuration Commands

A security configuration command begins with *security*.

### Firewall Control

You can manage firewall control features through the CLI. The firewall control lets you set up rules that permit or disallow access to the BCM2 from a specific or a range of IP addresses.

- An IPv4 firewall configuration command begins with *security ipAccessControl ipv4*.
- An IPv6 firewall configuration command begins with *security ipAccessControl ipv6*.

### Modifying Firewall Control Parameters

There are different commands for modifying firewall control parameters.

- *IPv4 commands*

- ▶ *Enable or disable the IPv4 firewall control feature:*

```
config:# security ipAccessControl ipv4 enabled <option>
```

- ▶ *Determine the default IPv4 firewall control policy for inbound traffic:*

```
config:# security ipAccessControl ipv4 defaultPolicyIn <policy>
```

- ▶ *Determine the default IPv4 firewall control policy for outbound traffic:*

```
config:# security ipAccessControl ipv4 defaultPolicyOut <policy>
```

- *IPv6 commands*

- ▶ *Enable or disable the IPv6 firewall control feature:*

```
config:# security ipAccessControl ipv6 enabled <option>
```

- ▶ *Determine the default IPv6 firewall control policy for inbound traffic:*

```
config:# security ipAccessControl ipv6 defaultPolicyIn <policy>
```

- *Determine the default IPv6 firewall control policy for outbound traffic:*

```
config:# security ipAccessControl ipv6 defaultPolicyOut <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the IP access control feature.
false	Disables the IP access control feature.

- <policy> is one of the options: *accept*, *drop* or *reject*.

Option	Description
accept	Accepts traffic from all IP addresses.
drop	Discards traffic from all IP addresses, without sending any failure notification to the source host.
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

## Managing Firewall Rules

You can add, delete or modify firewall rules using the CLI commands.

- An IPv4 firewall control rule command begins with *security ipAccessControl ipv4 rule*.
- An IPv6 firewall control rule command begins with *security ipAccessControl ipv6 rule*.

### Adding a Firewall Rule

Depending on where you want to add a new firewall rule in the list, the command for adding a rule varies.

- *IPv4 commands*

- *Add a new rule to the bottom of the IPv4 rules list:*

```
config:# security ipAccessControl ipv4 rule add <direction> <ip_mask>
        <policy>
```

- ▶ Add a new IPv4 rule by inserting it above or below a specific rule:

```
config:# security ipAccessControl ipv4 rule add <direction> <ip_mask>
        <policy> <insert> <rule_number>
```

-- OR --

```
config:# security ipAccessControl ipv4 rule add <direction> <insert>
        <rule_number> <ip_mask> <policy>
```

- IPv6 commands

- ▶ Add a new rule to the bottom of the IPv6 rules list:

```
config:# security ipAccessControl ipv6 rule add <direction> <ip_mask>
        <policy>
```

- ▶ Add a new IPv6 rule by inserting it above or below a specific rule:

```
config:# security ipAccessControl ipv6 rule add <direction> <ip_mask>
        <policy> <insert> <rule_number>
```

-- OR --

```
config:# security ipAccessControl ipv6 rule add <direction> <insert>
        <rule_number> <ip_mask> <policy>
```

#### Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <ip\_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept*, *drop* or *reject*.

Policy	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: <i>new rule's number = the specified rule number</i>
insertBelow	Inserts the new rule below the specified rule number. Then: <i>new rule's number = the specified rule number + 1</i>

- <rule\_number> is the number of the existing rule which you want to insert the new rule above or below.

## Modifying a Firewall Rule

Depending on what to modify in an existing rule, the command varies.

- *IPv4 commands*

### ► *Modify an IPv4 rule's IP address and/or subnet mask:*

```
config:# security ipAccessControl ipv4 rule modify <direction>
        <rule_number> ipMask <ip_mask>
```

### ► *Modify an IPv4 rule's policy:*

```
config:# security ipAccessControl ipv4 rule modify <direction>
        <rule_number> policy <policy>
```

► *Modify all contents of an existing IPv4 rule:*

```
config:# security ipAccessControl ipv4 rule modify <direction>
        <rule_number> ipMask <ip_mask> policy <policy>
```

- IPv6 commands

► *Modify an IPv6 rule's IP address and/or prefix length:*

```
config:# security ipAccessControl ipv6 rule modify <direction>
        <rule_number> ipMask <ip_mask>
```

► *Modify an IPv6 rule's policy:*

```
config:# security ipAccessControl ipv6 rule modify <direction>
        <rule_number> policy <policy>
```

► *Modify all contents of an IPv6 existing rule:*

```
config:# security ipAccessControl ipv6 rule modify <direction>
        <rule_number> ipMask <ip_mask> policy <policy>
```

*Variables:*

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule\_number> is the number of the existing rule that you want to modify.
- <ip\_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept*, *drop* or *reject*.

Option	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.

Option	Description
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

## Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

### ► IPv4 commands

```
config:# security ipAccessControl ipv4 rule delete <direction>
        <rule_number>
```

### ► IPv6 commands

```
config:# security ipAccessControl ipv6 rule delete <direction>
        <rule_number>
```

#### Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule\_number> is the number of the existing rule that you want to remove.

## Restricted Service Agreement

The CLI command used to set the Restricted Service Agreement feature begins with `security restrictedServiceAgreement`,

### Enabling or Disabling the Restricted Service Agreement

This command activates or deactivates the Restricted Service Agreement.

```
config:# security restrictedServiceAgreement enabled <option>
```

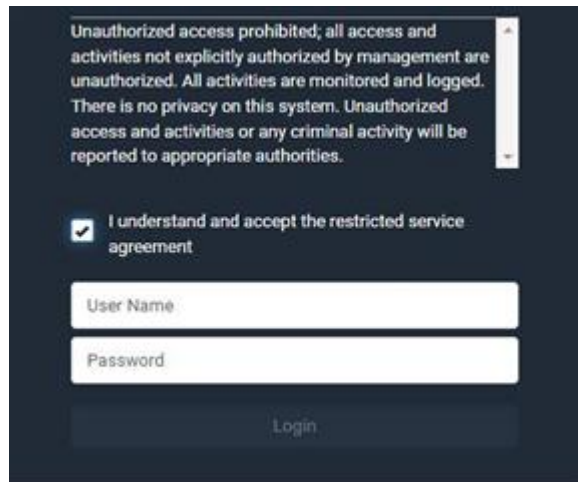
#### Variables:

- <option> is one of the options: *true* or *false*.



Option	Description
true	Enables the Restricted Service Agreement feature.
false	Disables the Restricted Service Agreement feature.

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed on the login screen.



Do either of the following, or the login fails:

- 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, first press Tab to go to the checkbox and then Enter.*

---

- 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.

---

## 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`.

### 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.

Option	Description
disable	Disables the password aging feature.

## Password Aging Interval

This command determines how often the password should be changed.

```
config:# security loginLimits passwordAgingInterval <value>
```

### Variables:

- <value> is a numeric value in days set for the password aging interval. The interval ranges from 7 to 365 days.

## Idle Timeout

This command determines how long a user can remain idle before that user is forced to log out of the BCM2 web interface or CLI.

```
config:# security loginLimits idleTimeout <value>
```

### Variables:

- <value> is a numeric value in minutes set for the idle timeout. The timeout ranges from 1 to 1440 minutes (24 hours).

## User Blocking

There are different commands for changing different user blocking parameters. These commands begin with `security userBlocking`.

- ▶ *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`.

### Enabling or Disabling Strong Passwords

This command enables or disables the strong password feature.

```
config:# security strongPasswords enabled <option>
```

*Variables:*

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the strong password feature.
false	Disables the strong password feature.

### Minimum Password Length

This command determines the minimum length of the password.

```
config:# security strongPasswords minimumLength <value>
```

*Variables:*

- <value> is an integer between 8 and 32.

### Maximum Password Length

This command determines the maximum length of the password.

```
config:# security strongPasswords maximumLength <value>
```

*Variables:*

- <value> is an integer between 16 and 64.

### Lowercase Character Requirement

This command determines whether a strong password includes at least a lowercase character.

```
config:# security strongPasswords enforceAtLeastOneLowerCaseCharacter  
        <option>
```

*Variables:*

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.
disable	No lowercase character is required.

### Uppercase Character Requirement

This command determines whether a strong password includes at least an 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.

Option	Description
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.

---

## 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.

## Enabling or Disabling Front Panel Outlet Switching

---

---

This section applies to outlet-switching capable models only.

---

---

The following CLI commands control whether you can turn on or off an outlet by operating the front panel display.

- *To enable the front panel outlet control feature:*

```
config:# security frontPanelPermissions add switchOutlet
```

- *To disable the front panel outlet control feature:*

```
config:# security frontPanelPermissions remove switchOutlet
```

---

Tip: If your BCM2 supports multiple front panel permissions, you can combine them into one command by adding a semicolon (;) between different permissions. For example, the following CLI command enables both front panel actuator control and outlet switching functions simultaneously.

```
security frontPanelPermissions add switchActuator;switchOutlet
```

---

## Enabling or Disabling Front Panel Actuator Control

The following CLI commands control whether you can turn on or off connected actuator(s) by operating the front panel LCD display.

- *To enable the front panel actuator control feature:*

```
config:# security frontPanelPermissions add switchActuator
```

- *To disable the front panel actuator control feature:*

```
config:# security frontPanelPermissions remove switchActuator
```

---

Tip: If your BCM2 supports multiple front panel permissions, you can combine them into one command by adding a semicolon (;) between different permissions. For example, the following CLI command enables both front panel actuator control and the internal beeper-muting functions simultaneously.

```
security frontPanelPermissions add switchActuator;muteBeeper
```

---

## Enabling or Disabling Front Panel Beeper-Sound Control

The following CLI commands control whether you can mute the internal beeper by operating the front panel LCD display when the beeper sounds.

- ▶ *To enable the front panel beeper sound control feature:*

```
config:# security frontPanelPermissions add muteBeeper
```

- ▶ *To disable the front panel actuator control feature:*

```
config:# security frontPanelPermissions remove muteBeeper
```

---

Tip: If your BCM2 supports multiple front panel permissions, you can combine them into one command by adding a semicolon (;) between different permissions. For example, the following CLI command enables both front panel actuator control and the the internal beeper-muting functions simultaneously.

```
security frontPanelPermissions add switchActuator;muteBeeper
```

---

## User Configuration Commands

Most user configuration commands begin with *user* except for the password change command.

### Creating a User Profile

This command creates a new user profile.

```
config:# user create <name> <option> <roles>
```

After performing the user creation command, the BCM2 prompts you to assign a password to the newly-created user. Then:

1. Type the password and press Enter.
2. Re-type the same password for confirmation and press Enter.

*Variables:*

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable CANNOT contain spaces.
- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the newly-created user profile.

Option	Description
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.

---

### 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, you are prompted 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.

#### ► Example

The following procedure illustrates how to change the password of the user "May."

1. Verify that you have entered the configuration mode.
2. Type the following command to change the password for the user profile "May."

```
config:#          user modify May password
```

3. Type a new password when prompted, and press Enter.
4. Type the same new password and press Enter.
5. If the password change is completed successfully, the config:# prompt appears.

### 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.

► *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 64 ASCII printable characters. The <full\_name> variable must be enclosed in quotes when it contains spaces.
- <phone\_number> is the phone number that can reach the specified user. The <phone\_number> variable must be enclosed in quotes when it contains spaces.
- <email\_address> is the email address of the specified user.

### Enabling or Disabling a User Profile

This command enables or disables a user profile. A user can log in to the BCM2 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.

- ▶ *Enable or disable the SNMP v3 access to BCM2 for the specified user:*

```
config:# user modify <name> snmpV3Access <option1>
```

- ▶ *Determine the security level:*

```
config:# user modify <name> securityLevel <option2>
```

- ▶ *Determine whether the authentication passphrase is identical to the password:*

```
config:# user modify <name> userPasswordAsAuthenticationPassphrase  
        <option3>
```

- ▶ *Determine the authentication passphrase:*

```
config:# user modify <name> authenticationPassPhrase
```

After performing the above command, the system prompts you to enter the authentication passphrase.

- ▶ *Determine whether the privacy passphrase is identical to the authentication passphrase:*

```
config:# user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase  
        <option4>
```



► *Determine the privacy passphrase:*

```
config:#          user modify <name> privacyPassPhrase
```

After performing the above command, the system prompts you to enter the privacy passphrase.

► *Determine the authentication protocol:*

```
config:#  user modify <name> authenticationProtocol <option5>
```

► *Determine the privacy protocol:*

```
config:#  user modify <name> privacyProtocol <option6>
```

*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.

- <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.

- <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.

- <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.

- <option5> is one of the following options:

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.
SHA-224	SHA-224 authentication protocol is applied.
SHA-256	SHA-256 authentication protocol is applied.
SHA-384	SHA-384 authentication protocol is applied.
SHA-512	SHA-512 authentication protocol is applied.

- <option6> is one of the following options:

Option	Description
DES	DES privacy protocol is applied.
AES-128	AES-128 privacy protocol is applied.
AES-192	AES-192 privacy protocol is applied.
AES-256	AES-256 privacy protocol is applied.
AES-192 (3DES key extension)	AES-192 privacy protocol is applied.
AES-256 (3DES key extension)	AES-256 privacy protocol is applied.

- An authentication or privacy passphrase is a string comprising 8 to 32 ASCII printable characters.

### 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.

## 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.

---

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

---

► *Set the preferred temperature unit:*

```
config:# user modify <name> preferredTemperatureUnit <option1>
```

► *Set the preferred length unit:*

```
config:# user modify <name> preferredLengthUnit <option2>
```

► *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.
- <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.

- <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.

- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

## Specifying the SSH Public Key

If the SSH key-based authentication is enabled, specify the SSH public key for each user profile using the following procedure.

### ► To specify or change 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.

### ► To remove an existing SSH public key:

1. Type the same command as shown above.
2. When the system prompts you to input the contents, press Enter without typing or pasting anything.

### ► Example

The following procedure illustrates how to change the SSH public key for the user "assistant."

1. Verify that you have entered the configuration mode.
2. Type the following command and press Enter.

```
config:#          user modify assistant sshPublicKey
```

3. You are prompted to enter a new SSH public key.
4. Type the new key and press Enter.

## 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 system prompts you to enter both current and new passwords respectively.

---

**Important: After the password is changed successfully, the new password is effective immediately whether or not you type the command "apply" to save the changes.**

---

### ► *Example*

This procedure changes your own password:

1. Verify that you have entered the configuration mode.
2. Type the following command and press Enter.

```
config:#                password
```

3. Type the existing password and press Enter when the following prompt appears.  
Current password:
4. Type the new password and press Enter when the following prompt appears.  
Enter new password:
5. Re-type the new password for confirmation and press Enter when the following prompt appears.  
Re-type new password:

## Setting Default Measurement Units

Default measurement units, including temperature, length, and pressure units, apply to the 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.

---

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

---

### ► *Set the default temperature unit:*

```
config:# user defaultpreferences preferredTemperatureUnit <option1>
```

► *Set the default length unit:*

```
config:# user defaultpreferences preferredLengthUnit <option2>
```

► *Set the default pressure unit:*

```
config:# user defaultpreferences preferredPressureUnit <option3>
```

*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.

- <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.

- <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.

## 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.
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

## All Privileges

This table lists all privileges. Note that available privileges vary according to the model you purchased. For example, a PDU without the outlet switching function does not have the privilege "switchOutlet."

Privilege	Description
acknowledgeAlarms	Acknowledge Alarms
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration
changeAuthSettings	Change Authentication Settings
changeDataTimeSettings	Change Date/Time Settings
changeExternalSensorsConfiguration	Change Peripheral Device Configuration
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePduConfiguration	Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings
changeUserSettings	Change Local User Management
changeWebcamSettings	Change Webcam Configuration
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update

Privilege	Description
performReset	Reset (Warm Start)
switchActuator*	Switch Actuator
switchOutlet**	Switch Outlet
switchOutletGroup***	Switch Outlet Group
viewAuthSettings	View Authentication Settings
viewEventSetup	View Event Settings
viewEverything	Unrestricted View Privileges
viewLog	View Local Event Log
viewSecuritySettings	View Security Settings
viewSnmpSettings	View SNMP Settings
viewUserSettings	View Local User Management
viewWebcamSettings	View Webcam Snapshots and Configuration

\* The "switchActuator" privilege requires an argument that is separated with a colon. The argument could be:

- All actuators, that is,  
`switchActuator:all`
- An actuator's ID number. For example:  
`switchActuator:1`  
`switchActuator:2`  
`switchActuator:3`
- A list of comma-separated ID numbers of different actuators. For example:  
`switchActuator:1,3,6`

---

*Note: The ID number of each actuator is shown in the BCM2 web interface. It is an integer.*

---

\*\* The "switchOutlet" privilege requires an argument that is separated with a colon. The argument could be:

- All outlets, that is,  
`switchOutlet:all`
- An outlet number. For example:  
`switchOutlet:1`  
`switchOutlet:2`



```
switchOutlet:3
```

- A list of comma-separated outlets. For example:

```
switchOutlet:1,3,5,7,8,9
```

\*\*\* The "switchOutletGroup" privilege requires an argument that is separated with a colon. The argument could be:

- All outlet groups, that is,

```
switchOutletGroup:all
```

- An outlet group number. For example:

```
switchOutletGroup:1
```

```
switchOutletGroup:2
```

```
switchOutletGroup:3
```

- A list of comma-separated outlet groups. For example:

```
switchOutletGroup:1,3,5,7,8,9
```

## 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>"
```

- ▶ *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>...;  
...
```

- ▶ *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.
- <description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See *All Privileges* (on page ).
- <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. For arguments syntax, see *All Privileges* (on page ).

## Deleting a Role

This command deletes an existing role.

```
config:#          role delete <name>
```

## Example - Creating a Role

The following command creates a new role and assigns privileges to the role.

```
config:#  role create tester firmwareUpdate;viewEventSetup
```

*Results:*

- A new role "tester" is created.
- Two privileges are assigned to the role: firmwareUpdate (Firmware Update) and viewEventSetup (View Event Settings).

## Authentication Commands

An authentication configuration command begins with *authentication*.

## Determining the Authentication Method

You can choose to set the authentication type only, or both set the authentication type and determine whether to switch to local authentication in case the remote authentication is not available.

- *Determine the authentication type only:*

```
config:# authentication type <option1>
```

- *Determine the authentication type and enable/disable the option of switching to local authentication:*

```
config:# authentication type <option1> useLocalIfRemoteUnavailable  
      <option2>
```

---

Note: You cannot enable or disable the option of switching to local authentication without determining the authentication type in the CLI. Therefore, always type "authentication type <option1>" when setting up "useLocalIfRemoteUnavailable".

---

*Variables:*

- <option1> is one of the options: *local*, *ldap* or *radius*.

Option	Description
local	Enable Local authentication only.
ldap	Enable LDAP authentication only.
radius	Enable Radius authentication only.
tacplus	Enable TACACS+ authentication only.

- <option2> is one of the options: *true* or *false*.

Option	Description
true	Remote authentication is the first priority. The device will switch to local authentication when the remote authentication is not available.
false	Always stick to remote authentication regardless of the availability of remote authentication.

## LDAP Settings

All LDAP-related commands begin with *authentication ldap*.

If you enable LDAP authentication, you must add at least one LDAP server. Later you can modify or delete any existing LDAP server as needed.

## Adding an LDAP Server

Adding an LDAP server requires the entry of quite a lot of parameters, such as the server's IP address, TCP port number, Base DN and so on.

You can repeat the following CLI command to add more than one LDAP server.

► **Add a new LDAP server:**

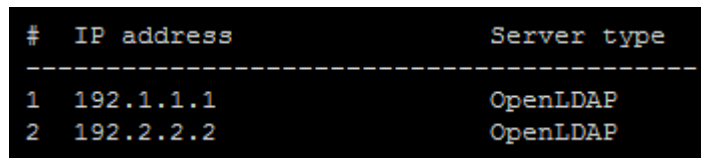
```
config:# authentication ldap add <host> <port> <ldap_type> <security>
      <bind_type> <base_DN> <login_name_att> <user_entry_class> "Optional
      Parameters"
```

---

Note: "Optional Parameters" refer to one or multiple parameters listed in the section *Optional Parameters*. They are required only when your server settings need to specify these parameters. For example, if setting the <bind\_type> to "authenticatedBind", then you must add the parameter "bindDN" to this command.

---

When the above command is successfully performed, a list of all LDAP servers, including the newly-added one, will be displayed, which is similar to the following diagram.



```
# IP address          Server type
-----
1 192.1.1.1           OpenLDAP
2 192.2.2.2           OpenLDAP
```

*Variables:*

- <host> is the IP address or host name of the LDAP server.
- <port> is the port number assigned for communication with the LDAP server.
- <ldap\_type> is one of the LDAP server types: *openldap* or *activeDirectory*.

Type	Description
openldap	OpenLDAP server
activeDirectory	Microsoft Active Directory

- <security> is one of the security options: *none*, *startTls* or *tls*.

Type	Description
none	No security
startTls	StartTLS

Type	Description
tls	TLS

- <bind\_type> is one of the bind options: *anonymousBind*, or *authenticatedBind*.

Type	Description
anonymousBind	Enable the anonymous Bind. Bind DN and password are NOT required.
authenticatedBind	Enable the Bind with authentication. Bind DN and password are required.

- <base\_DN> is the base DN for search.
- <login\_name\_att> is the login name attribute.
- <user\_entry\_class> is the User Entry Object Class.

### Optional Parameters

You can add one or multiple "optional parameters", such as specifying the Bind DN or certificate upload, to an LDAP-server-adding command as illustrated below. If adding multiple optional parameters, you must add them to the END of the command and separate them with a space.

- *Example 1 -- Specify an Active Directory Domain's name:*

```
config:# authentication ldap add <host> <port> <ldap_type> <security>
      <bind_type> <base_DN> <login_name_att> <user_entry_class>
      adDomain <AD_domain>
```

- *Example 2 -- Set up the bind DN:*

```
config:# authentication ldap add <host> <port> <ldap_type> <security>
      <bind_type> <base_DN> <login_name_att> <user_entry_class> bindDN
      <bind_DN>
```

#### ► "Optional Parameters" table:

Parameters	To configure
userSearchSubfilter <filter>	User search subfilter
bindDN <bind_DN>	bind DN <ul style="list-style-type: none"> <li>• The system will prompt you to enter and re-confirm the bind password after adding this parameter to the command.</li> </ul>
adDomain <AD_domain>	Active Directory Domain name

Parameters	To configure
verifyServerCertificate <verify_cert>	Certificate verification setting <ul style="list-style-type: none"> <li>After setting to true, the system will prompt you to upload a certificate.</li> </ul>
allowExpiredCertificate <allow_exp_cert>	Whether to accept expired or not valid yet certificate

*Variables:*

- <filter> is the user search subfilter you specify.
- <bind\_DN> is bind DN.
- <AD\_domain> is the Active Directory Domain.
- <verify\_cert> is one of the options: *true* or *false*.

Option	Description
true	Enable the verification of the LDAP server certificate.
false	Disable the verification of the LDAP server certificate.

- <allow\_exp\_cert> is one of the options: *true* or *false*.

Option	Description
true	Certificates that are either expired or not valid yet are all accepted.
false	Only valid certificates are accepted.

### Illustrations of Adding LDAP Servers

This section shows several LDAP command examples. Those words highlighted in bold are required for their respective examples.

► *An OpenLDAP server:*

```
config:# authentication ldap add op-ldap.raritan.com 389 openldap none
anonymousBind dc=raritan,dc=com uid inetOrgPerson
```

► *A Microsoft Active Directory server:*

```
config:# authentication ldap add ac-ldap.raritan.com 389 activeDirectory none
anonymousBind dc=raritan,dc=com SAMAccountName user adDomain
raritan.com
```

► *An LDAP server with a TLS certificate uploaded:*

**a. Enter the CLI command with the following two TLS-related options set and/or added:**

- <security> is set to `tls` or `startTls`.
- The `"verifyServerCertificate"` parameter is added to the command and set to `"true"`.

```
config:# authentication ldap add ldap.raritan.com 389 openldap startTls ...
      inetOrgPerson verifyServerCertificate true
```

**b. The system now prompts you to enter the certificate's content.**

**c. Type or copy the certificate's content in the CLI and press Enter.**

---

Note: Select and copy the content including the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE."

---

► An LDAP server with the bind DN and bind password configured:

**a. Enter the CLI command with the "bindDN" parameter and its data added.**

```
config:# authentication ldap add op-ldap.raritan.com 389 openldap none
      authenticatedBind cn=Manager,dc=raritan,dc=com uid inetOrgPerson bindDN
      user@raritan.com
```

**b. The system prompts you to specify the bind DN password.**

**c. Type the password and press Enter.**

**d. Re-type the same password.**

## Copying an Existing Authentication Server's Settings

If the server that you will add completely shares the same settings with any server that has been configured, use the following command.

► Add an LDAP server by copying an existing server's settings:

```
config:# authentication ldap addClone <server_num> <host>
```

*Variables:*

- <host> is the IP address or host name of the LDAP server.
- <server\_num> is the sequential number of the specified server shown on the server list.

## Modifying an Existing LDAP Server

You can modify one or multiple parameters of an existing LDAP server, such as its IP address, TCP port number, Base DN and so on. Besides, you can also change the priority or sequence of existing LDAP servers in the server list.

► *Command syntax:*

A command to modify an existing LDAP server's settings looks like the following:

```
config:# authentication ldap modify <server_num> "parameters"
```

*Variables:*

- <server\_num> is the sequential number of the specified server in the LDAP server list.
- Replace "parameters" with one or multiple commands in the following table, depending on which parameter(s) you want to modify.

► *Parameters:*

Parameters	Description
<b>host &lt;host&gt;</b>	Change the IP address or host name. <ul style="list-style-type: none"> <li>• &lt;host&gt; is the new IP address or host name.</li> </ul>
<b>port &lt;port&gt;</b>	Change the TCP port number. <ul style="list-style-type: none"> <li>• &lt;port&gt; is the new TCP port number.</li> </ul>
<b>serverType &lt;ldap_type&gt;</b>	Change the server type. <ul style="list-style-type: none"> <li>• &lt;ldap_type&gt; is the new type of the LDAP server.</li> <li>• &lt;ldap_type&gt; values include: <code>openldap</code> and <code>activeDirectory</code>.</li> </ul>
<b>securityType &lt;security&gt;</b>	Change the security type. <ul style="list-style-type: none"> <li>• &lt;security&gt; is the new security type.</li> <li>• &lt;security&gt; values include: <code>none</code>, <code>startTls</code>, and <code>ssl</code></li> </ul>
<b>bindType &lt;bind_type&gt;</b>	Change the bind type. <ul style="list-style-type: none"> <li>• &lt;bind_type&gt; is the new bind type.</li> <li>• &lt;bind_type&gt; values include: <code>anonymousBind</code> and <code>authenticatedBind</code>.</li> </ul>
<b>searchBaseDN &lt;base_DN&gt;</b>	Change the base DN for search. <ul style="list-style-type: none"> <li>• &lt;base_DN&gt; is the new base DN for search.</li> </ul>
<b>loginNameAttribute &lt;login_name_att&gt;</b>	Change the login name attribute. <ul style="list-style-type: none"> <li>• &lt;login_name_att&gt; is the new login name attribute.</li> </ul>
<b>userEntryObjectClass &lt;user_entry_class&gt;</b>	Change the user entry object class. <ul style="list-style-type: none"> <li>• &lt;user_entry_class&gt; is the new user entry class.</li> </ul>
<b>userSearchSubfilter &lt;user_search_filter&gt;</b>	Change the user search subfilter. <ul style="list-style-type: none"> <li>• &lt;user_search_filter&gt; is the new user search subfilter.</li> </ul>



Parameters	Description
<b>adDomain &lt;AD_domain&gt;</b>	Change the Active Directory Domain name. <ul style="list-style-type: none"> <li>&lt;AD_domain&gt; is the new domain name of the Active Directory.</li> </ul>
<b>verifyServerCertificate &lt;verify_cert&gt;</b>	Enable or disable the certificate verification. <ul style="list-style-type: none"> <li>&lt;verify_cert&gt; enables or disables the certificate verification feature.</li> <li>Available values include: <code>true</code>, <code>false</code></li> </ul>
<b>certificate</b>	Re-upload a different certificate. <ol style="list-style-type: none"> <li>First add the "certificate" parameter to the command, and press Enter.</li> <li>The system prompts you for the input of the certificate.</li> <li>Type or copy the content of the certificate in the CLI and press Enter.</li> </ol>
<b>allowExpiredCertificate &lt;allow_exp_cert&gt;</b>	Determine whether to accept a certificate which is expired or not valid yet. <ul style="list-style-type: none"> <li>&lt;allow_exp_cert&gt; determines whether to accept an expired or not valid yet certificate</li> <li>&lt;allow_exp_cert&gt; values include: <code>true</code>, and <code>false</code></li> </ul>
<b>bindDN &lt;bind_DN&gt;</b>	Change the bind DN. <ul style="list-style-type: none"> <li>&lt;bind_DN&gt; is the new bind DN.</li> </ul>
<b>bindPassword</b>	Change the bind DN password. <ol style="list-style-type: none"> <li>First add the "bindPassword" parameter to the command, and press Enter.</li> <li>The system prompts you for the input of the password.</li> <li>Type the password and press Enter.</li> </ol>
<b>sortPosition &lt;position&gt;</b>	Change the priority of the server (that is, resorting). <ul style="list-style-type: none"> <li>&lt;position&gt; is the new sequential number of the server in the LDAP server list.</li> </ul>

► *Examples:*

- Change the IP address of the 1st LDAP server

```
config:# authentication ldap modify 1 host 192.168.3.3
```

- Change both the IP address and TCP port of the 1st LDAP server

```
config:# authentication ldap modify 1 host 192.168.3.3 port 633
```

- Change the IP address, TCP port and the type of the 1st LDAP server

```
config:# authentication ldap modify 1 host 192.168.3.3 port 633
serverType activeDirectory
```

## Removing an Existing LDAP Server

This command removes an existing LDAP server from the server list.

```
config:# authentication ldap delete <server_num>
```

*Variables:*

- <server\_num> is the sequential number of the specified server in the LDAP server list.

## Radius Settings

All Radius-related commands begin with *authentication radius*.

If you enable Radius authentication, you must add at least one Radius server. Later you can modify or delete any existing Radius server as needed.

### Adding a Radius Server

You can repeat the following commands to add Radius servers one by one.

► *Command syntax:*

```
config:# authentication radius add <host> <rds_type> <auth_port>  
      <acct_port> <timeout> <retries>
```

*Variables:*

- <host> is the IP address or host name of the Radius server.
- <rds\_type> is one of the Radius authentication types: *pap*, *chap*, *msChapV2*.

Type	Description
chap	CHAP
pap	PAP
msChapV2	MSCHAP v2

- <auth\_port> is the authentication port number.
- <acct\_port> is the accounting port number.
- <timeout> is the timeout value in seconds. It ranges between 1 to 10 seconds.
- <retries> is the number of retries. It ranges between 0 to 5.

► *To enter the shared secret:*

1. After executing the above Radius command, the system automatically prompts you to enter the shared secret.
2. Type the secret and press Enter.
3. Re-type the same secret and press Enter.

► *Example:*

```
config:# authentication radius add 192.168.7.99 chap 1812 1813 10 3
```

## Modifying an Existing Radius Server

You can modify one or multiple parameters of an existing Radius server, or change the priority or sequence of existing servers in the server list.

► *Change the IP address or host name:*

```
config:# authentication radius modify <server_num> host <host>
```

► *Change the Radius authentication type:*

```
config:# authentication radius modify <server_num> authType <rds_type>
```

► *Change the authentication port:*

```
config:# authentication radius modify <server_num> authPort <auth_port>
```

► *Change the accounting port:*

```
config:# authentication radius modify <server_num> accountPort <acct_port>
```

► *Change the timeout value:*

```
config:# authentication radius modify <server_num> timeout <timeout>
```

► *Change the number of retries:*

```
config:# authentication radius modify <server_num> retries <retries>
```

► *Change the shared secret:*

```
config:# authentication radius modify <server_num> secret
```

► *Change the priority of the specified server:*

```
config:# authentication radius modify <server_num> sortPositon <position>
```

---

**Tip:** You can add more than one parameters to the command. For example, "authentication radius modify <server\_num> host <host> authType <rds\_type> authPort <auth\_port> accountPort <acct\_port> ...".

---

*Variables:*

- <server\_num> is the sequential number of the specified server in the Radius server list.
- <host> is the new IP address or host name of the Radius server.
- <rds\_type> is one of the Radius authentication types: *pap, chap, msChapV2*.
- <auth\_port> is the new authentication port number.
- <acct\_port> is the new accounting port number.
- <timeout> is the new timeout value in seconds. It ranges between 1 to 10 seconds.
- <retries> is the new number of retries. It ranges between 0 to 5.

► *To enter the shared secret:*

1. After executing the above Radius command, the system automatically prompts you to enter the shared secret.
2. Type the secret and press Enter.
3. Re-type the same secret and press Enter.

► *Example:*

```
config:# authentication radius add 192.168.7.99 chap 1812 1813 10 3
```

## Removing an Existing Radius Server

This command removes an existing Radius server from the server list.

```
config:# authentication radius delete <server_num>
```

*Variables:*

- <server\_num> is the sequential number of the specified server in the Radius server list.

## TACACS+ Settings

All TACACS+ related commands begin with *authentication tacplus*.

If you enable TACACS+ authentication, you must add at least one TACACS+ server. Later you can modify or delete any existing TACACS+ server as needed.

### Adding TACACS+ Server

You can repeat the following commands to add TACACS+ server one by one.

#### ► *Command syntax:*

```
config:# authentication tacplus add <host> [port <port>] [type ] [timeout  
      <timeout>] [retries <retries>] [disableAcct <disableacct>]
```

*Variables:*

- <host> is the IP address or host name of the TACACS+ server.
- <port> is the port number (Default: 49) (1..65535).
- is one of the authentication type (Default: msChap) (ascii/pap/chap/msChap).

Type	Description
ascii	ASCII
chap	CHAP
pap	PAP
msChap	MSCHAP

- <timeout> is the timeout value in seconds. It ranges between 1 to 60 seconds.
- <retries> is the number of retries. It ranges between 0 to 5.
- <disableAcct> is disable Accounting (true/false).

#### ► *To enter the shared secret:*

1. After executing the above TACACS+ command, the system automatically prompts you to enter the shared secret.
2. Type the secret and press Enter.
3. Re-type the same secret and press Enter.

► *Example:*

```
config:# authentication tacplus add 192.168.7.99 port 49 type chap timeout  
5 retries 3 disableAcct false
```

### Modifying an Existing TACACS+ Server

You can modify one or multiple parameters of an existing TACACS+ server, or change the priority or sequence of existing servers in the server list.

► *Change the IP address or host name:*

```
config:# authentication tacplus modify <index> host <host>
```

► *Change the authentication type:*

```
config:# authentication tacplus modify <index> type
```

► *Change the authentication port:*

```
config:# authentication tacplus modify <index> port <port>
```

► *Change the timeout value:*

```
config:# authentication tacplus modify <index> timeout <timeout>
```

► *Change the number of retries:*

```
config:# authentication tacplus modify <index> retries <retries>
```

► *Disable or Enable the account:*

```
config:# authentication tacplus modify <index> disableAcct <disableacct>
```

► *Change the shared secret:*

```
config:# authentication tacplus modify <index> secret
```

► *Change the priority of the specified server:*

```
config:# authentication tacplus modify <index> sortPositon <position>
```

---

Tip: You can add more than one parameters to the command. For example, "authentication tacplus modify <index> host <host> type port <port> disableAcct <disableacct> ...".

---

*Variables:*

- <index> is the sequential number of the specified server in the TACACS+ server list.
- <host> is the new IP address or host name of the TACACS+ server.
- <port> is the new authentication port number.
- is one of the TACACS+ authentication types: *pap*, *chap*, *msChapV2*.
- <timeout> is the new timeout value in seconds. It ranges between 1 to 10 seconds.
- <retries> is the new number of retries. It ranges between 0 to 5.
- <disableacct> is to disable or enable the account.

► *To enter the shared secret:*

1. After executing the above TACACS+ command, the system automatically prompts you to enter the shared secret.
2. Type the secret and press Enter.
3. Re-type the same secret and press Enter.

► *Example:*

```
config:# authentication tacplus modify 1 host 192.168.25.1 port 49 type  
pap timeout 5 retries 3 disableAcct False
```

## Removing an Existing TACACS+ Server

This command removes an existing TACACS+ server from the server list.

```
config:# authentication tacplus delete <index>
```

*Variables:*

- <index> is the sequential number of the specified server in the TACACS+ server list.

## 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. Actuators are configured with their own commands.

### 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 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.
- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

### Specifying the CC Sensor Type

Raritan's contact closure sensor supports the connection of diverse third-party. You must specify the type of connected detector/switch for proper operation. Use this command when you need to specify the sensor type.

```
config:# externalsensor <n> sensorSubType <sensor_type>
```

*Variables:*

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.
- <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 BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

## Setting the Y Coordinate

This command specifies the Y coordinate of an environmental sensor.

```
config:# externalsensor <n> ylabel "<coordinate>"
```

*Variables:*

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.
- <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 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.
- 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.

## 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 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes when it contains spaces.

## Using Default Thresholds

This command determines whether default thresholds, including the deassertion hysteresis and assertion timeout, are applied to a specific environmental sensor.

```
config:# externalsensor <n> useDefaultThresholds <option>
```

### Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.
- <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 DX2-passive infrared sensor

This command determines the value of the Alarmed to Normal Delay setting for a Raritan presence detector.

```
config:# externalsensor <n> alarmedToNormalDelay <time>
```

*Variables:*

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the BCM2 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.
- <time> is an integer number in seconds, ranging between 0 and 300.

## 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.

- ▶ *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 <sup>3</sup> (that is, g/m <sup>3</sup> )
relativeHumidity	%
temperature	Degrees Celsius (°C) or Fahrenheit (°F), depending on your measurement unit settings.
airPressure	Pascal (Pa) or psi, depending on your measurement unit settings.
airFlow	m/s
vibration	g

- <hy\_value> is the deassertion hysteresis value applied to the specified sensor type.
- <as\_value> is the assertion timeout value applied to the specified sensor type. It ranges from 0 to 100 (samples).

## Example - Default Upper Thresholds for Temperature

It is assumed that your preferred measurement unit for temperature is set to degrees Celsius. Then the following command sets the default Upper Warning threshold to 20 °C and Upper Critical threshold to 24 °C for all temperature sensors.

```
config:# defaultThresholds temperature upperWarning 20
        upperCritical 24
```

## Commands for Environmental Sensors

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.

- ▶ *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 web interface or using the command "show externalsensors <n>" in the CLI. It is an integer starting at 1.
- <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

---

*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.
- <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.

## 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.

► *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 web interface or CLI. It is an integer starting at 1.
- <name> is a string comprising up to 64 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.

- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes when it contains spaces.

## Example - Actuator Naming

The following command assigns the name "Door lock of cabinet 3" to the actuator whose ID number is 9.

```
config:# actuator 9 name "Door lock of cabinet 3"
```

## 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 an unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the BCM2 resumes pinging after declaring the monitored device "Unreachable." Valid range is 5 to 120 (seconds).
- <disable\_count> is the number of consecutive "Unreachable" declarations before the BCM2 disables the ping monitoring feature for the monitored device and returns to the "Waiting for reliable connection" state. Valid range is 1 to 100 or *unlimited*.

## Deleting a Monitored Device

This command removes a monitored IT device from the server reachability list.

```
config:#      serverReachability delete <n>
```

*Variables:*

- <n> is a number representing the sequence of the IT device in the monitored server list. You can find each IT device's sequence number using the CLI command of `show serverReachability` as illustrated below.

#	IP address	Enabled	Status
1	192.168.84.126	Yes	Waiting for reliable connection
2	www.raritan.com	Yes	Waiting for reliable connection

## Modifying a Monitored Device's Settings

The command to modify a monitored IT device's settings begins with `serverReachability modify`.

You can modify various settings for a monitored device at a time.

- ▶ *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 an unsuccessful ping:**

```
config:# serverReachability modify <n> waitTimeAfterUnsuccessfulPing
      <fail_wait>
```

- ▶ **Modify the wait time before resuming pingging after declaring "Unreachable":**

```
config:# serverReachability modify <n> waitTimeBeforeResumingPingging
      <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 an unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the system 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 disabling 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
```

## Peripheral Devices Configuration Commands

You can use the CLI to set the Z Coordinate format for external sensors, set the device altitude, enable/disable device auto management, set the active powered dry contact limit, and enable/disable the "mute other door handle" setting.

Peripheral device configuration commands begin with:

```
config:# peripheralDevicesSetup
```

Field	Description	More Information
<i>externalSensorsZCoordinateFormat</i>	Keyword	Z coordinate refers to the height of sensors.
<i>rackUnits / freeForm</i>	Enter one of these values	rackUnits: The height of the Z coordinate is measured in standard rack units. Type a numeric value in the rack unit to describe the Z coordinate. freeForm: Any alphanumeric string can be used for specifying the Z coordinate.
<i>deviceAltitude</i>	Keyword	Specifies the altitude of your PDU above sea level (in meters). Must be set if a differential air pressure sensor is attached because the device's altitude is associated with the altitude correction factor.

<i>number1</i>	Enter an integer number from -425 up to 3000 when using Meters.	Negative numbers indicate altitude below sea level.
<i>peripheralDeviceAutoManagement</i>	Keyword	Enable or disable the automatic management feature for sensors.
<i>enable / disable</i>	Enter one of these values	
<i>activePoweredDryContactLimit</i>	Keyword	You need either 'Change Peripheral Device Configuration' privilege or 'Administrator Privileges'.
<i>number2</i>	Enter an integer number from 0 - 24.	An "active" actuator is turned ON, or, if with a door handle connected, is OPENED.
<i>muteOtherDoorHandle</i>	Keyword	
<i>enable / disable</i>	Enter one of these values	

► **Examples:**

```
config:# peripheralDevicesSetup
externalSensorsZCoordinateFormat freeForm
deviceAltitude 3
peripheralDeviceAutoManagement enable
activePoweredDryContactLimit 2
muteOtherDoorHandle disable
```

## Asset Management Commands

You can use the CLI commands to change the settings of the connected asset strip (if any) or the settings of LEDs on the asset strip.

## Asset Strip Management

An asset strip management configuration command begins with `assetStrip`.

## Rack Unit Configuration (Tag Ports)

A rack unit refers to a tag port on the asset strips. A rack unit configuration command begins with `rackUnit`.

## Example - Asset Management

This section illustrates several asset management examples.

### ► *Example 1 - Asset Strip 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"
```

## Serial Port Configuration Commands

A serial port configuration command begins with `serial`.

### Setting the Baud Rates

The following commands set the baud rate (bps) of the serial port labeled CONSOLE / MODEM on the BCM2 device. Change the baud rate before connecting it to the desired device, such as a computer, a Raritan's P2CIM-SER, or a modem, through the serial port, or there are communications errors. If you change the baud rate dynamically after the connection has been made, you must reset the BCM2 or power cycle the connected device for proper communications.

### ► *Determine the CONSOLE baud rate:*

```
config:#  serial consoleBaudRate <baud_rate>
```

---

Note: The serial port bit-rate change is required when the BCM2 works in conjunction with Raritan's Dominion LX KVM switch. Dominion LX only supports 19200 bps for communications over the serial interface.

---

► **Determine the MODEM baud rate:**

```
config:#    serial modemBaudRate <baud_rate>
```

*Variables:*

- <baud\_rate> is one of the baud rate options: *1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.*

## Forcing the Device Detection Mode

This command forces the serial port on the BCM2 to enter a specific device detection mode.

```
config:#    serial deviceDetectionType <mode>
```

*Variables:*

- <mode> is one of the detection modes: *automatic, forceConsole, forceAnalogModem, or forceGsmModem.*

Option	Description
automatic	The BCM2 automatically detects the type of the device connected to the serial port. Select this option unless your BCM2 cannot correctly detect the device type.
forceConsole	The BCM2 attempts to recognize that the connected device is set for the console mode.
forceAnalogModem	The BCM2 attempts to recognize that the connected device is an analog modem.
forceGsmModem	The BCM2 attempts to recognize that the connected device is a GSM modem.

## Example - Baud Rate

The following command sets the CONSOLE baud rate of the BCM2 device's serial port to 9600 bps.

```
config:#    serial consoleBaudRate 9600
```

## Actuator Control Operations

An actuator, which is connected to a dry contact signal channel of a sensor package, 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.

### Switching On an Actuator

This command syntax turns on one actuator.

```
# control actuator <n> on
```

To quicken the operation, you can add the parameter `"/y"` to the end of the command, which confirms the operation.

```
# control actuator <n> on /y
```

#### *Variables:*

- `<n>` is an actuator's ID number.  
The ID number is available in the BCM2 web interface or using the show command in the CLI. It is an integer starting at 1.

If you entered the command without `"/y"`, a message appears, prompting you to confirm the operation. Then:

- Type `y` to confirm the operation, OR
- Type `n` to abort the operation

### Switching Off an Actuator

This command syntax turns off one actuator.

```
# control actuator <n> off
```

To quicken the operation, you can add the parameter `"/y"` to the end of the command, which confirms the operation.

```
# control actuator <n> off /y
```

#### *Variables:*

- `<n>` is an actuator's ID number.

The ID number is available in the BCM2 web interface or using the show command in the CLI. It is an integer starting at 1.

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, you can unblock them at the local console.

### ► *To unblock a user:*

1. Access the CLI interface using any terminal program via a local connection.
2. When the Username prompt appears, type `unlock` and press Enter.

**Username: unlock**

3. When the "Username to unblock" prompt appears, type the name of the blocked user and press Enter.

**Username to unblock:**

4. A message appears, indicating that the specified user was unblocked successfully.

## Resetting the BCM2

You can reset the BCM2 to factory defaults or simply restart it using the CLI commands.

## Restarting the BCM2

This command restarts the BCM2. It is not a factory default reset.

### ► *To restart the BCM2:*

1. Ensure you have entered administrator mode and the `#` prompt is displayed.
2. Type either of the following commands to restart the BCM2.

```
# 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 reset is complete.

---

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

---

## Resetting to Factory Defaults

The following commands restore all settings of the BCM2 to factory defaults.

- ▶ To reset BCM2 settings after login, use either command:

```
# reset factorydefaults
```

-- OR --

```
# reset factorydefaults /y
```

- ▶ To reset BCM2 settings before login:

```
Username: factorydefaults
```

See Using the CLI Command for details.

---

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

---

## Network Troubleshooting in Diagnostic Mode

The BCM2 provides 4 diagnostic commands for troubleshooting network problems: *nslookup*, *netstat*, *ping*, and *traceroute*. The diagnostic commands function as corresponding Linux commands and can get corresponding Linux outputs.

The diagnostic command syntax varies from command to command.

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.

- ▶ To quit the diagnostic mode:

```
diag> exit
```

The # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode.

## Querying DNS Servers

This command syntax queries Internet domain name server (DNS) information of a network host.

```
diag> nslookup <host>
```

*Variables:*

- <host> is the name or IP address of the host whose DNS information you want to query.

## Showing Network Connections

This command syntax displays network connections and/or status of ports.

```
diag> netstat <option>
```

*Variables:*

- <option> is one of the options: *ports* or *connections*.

Option	Description
ports	Shows TCP/UDP ports.
connections	Shows network connections.

## Testing the Network Connectivity

This ping command sends the ICMP ECHO\_REQUEST message to a network host for checking its network connectivity. If the output shows the host is responding properly, the network connectivity is good. If not, either the host is shut down or it is not being properly connected to the network.

```
diag> ping <host>
```

*Variables:*

- <host> is the host name or IP address whose networking connectivity you want to check.

*Options:*

- You can include any or all of additional options listed below in the ping command.

Options	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number between 1 and 100.
size <number2>	Determines the packet size. <number2> is an integer number in bytes between 1 and 65468.

Options	Description
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds ranging from 1 to 600.

The command looks like the following when it includes all options:

```
diag> ping <host> count <number1> size <number2> timeout <number3>
```

## Tracing the Route

This command syntax traces the network route between your BCM2 and a network host.

```
diag> traceroute <host> <useICMP> <timeout>
```

*Variables:*

- <host> is the name or IP address of the host you want to trace.
- <useICMP> is optional. It has only one value -- useICMP. Type useICMP in the end of this command only when you want to use ICMP packets rather than UDP packets.
- <timeout> is the maximum amount of time (in seconds) until traceroute will be terminated (1..900).

## 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. You can also use ipv6 address to check the connectivity.

```
diag> ping 192.168.84.222 count 5

ping fd07:a47c:0000:823e:3b02:0000:982b:0463
count 5
```

## Appendices

## Equipment Setup Worksheet Sample

► BCM2 Model \_\_\_\_\_

► BCM2 Serial Number \_\_\_\_\_

OUTLET 1	OUTLET 2	OUTLET 3
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 4	OUTLET 5	OUTLET 6
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 7	OUTLET 8	OUTLET 9
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 10	OUTLET 11	OUTLET 12
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 13	OUTLET 14	OUTLET 15
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 16	OUTLET 17	OUTLET 18
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 19	OUTLET 20	OUTLET 21
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 22	OUTLET 23	OUTLET 24
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

► *Types of adapters*

---

▶ *Types of cables*

---

▶ *Name of software program*

---



## Special Configuration and Upgrade Methods

### In This Chapter

Configuration or Firmware Upgrade with a USB Drive. . . . .	417
Bulk Configuration or Firmware Upgrade via DHCP (TFTP/HTTPS). . . . .	429
Raw Configuration Upload and Download. . . . .	446
Bulk Configuration, Firmware Upgrade, or Backup/Restore via SCP. . . . .	451

### Configuration or Firmware Upgrade with a USB Drive

You can accomplish the following tasks simultaneously by plugging a USB flash drive which contains special configuration files into the device.

- Configuration changes
- Firmware upgrade
- Diagnostic data download

### Device Configuration/Upgrade Procedure

---

---

Firmware downgrade is NOT supported by default. Contact Technical Support.

---

---

You can use one USB drive to configure or upgrade multiple devices one by one as long as it contains valid configuration files.

► *To use a USB drive to configure or upgrade firmware:*

1. Check requirements. [System and USB Requirements](#) (on page 418).
2. Prepare required configuration files. See [Configuration Files](#) (on page 418).
3. Copy required configuration files to the root directory of the USB drive.
  - For firmware upgrade, an appropriate firmware binary file is also required.
4. Plug the USB drive into the USB-A port of the device.
5. The initial message shown on the front panel display depends on the first task performed.
  - If the USB contains a firmware upgrade, that task happens first. The front panel display shows an upgrade message. When the firmware upgrade completes successfully, then a happy smiley appears.
  - If no firmware upgrade task will be performed, a happy smiley is displayed after around 30 seconds.



6. If nothing is shown on the display and no task is performed after plugging the USB drive, check the log file in the USB drive.
7. After the happy smiley appears, press one of the control buttons next to the display for one second until the smiley disappears. Wait for several seconds until the device resumes normal operation, indicated by the normal message of the display.

---

Tip: Once the happy smiley displays, you can safely remove the USB drive and move it to the next device you are working on.

---

## System and USB Requirements

You must satisfy ALL of the following requirements prior to using a USB flash drive to perform device configuration and/or firmware upgrade.

► *System requirements:*

- There is at least one USB-A port available on your Xerus device.
- Your Xerus device must run firmware version 2.2.13 or later.

► *USB drive requirements:*

- The drive contains either a single partition formatted as a Windows FAT32 filesystem, or NO partition tables (that is, a superfloppy-formatted drive).

## Configuration Files

There are three types of configuration files. To generate these files, use the Mass Deployment Utility. See [Creating Configuration Files via Mass Deployment Utility](#) (on page 426).

- `fwupdate.cfg`:  
This file MUST always be present for performing configuration or firmware upgrade tasks. See [fwupdate.cfg](#) (on page 418).
- `config.txt`:  
This file is used for configuring device settings. See [config.txt](#) (on page 422).
- `devices.csv`:  
This file is required only when there are device-specific settings to configure for multiple devices. See [devices.csv](#) (on page 424).

### `fwupdate.cfg`

The configuration file, *fwupdate.cfg*, is an ASCII text file containing key-value pairs, one per line.

Each value in the file must be separated by an equal sign (=), without any surrounding spaces. Keys are not case sensitive.

**Illustration:**

```
user=admin
password=adm
set_password=newpassword
logfile=log.txt
config=config.txt
device_list=devices.csv
```

This section explains common options in the file.

► *user*

- A required option.
- Specify the name of a user account with Administrator Privileges.

► *password*

- A required option.
- Specify the password of the specified admin user.

---

**Tip: You can add multiple user credentials to fwupdate.cfg. Each 'user' line must be immediately followed by its 'password' line. Each user will be authenticated until one of them succeeds, or until all user credentials fail.**

---

► *set\_password*

- You are required to change the default password for all units. Access to units with factory default password settings will be denied unless this option is used.
- Changes the password of the given user before executing any commands.

► *logfile*

- Specify the name of a text file where the where log messages will be saved when interpreting the USB drive contents.
- If the specified file does not exist in the USB drive, it will be automatically created.
- If this option is not set, no log messages are recorded, and there will be no feedback if there is a problem with the USB drive contents.

▶ *firmware*

- Specify the name of a firmware file.
- The specified firmware file must be compatible with your device.
- The default is to NOT permit any firmware downgrade . To do this, the parameter "allow\_downgrade" must be present and properly set in the *fwupdate.cfg* file.

▶ *config*

- Specify the name of the configuration file containing device settings.
- The default filename is *config.txt*.

▶ *device\_list*

- Specify the name of the configuration file listing all devices to configure and their device-specific settings.
- This file is required if any macros are used in the device configuration file "config.txt."
- The default filename is *devices.csv*.

▶ *match*

- Specify a match condition for identifying a device in the device configuration file "devices.csv." The option's value comprises one word and one number as explained below:
  - The word prior to the colon is an identification property, which is either `serial` for serial number or `mac` for MAC address.
  - The number following the colon indicates a column in the *devices.csv* file.For example, `mac:7` will search for the MAC address in the 7th column of the "devices.csv" file.
- The default value is `serial:1`, to search for its serial number in the first column.
- This option is used only if the "device\_list" option has been set.

▶ *factory\_reset*

- If this option is set to `true`, the device will be reset to factory defaults.
- If the device configuration will be updated at the same time, the factory reset will be executed before updating the device configuration.

▶ *bulk\_config\_restore*

- Specify the name of the bulk configuration file used to configure or restore.

---

Note: See [Bulk Configuration or Firmware Upgrade via DHCP \(TFTP/HTTPS\)](#) (on page 429) for instructions on generating a bulk configuration file.

---

- Additional configuration keys set via the *config.txt* file will be applied after performing the bulk restore operation.
- This option CANNOT be used with the option "full\_config\_restore."
- If a firmware upgrade will be performed at the same time, you must generate the bulk configuration file based on the NEW firmware version instead of the current firmware version.

► *full\_config\_restore*

- Specify the name of the full configuration backup file used to restore the device.
- Additional configuration keys set via the *config.txt* file will be applied after performing the configuration restore operation.
- This option CANNOT be used with the option "bulk\_config\_restore."
- If a firmware upgrade will be performed at the same time, you must generate the full configuration backup file based on the NEW firmware version instead of the current firmware version.

► *collect\_diag*

- If this option is set to `true`, the diagnostic data is transmitted to the USB drive.
- The filename of the diagnostic data written into the USB drive is:  
*diag\_<unit-serial>.zip*
- The device beeps after it finishes writing the diagnostic data to the USB drive.

► *switch\_outlets*

- This feature works on outlet-switching capable models only.
- Switch on or off specific outlets.
- The option's value comprises outlet numbers and the setting "on" or "off" as explained below:
  - Each "on" or "off" setting consists of three parts: outlet numbers, a colon, and the word "on" or "off".
  - Each "on" or "off" setting is separated with a semicolon.
  - If all outlets will share the same "on" or "off" setting, replace the outlet numbers with the word "all".
- Examples:
  - Turn on outlets 1 to 3, and 10, and turn off outlets 4 to 9.  
`switch_outlets=1,2,3:on;4-9:off;10:on`
  - Turn on all outlets.

```
switch_outlets=all:on
```

► *tls\_cert\_file*

- Specify the filename of the wanted TLS server certificate. The filename can contain a single placeholder `{SERIAL}` that is replaced with the serial number of the device.
- This option should be used with `tls_key_file` listed below.
- *This option is NOT supported by bulk configuration or backup/restore via DHCP/TFTP.*

► *tls\_key\_file*

- Specify the filename of the wanted TLS server key. The filename can contain a single placeholder `{SERIAL}` that is replaced with the serial number of the device.
- This option should be used with `tls_cert_file` listed above.
- *This option is NOT supported by bulk configuration or backup/restore via DHCP/TFTP.*

► *execute\_lua\_script*

- Specify a Lua script file. For example:  
`execute_lua_script=my_script.lua`
- Script output will be recorded to a log file -- `<BASENAME_OF_SCRIPT>.<SERIAL_NUMBER>.log`. Note this log file's size is limited on DHCP/TFTP.
- A DHCP/TFTP-located script has a timeout of 60 seconds. After that duration the script will be removed.
- This feature can be used to manage LuaService, such as upload, start, get output, and so on.
- If you unplug the USB drive while the Lua script is still running, the script will be removed.
- An exit handler can be used but the execution time is limited to three seconds. Note that this is not implemented on DHCP/TFTP yet.

## config.txt

To perform device configuration using a USB drive, you must:

- Copy the device configuration file "config.txt" to the root directory of the USB drive.
- Reference the "config.txt" file in the *config* option of the "fwupdate.cfg" file.

The file, *config.txt*, is a text file containing a number of configuration keys and values to configure or update.

This section only introduces the device configuration file in brief, and does not document all configuration keys, which vary according to the firmware version and your model.

You can use the Mass Deployment Utility to create this file by yourself, or contact Technical Support to get a device configuration file specific to your model and firmware version.

---

Tip: You can choose to encrypt important data in the "config.txt" file so that people cannot easily recognize it, such as the SNMP write community string. See [Data Encryption in 'config.txt'](#) (on page 427).

---

---

If you are using a password as auth/priv passphrases, you must set the password in the config file to ensure it generates the SNMPv3 hash.

---

► *Regular configuration key syntax:*

- Each configuration key and value pair is in a single line as shown below:

```
key=value
```

---

*Note: Each value in the file must be separated by an equal sign (=), without any surrounding spaces.*

---

- Multi-line values are supported by using the *Here Document Syntax* with a user-chosen delimiter. The following illustration declares a value in two lines. You can replace the delimiter `EOF` with other delimiter strings.

```
key<<EOF
value line 1
value line 2
EOF
```

---

*Note: The line break before the closing EOF is not part of the value. If a line break is required in the value, insert an additional empty line before the closing EOF.*

---

► *Special configuration keys:*

There are 3 special configuration keys that are prefixed with `magic:`.

- A special key that sets a user account's password without knowing the firmware's internal encryption/hashing algorithms is implemented.

Example:

```
magic:users[1].cleartext_password=joshua
```

- Two special keys that set the SNMPv3 passphrases without knowing the firmware's internal encryption/hashing algorithms are implemented.

Examples:

```
magic:users[1].snmp_v3.auth_phrase=swordfish
magic:users[1].snmp_v3.priv_phrase=opensesame
```

► *To configure device-specific settings:*

1. Make sure the device list configuration file "devices.csv" is available in the USB drive.
2. In the "config.txt" file, refer each device-specific configuration key to a specific column in the "devices.csv" file. The syntax is: `${column}`, where "column" is a column number.

Examples:

```
net.interfaces[eth0].ipv4.static.addr_cidr.addr=${4}
```

```
pdu.name=${16}
```

► *To rename the admin user:*

You can rename the admin user by adding the following configuration key:

```
users[0].name=new admin name
```

Example:

```
users[0].name=May
```

► *To restore a specific setting to factory default:*

Add "delete:" to the beginning of the key whose setting you want to remove. The custom setting will be removed and then reset to factory default.

Example:

```
delete:net.port_forwarding
```

### devices.csv

If there are device-specific settings to configure, you must create a device list configuration file - *devices.csv*, to store unique data of each device.

This file must be:

- A CSV (comma-separated values) format file exported from a spreadsheet application like Excel.
- Copied to the root directory of USB drive.
- Referenced in the *device\_list* option of the "fwupdate.cfg" file. See [fwupdate.cfg](#) (on page 418).

Every device identifies its entry in the "devices.csv" file by comparing its serial number or MAC address to one of the columns in the file.

► *Determine the column to identify devices:*

- By default, each device searches for its serial number in the 1st column of "devices.csv".
- To override the default, set the *match* option in the "fwupdate.cfg" file to a different column.

► *Syntax:*

- Values containing commas, line breaks or double quotes are all supported.
- The commas and line breaks to be included in the values must be enclosed in double quotes.
- Every double quote to be included in the value must be escaped with another double quote.

For example:

```
Value-1, "Value-2, with, three, commas", Value-3
```

```
Value-1, "Value-2, ""with""three""double-quotes", Value-3
```

```
Value-1, "Value-2
```



with a line break", Value-3

## Configuration Files for Linking

When Linking is enabled multiple versions of config.txt are required:

- config\_link\_unit.txt containing the configuration for all link units
- config\_<serial>.txt for each primary unit containing its specific settings, including a list of link units.

### ► *Commands for device Linking:*

The following commands are used in the fwupdate.cfg file to configure Linking.

### ► *add\_link\_unit*

Add a new link unit. The option can be specified more than once to add multiple link units.

```
add_link_unit=<id>,<host>,<login>:<password>
```

- Parameters are: <id>: new link unit id (2..8), <host>: hostname or IP address, <login>:<password>: credentials for admin user

### ► *add\_link\_unit\_new\_password:*

Change the password when adding a new link unit. Required in case the link unit still uses the factory default password.

```
add_link_unit_new_password=<id>,<new_password>
```

### ► *add\_cascade\_link\_units*

Add port-forwarding expansion units as link units. The option can be specified more than once to link multiple port-forwarding nodes with different parameters.

```
add_cascade_link_units=<link ids>:<nodes>:<position dependent>:<login>:<password>
```

Parameters are:

<link ids>: comma-separated list of new link unit ids (2..8)

<nodes>: comma-separated list of port-forwarding node indices (1..31, needs to be same length as <link ids>), or the special word "all", which will link all port-forwarding nodes until an error occurs.

<position dependent>: "true" or "false": if true, use position-dependent host-names (i.e. expansion-<n>.pf-cascade) or, if false, use link-local IPv6 addresses.

<login>:<password>: credentials for admin user on the port-forwarding node

- Example: `add_cascade_link_units=2,3:1,2:false:admin:<password>`

## Configuration Files for Linking: Port-Forwarding Cascade Example

In this example, you can configure a port-forwarding cascade containing a Primary PDU and supported Expansion Units. Complete physical, wired setup first, then use the USB drive method with a `fwupdate.cfg` file as described here.

- Prerequisite: Wired setup with primary units and connected expansion units
1. Prepare a USB drive with a `fwupdate.cfg` file with the following included details  
`port_forwarding_auto_setup=[downstreamInterface:<INTERFACE-LABEL>,<number of expansion units>],admin:<password>`
  2. Attach the USB drive to the primary units to automatically setup the port-forwarding cascade and linking.

## Creating Configuration Files via Mass Deployment Utility

The Mass Deployment Utility is an Excel file that lets you fill in basic information required for the three configuration files, such as the admin account and password.

After entering required information, you can generate all configuration files with only one click, including `fwupdate.cfg`, `config.txt` and `devices.csv`.

---

Note: The firmware version of your device must match the version of the Mass Deployment Utility spreadsheet. Do not mix versions.

---

New commands that have been introduced in later versions of the spreadsheet will not be effective on devices with older firmware.

---

### ► To use the Mass Deployment Utility:

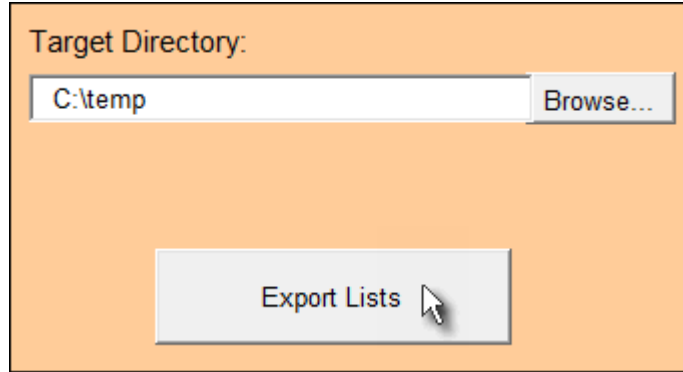
1. Download the Mass Deployment Utility from the support page.
  - The utility is named `mass_deployment-xxx` (where xxx is the firmware version number).
2. Launch Excel to open this utility.

---

Note: Other programs, such as OpenOffice and LibreOffice, are not supported.

---

3. Read the instructions in the 1st worksheet of the utility, and make sure Microsoft Excel's security level has been set to Medium or the equivalent for executing unsigned macros of this utility.
4. Enter information in the 2nd and 3rd worksheets.
  - The 2nd worksheet contains information required for `fwupdate.cfg` and `config.txt`.
  - The 3rd worksheet contains device-specific information for `devices.csv`.
5. Return to the 2nd worksheet to execute the export macro.
  - a. In the Target Directory field, specify the folder where to generate the configuration files. For example, you can specify the root directory of a connected USB drive.
  - b. Click Export Lists to generate configuration files.



Verify that at least 3 configuration files are created - *fwupdate.cfg*, *config.txt* and *devices.csv*. You are ready to configure or upgrade with these files.

### Data Encryption in 'config.txt'

When intending to prevent people from identifying the values of any settings, you can encrypt them. Encrypted data still can be properly interpreted and performed by any device running Xerus firmware version 3.2.20 or later.

#### ► *Data encryption procedure:*

1. Open the "config.txt" file to determine which setting(s) to encrypt.
2. Launch a terminal to log in to the CLI of the device.
3. Type the encryption command and the value of the setting you want to encrypt.
  - The value *cannot* contain any double quotes (") or backslashes (\).
  - If the value contains spaces, it must be enclosed in double quotes.

```
# config encrypt <value>
```

-- OR --

```
# config encrypt "<value with spaces>"
```

4. Press Enter. The CLI generates and displays the encrypted form of the typed value.
5. Go to the "config.txt" file and replace the chosen value with the encrypted one by typing or copying the encrypted value from the CLI.
6. Add the text "encrypted:" to the beginning of the encrypted setting.
7. Repeat steps for additional settings you intend to encrypt.
8. Save the changes made to the "config.txt" file. Now you can use this file to configure other devices.

#### ► *Illustration:*

In this example, we will encrypt the word "private", which is the value of the SNMP write community in the "config.txt" file.

```
snmp.write_community=private
```

1. In the CLI, type the following command to encrypt "private."

```
# config encrypt private
```

2. The CLI generates and shows the encrypted form of "private."

```
ZTtnYcvQUw==
```

3. In the "config.txt" file, make the following changes to the SNMP write community setting.
  - a. Replace the word "private" with the encrypted value that CLI shows.

```
snmp.write_community=ZTtnYcvQUw==
```

- b. Add "encrypted:" to the beginning of that setting.

```
encrypted:snmp.write_community=ZTtnYcvQUw==
```

## Firmware Upgrade via USB

Firmware files are available on the product support page.

Note that if the firmware file used for firmware upgrade is the same as the firmware version running on the BCM2, no firmware upgrade will be performed unless you have set the *force\_update* option to true in the "fwupdate.cfg" file.

### ► To use a USB drive to upgrade the BCM2:

1. Copy the configuration file "fwupdate.cfg" and an appropriate firmware file to the root directory of the USB drive.
2. Reference the firmware file in the *firmware* option of the "fwupdate.cfg" file.
3. Plug the USB drive into the USB-A port on the BCM2.
4. The front panel display shows the firmware upgrade progress.

---

*Tip: You can remove the USB drive and plug it into another unit for firmware upgrade when the firmware upgrade message displays.*

---

5. It may take one to five minutes to complete the firmware upgrade, depending on your product.
6. When the firmware upgrade finishes, the front panel display indicates the firmware upgrade result.
  - Happy smiley: Successful.



- Sad smiley: Failed. Check the log file in the USB drive or contact Technical Support to look into the failure cause.



---

Note: If your unit does not have a front panel display, you should wait for few minutes, remove the USB drive, and reboot the unit.

---

1. Remove USB drive and push any front panel button to continue.

## Bulk Configuration or Firmware Upgrade via DHCP (TFTP/HTTPS)

If a TFTP or HTTPS server is available, you can use it and appropriate configuration files to perform any or all of the following tasks for a large number of devices in the same network.

- Initial deployment
- Configuration changes
- Firmware upgrade
- Downloading diagnostic data

This feature is useful if you have hundreds or even thousands of devices to configure or upgrade.

---

---

Warning: The feature of bulk configuration or firmware upgrade via DHCP (TFTP/HTTPS) only works on standalone devices directly connected to the network. This feature does NOT work for expansion units in a cascading configuration.

---

---

## Bulk Configuration/Upgrade Procedure

---

---

Firmware downgrade is NOT supported by default. Contact Technical Support.

---

---

► *Steps of using DHCP (TFTP/HTTPS) for bulk configuration/upgrade:*

1. Create configuration files specific to your BCM2 models and firmware versions. Create your own or contact Technical Support to properly prepare some or all of the following files:
  - *fwupdate.cfg* (always required)
  - *config.txt*
  - *devices.csv*

---

*Note: Supported syntax of "fwupdate.cfg" and "config.txt" may vary based on different firmware versions. If you have existing configuration files, it is suggested to double check with Technical Support for the correctness of these files prior to using this feature.*

---

2. Configure your TFTP or HTTPS server properly.
  3. Copy ALL required configuration files into the TFTP or HTTPS root directory. If the tasks you will perform include firmware upgrade, an appropriate firmware binary file is also required.
  4. Properly configure your DHCP server so that it refers to the file "fwupdate.cfg" on the TFTP/HTTPS server.
  5. Make sure all of the desired devices use DHCP as the IP configuration method and have been *directly* connected to the network.
  6. Reboot these devices. The DHCP server will execute the commands in the "fwupdate.cfg" file on the TFTP server to configure or upgrade those devices supporting DHCP in the same network.
- DHCP will execute the "fwupdate.cfg" commands once for IPv4 and once for IPv6 respectively if both IPv4 and IPv6 settings are configured properly in DHCP.

---

Note: If both TFTP and HTTP server options are specified, HTTP takes precedence. For HTTP, both 'http' and 'https' schemes are supported, but when using https, the certificate is not checked.

---

## TFTP/HTTPS Requirements

To perform bulk configuration or firmware upgrade successfully, your TFTP/HTTPS server must meet the following requirements:

- The server is able to work with both IPv4 and IPv6.  
In Linux, remove any IPv4 or IPv6 flags from */etc/xinetd.d/tftp*.

---

*Note: DHCP will execute the "fwupdate.cfg" commands once for IPv4 and once for IPv6 respectively if both IPv4 and IPv6 settings are configured properly in DHCP.*

---

- All required configuration files are available in the TFTP/HTTPS root directory. See *Bulk Configuration/Upgrade Procedure* (on page ).

If you are going to upload any BCM2 diagnostic file or create a log file in the TFTP server, the first of the following requirements is also required.

---

Note: The HTTPS server does not support file writes(diag data, log files etc.).

---

► *TFTP Server:*

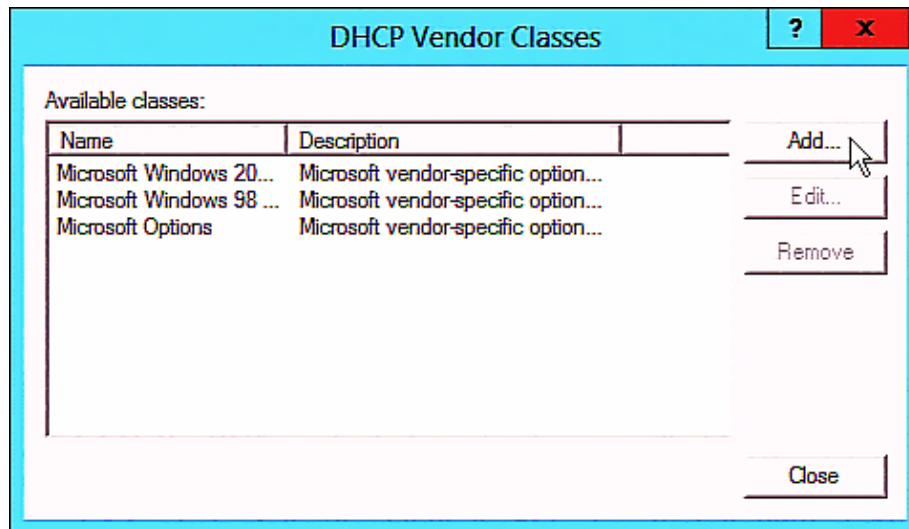
- The TFTP server supports the write operation, including file creation and upload.  
In Linux, provide the option "-c" for write support.
- Required for uploading the diagnostic file only - the timeout for file upload is set to one minute or longer.

## DHCP IPv4 Configuration in Windows

For those BCM2 devices using IPv4 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

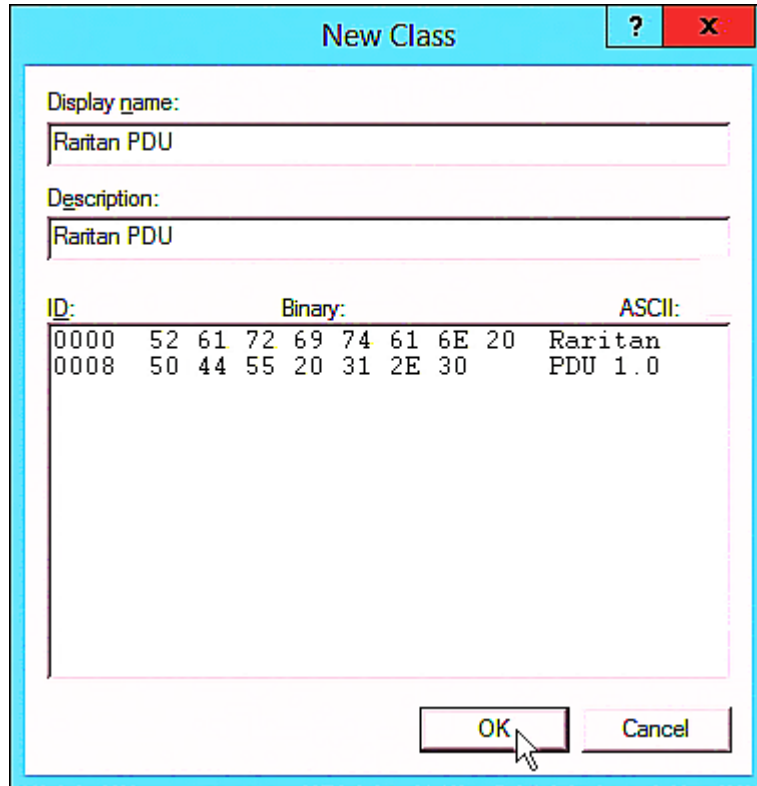
► *Required Windows IPv4 settings in DHCP:*

1. Add a new vendor class for BCM2 under IPv4.
  - a. Right-click the IPv4 node in DHCP to select Define Vendor Classes.
  - b. Click Add to add a new vendor class.



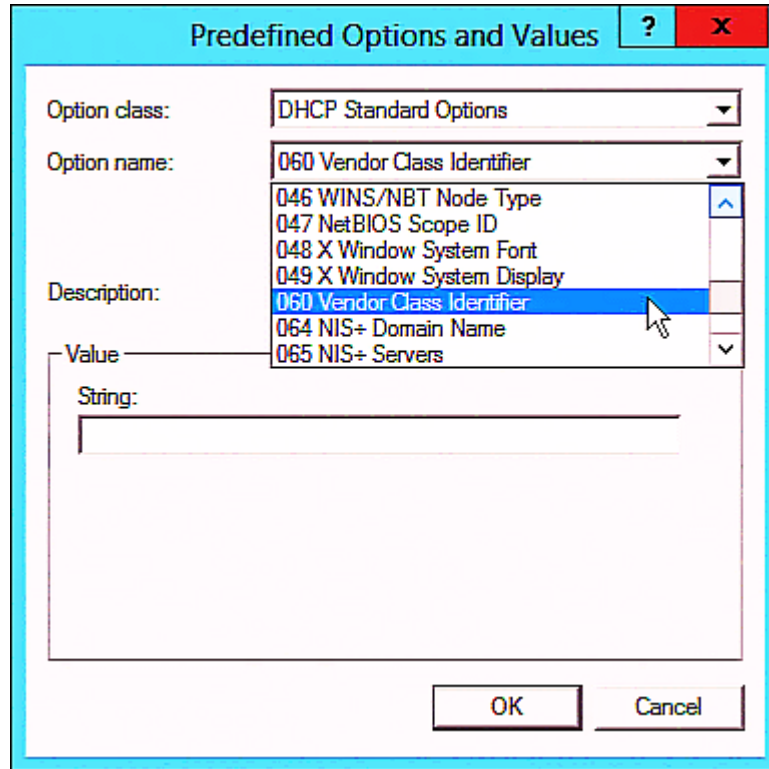
- c. Specify a unique name for this vendor class and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU" in this illustration.

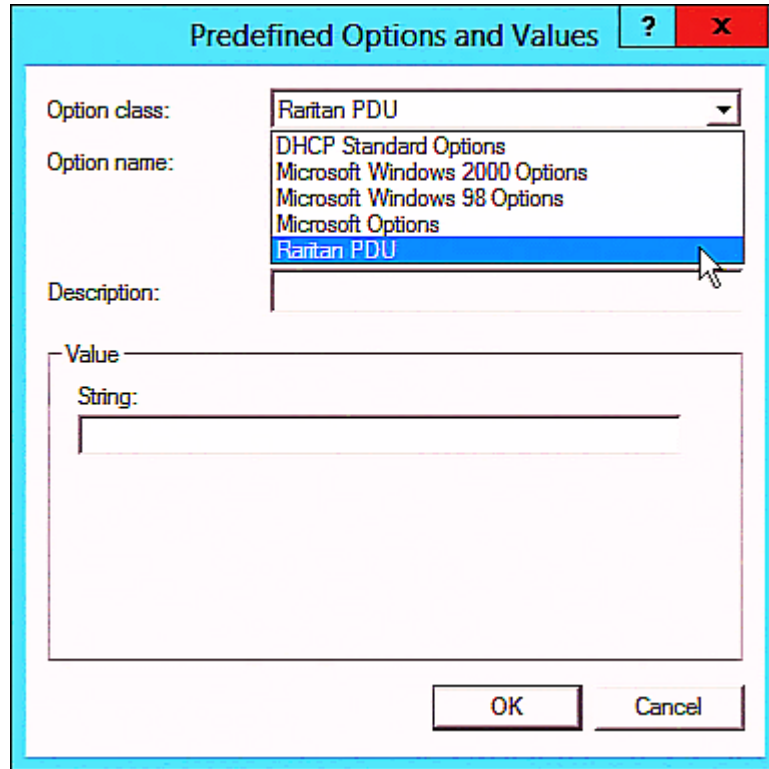


2. Define one DHCP standard option - Vendor Class Identifier.
  - a. Right-click the IPv4 node in DHCP to select Set Predefined Options.
  - b. Select DHCP Standard Options in the "Option class" field, and Vendor Class Identifier in the "Option name" field. Leave the String field blank.

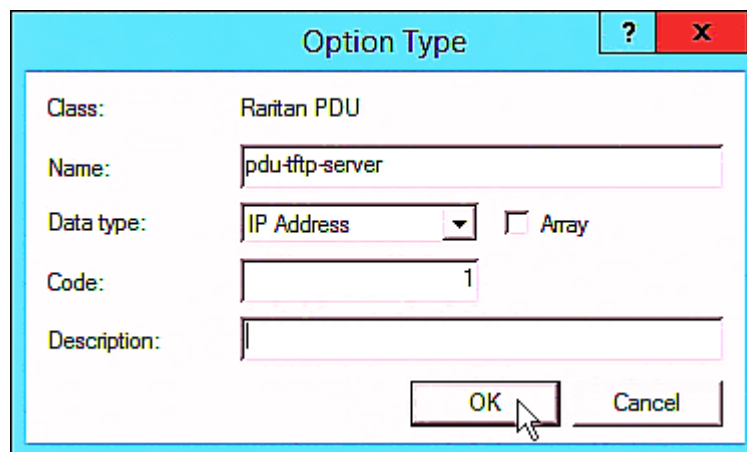




3. Add three options to the new vendor class "Raritan PDU" in the same dialog.
  - a. Select Raritan PDU in the "Option class" field.



- b. Click Add to add the first option. Type "pdu-tftp-server" or "pdu-https-server" in the Name field, select IP Address as the data type, and type 1 in the Code field for tftp server and type 7 in the Code field for https server.



- c. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.

**Option Type** [?] [X]

Class: Raritan PDU

Name: pdu-update-control-file

Data type: String  Array

Code: 2

Description:

OK Cancel

- d. Click Add to add the third one. Type "pdu-update-magic" in the Name field, select String as the data type, and type 3 in the Code field.

**Option Type** [?] [X]

Class: Raritan PDU

Name: pdu-update-magic

Data type: String  Array

Code: 3

Description:

OK Cancel

4. Create a new policy associated with the "Raritan PDU" vendor class.
  - a. Right-click the Policies node under IPv4 to select New Policy.
  - b. Specify a policy name, and click Next.  
The policy is named "PDU" in this illustration.

**DHCP Policy Configuration Wizard**

**Policy based IP Address and Option Assignment**

This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).

This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.

Policy Name:

Description:

- c. Click Add to add a new condition.
- d. Select the vendor class "Raritan PDU" in the Value field, click Add and then Ok.

**Add/Edit Condition**

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria:

Operator:

Value(s)

Value:

Prefix wildcard(\*)

Append wildcard(\*)

- e. Click Next.
- f. Select DHCP Standard Options in the "Vendor class" field, select "060 Vendor Class Identifier" from the Available Options list, and type "Raritan PDU 1.0" in the "String value" field.

**DHCP Policy Configuration Wizard**

**Configure settings for the policy**  
If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class:

Available Options	Description
<input type="checkbox"/> 049 X Window System Display	Array of X Windows Display M...
<input checked="" type="checkbox"/> 060 Vendor Class Identifier	
<input type="checkbox"/> 064 NIS+ Domain Name	The name of the client's NIS+

Data entry

String value:

- g. Select the "Raritan PDU" in the "Vendor class" field, select "001 pdu-tftp-server" or "007 pdu-https-server" from the Available Options list, and type your TFTP/https server's IPv4 address in the "IP address" field.

**DHCP Policy Configuration Wizard**

**Configure settings for the policy**  
If the conditions specified in the policy match a client request, the settings will be applied.

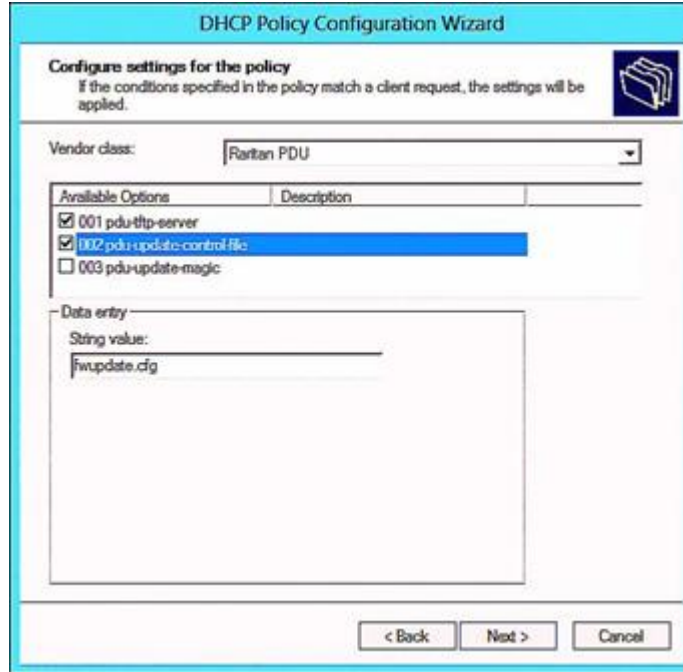
Vendor class:

Available Options	Description
<input checked="" type="checkbox"/> 001 pdu-tftp-server	
<input type="checkbox"/> 002 pdu-update-control-file	
<input type="checkbox"/> 003 pdu-update-magic	

Data entry

IP address:

- h. Select "002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.



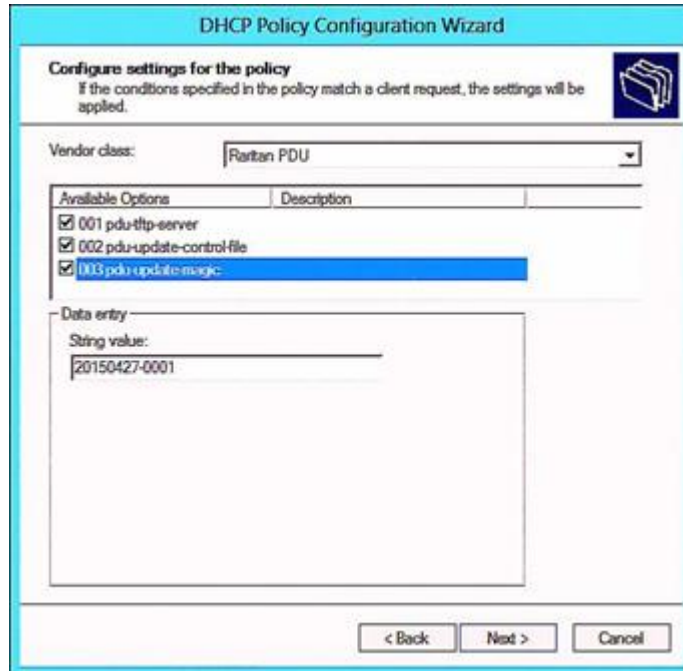
- i. Select "003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the `fwupdate.cfg` commands from being executed repeatedly. It does NOT matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

---

*Important: The magic cookie is transmitted to and stored in BCM2 at the time of executing the "fwupdate.cfg" commands. The DHCP(TFTP/HTTPS) operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in BCM2. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.*

---

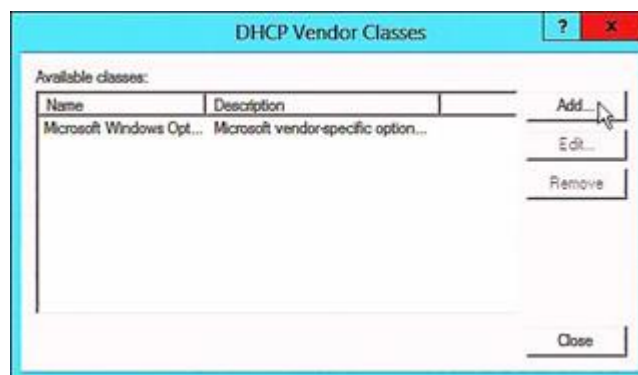


## DHCP IPv6 Configuration in Windows

For those BCM2 devices using IPv6 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

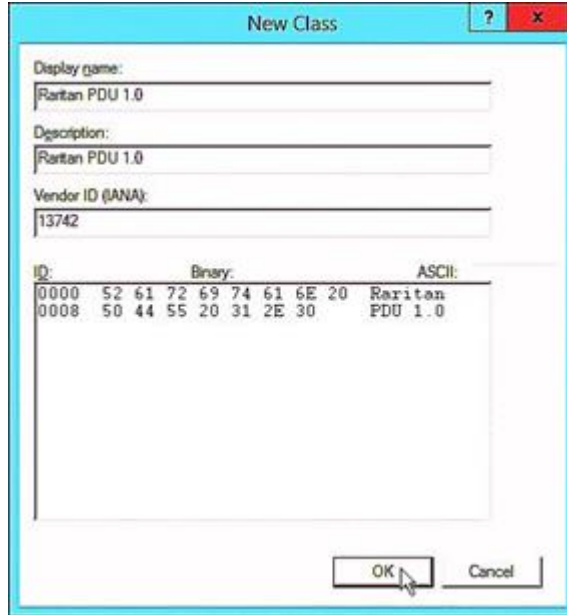
► *Required Windows IPv6 settings in DHCP:*

1. Add a new vendor class for Raritan's BCM2 under IPv6.
  - a. Right-click the IPv6 node in DHCP to select Define Vendor Classes.
  - b. Click Add to add a new vendor class.

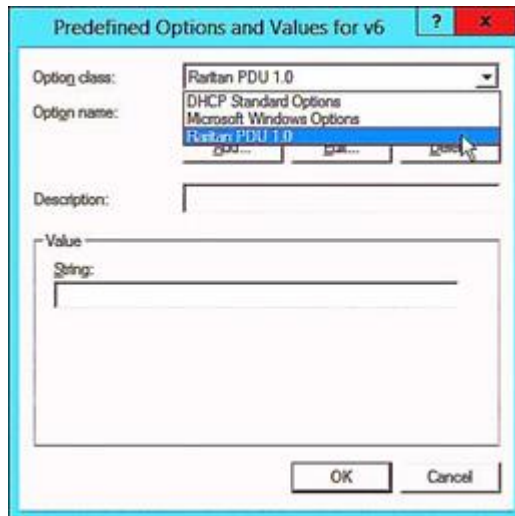


- c. Specify a unique name for the vendor class, type "13742" in the "Vendor ID (IANA)" field, and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU 1.0" in this illustration.



2. Add three options to the "Raritan PDU 1.0" vendor class.
  - a. Right-click the IPv6 node in DHCP to select Set Predefined Options.
  - b. Select Raritan PDU 1.0 in the "Option class" field.



- c. Click Add to add the first option. Type "pdu-ftp-server" or "pdu-https-server" in the Name field, select IP Address as the data type, and type 1 in the Code field and type 7 in the Code field for https server.

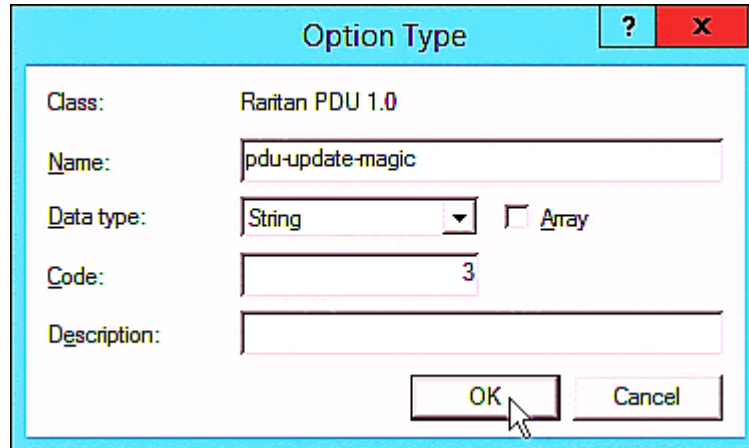


The dialog box titled "Option Type" has a blue header with a question mark and a close button. The main content area is white with a light blue border. It contains the following fields: "Class" is set to "Raritan PDU 1.0"; "Name" is "pdu-ftp-server"; "Data type" is a dropdown menu set to "IP Address" with an unchecked "Array" checkbox; "Code" is a text box containing "1"; and "Description" is an empty text box. At the bottom right are "OK" and "Cancel" buttons, with a mouse cursor pointing at the "OK" button.

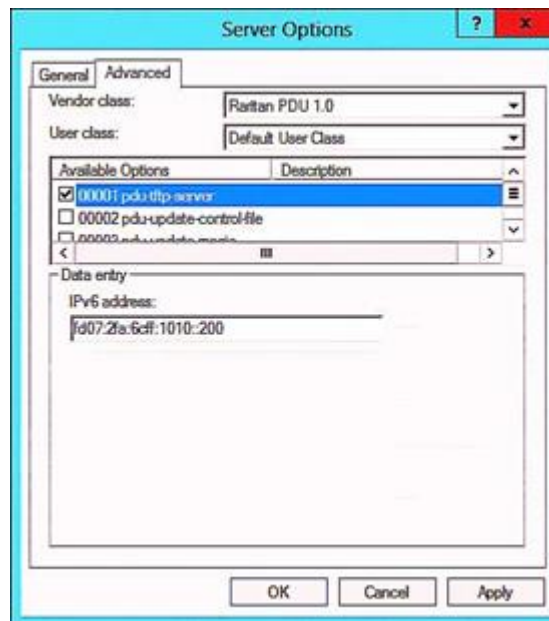
- d. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.

The dialog box titled "Option Type" has a blue header with a question mark and a close button. The main content area is white with a light blue border. It contains the following fields: "Class" is set to "Raritan PDU 1.0"; "Name" is "pdu-update-control-file"; "Data type" is a dropdown menu set to "String" with an unchecked "Array" checkbox; "Code" is a text box containing "2"; and "Description" is an empty text box. At the bottom right are "OK" and "Cancel" buttons, with a mouse cursor pointing at the "OK" button.

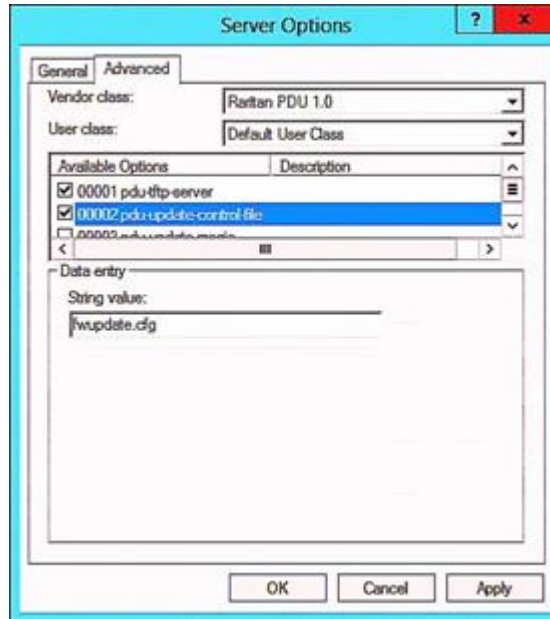
- e. Click Add to add the third one. Type "pdu-update-magic" in the Name field, select String as the data type, and type 3 in the Code field.



3. Configure server options associated with the "Raritan PDU 1.0" vendor class.
  - a. Right-click the Server Options node under IPv6 to select Configure Options.
  - b. Click the Advanced tab.
  - c. Select "Raritan PDU 1.0" in the "Vendor class" field, select "00001 pdu-tftp-server" or "00007 pdu-https-server" from the Available Options list, and type your TFTP/HTTPS server's IPv6 address in the "IPv6 address" field.



- d. Select "00002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.



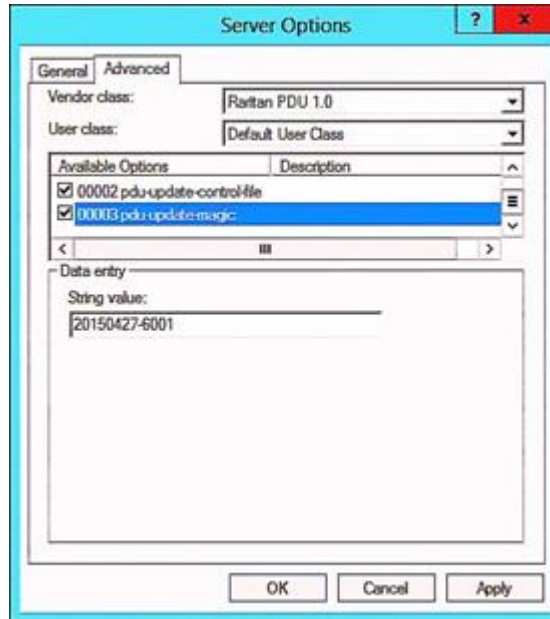
- e. Select "00003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the `fwupdate.cfg` commands from being executed repeatedly. It does NOT matter whether the IPv6 magic cookie is identical to or different from the IPv4 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

---

*Important: The magic cookie is transmitted to and stored in BCM2 at the time of executing the "fwupdate.cfg" commands. The DHCP(TFTP/HTTPS) operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in BCM2. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.*

---



## DHCP IPv4 Configuration in Linux

Modify the "dhcpd.conf" file for IPv4 settings when your DHCP server is running Linux.

### ► Required Linux IPv4 settings in DHCP:

1. Locate and open the "dhcpd.conf" file of the DHCP server.
2. The BCM2 will provide the following value of the vendor-class-identifier option (option 60).
  - vendor-class-identifier = "Raritan PDU 1.0"

Configure the same option in DHCP accordingly. The BCM2 accepts the configuration or firmware upgrade only when this value in DHCP matches.

3. Set the following three sub-options in the "vendor-encapsulated-options" (option 43).
  - code 1 (pdu-tftp-server) = the TFTP server's IPv4 address or
  - code 7 (pdu-https-server) = the HTTPS server's IPv4 address
  - code 2 (pdu-update-control-file) = the name of the control file "fwupdate.cfg"
  - code 3 (pdu-update-magic) = any string

This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

---

*Important: The magic cookie is transmitted to and stored in BCM2 at the time of executing the "fwupdate.cfg" commands. The DHCP(TFTP/HTTPS) operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in BCM2. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.*

---

► IPv4 illustration example in *dhcpd.conf*:

```
[...]  
  
set vendor-string = option vendor-class-identifier;  
option space RARITAN code width 1 length width 1 hash size 3;  
option RARITAN.pdu-tftp-server code 1 = ip-address;  
option RARITAN.pdu-update-control-file code 2 = text;  
option RARITAN.pdu-update-magic code 3 = text;  
option RARITAN.pdu-model code 4 = text;  
option RARITAN.pdu-serial code 5 = text;  
option RARITAN.pdu-cascading-info code 6 = text;  
option RARITAN.pdu-http-uri-base code 7 = text;  
  
option local-encapsulation code 43 = encapsulate RARITAN;  
  
class "raritan" {  
    match if option vendor-class-identifier = "Raritan PDU 1.0";  
    vendor-option-space RARITAN;  
    option RARITAN.pdu-tftp-server 192.168.1.7;  
    option RARITAN.pdu-http-uri-base "https://192.168.1.100/update";  
    option RARITAN.pdu-updateupdate-control-file "fwupdate.cfg";  
    option RARITAN.pdu-update-magic "20150123-0001";  
    option vendor-class-identifier "Raritan PDU 1.0";  
  
    # optional logging of the parameters sent by the PDU  
    log(info, concat("PDU model: ", option RARITAN.pdu-model));  
    log(info, concat("PDU serial: ", option RARITAN.pdu-serial));  
    log(info, concat("PDU cascading info: ", option RARITAN.pdu-cascading-info));  
}  
  
[...]
```

## DHCP IPv6 Configuration in Linux

Modify the "dhcpd6.conf" file for IPv6 settings when your DHCP server is running Linux.

► *Required Linux IPv6 settings in DHCP:*

1. Locate and open the "dhcpd6.conf" file of the DHCP server.
2. The BCM2 will provide the following values to the "vendor-class" option (option 16). Configure related settings in DHCP accordingly.
  - 13742 (Raritan's IANA number)
  - Raritan PDU 1.0
  - 15 (the length of the above string "Raritan PDU 1.0")
3. Set the following three sub-options in the "vendor-opts" (option 17).
  - code 1 (pdu-tftp-server) = the TFTP server's IPv6 address or
  - code 7 (pdu-https-server) = the HTTPs server's IPv6 address
  - code 2 (pdu-update-control-file) = the name of the control file "fwupdate.cfg"
  - code 3 (pdu-update-magic) = any string

This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv6 magic cookie is identical to or different from the IPv4 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

---

*Important: The magic cookie is transmitted to and stored in BCM2 at the time of executing the "fwupdate.cfg" commands. The DHCP(TFTP/HTTPS) operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in BCM2. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.*

---

► IPv6 illustration example in dhcpd6.conf:

```
[...]  
  
option space RARITAN code width 2 length width 2 hash size 3;  
option RARITAN.pdu-tftp-server code 1 = ip6-address;  
option RARITAN.pdu-update-control-file code 2 = text;  
option RARITAN.pdu-update-magic code 3 = text;  
option RARITAN.pdu-model code 4 = text;  
option RARITAN.pdu-serial code 5 = text;  
option RARITAN.pdu-cascading-info code 6 = text;  
option RARITAN.pdu-http-uri-base code 7 = text;  
option vsio.RARITAN code 13742 = encapsulate RARITAN;  
  
[...]  
  
# optional logging of the parameters sent by the PDU  
log(info, concat("PDU model: ", option RARITAN.pdu-model));  
log(info, concat("PDU serial: ", option RARITAN.pdu-serial));  
log(info, concat("PDU cascading info: ", option RARITAN.pdu-cascading-info));  
  
subnet6 xxxx {  
  
[...]  
    option RARITAN.pdu-tftp-server 1::2;  
    option RARITAN.pdu-http-uri-base "https://192.168.1.100/update";  
    option RARITAN.pdu-update-control-file "fwupdate.cfg";  
    option RARITAN.pdu-update-magic "20150123-0001";  
[...]  
}
```

## Raw Configuration Upload and Download

You can modify any existing "config.txt", and then upload it to a specific device for modifying part or all of its settings. Both configuration download and upload operations require the Administrator Privileges.

There are two ways to get one "config.txt":

- You create this file by yourself. See [Configuration Files](#) (on page 418).
- You download the raw configuration data from the device.

The downloaded raw configuration contains almost all of current settings on your device.

---

Warning: When you download the raw configuration data, some configuration keys are commented out and must remain that way. See [Keys that Cannot Be Uploaded](#) (on page 459).

---

## Download via Web Browsers

There are two scenarios by using web browsers.

### ► *URL containing login credentials:*

To log in immediately while issuing the download request, type an URL containing the login credentials in the web browser.

```
http(s)://<user>:<password>@<device IP>/cgi-bin/raw_config_download.cgi
```

Parameter	Description
<user>	Any user name that has the Administrator Privileges.
<password>	The password of the specified user name.
<device IP>	Hostname or IP address of the device whose raw configuration you want to download.

- For example:

```
https://admin:adm@192.168.84.114/cgi-bin/raw_config_download.cgi
```

### ► *URL without login credentials contained:*

If you would like to log in after issuing the download request, type an URL without login credentials contained in the web browser. The system will then prompt you to enter the login credentials.

```
http(s)://<device IP>/cgi-bin/raw_config_download.cgi
```

- For example:

```
https://192.168.84.114/cgi-bin/raw_config_download.cgi
```

## Download via Curl

If you have installed curl on your computer, you can download the raw configuration from your device by performing the curl command.

### ► *To download raw configuration via curl:*

1. Type the following curl command in the command line interface.

```
curl -k https://<user>:<password>@<device IP>/cgi-bin/  
raw_config_download.cgi > config.txt
```

Parameter	Description
<user>	Any user name that has the Administrator Privileges.
<password>	The password of the specified user name.
<device IP>	Hostname or IP address of the device whose raw configuration you want to download.

2. When the download is complete, a line indicates 100 in the first % column.

```

% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
100 20184    0 20184    0     0  9511      0  --:--:--  0:00:02  --:--:--  9584

```

3. Go to the directory where you perform the curl command to find the "config.txt" file.

---

Tip: In the above curl command, you can replace the filename "config.txt" with any filename you prefer.

---

► **Example:**

```

curl -k https://admin:admn@192.168.84.114/cgi-bin/raw_config_download.cgi
> config.txt

```

## Uploading Raw Configuration

There are two upload methods:

- *SCP or PSCP command:* See [Raw Configuration Upload and Download](#) (on page 446).
- *CURL command:* See [Upload via Curl](#) (on page 448).

The uploaded raw configuration file can contain only partial configuration keys that you want to modify. Other settings that are not contained in the uploaded file will remain unchanged.

Authentication-related data or HTTP(S) port may be no longer the same after uploading raw configuration. Therefore, it is suggested to double check what configuration keys will be changed in the raw configuration file that you will upload.

### Upload via Curl

If curl is available on your computer, you can upload the raw configuration to BCM2 with the curl command.



There are two scenarios with the curl upload methods.

- When there are NO device-specific settings involved, you upload the configuration file only, regardless of the number of BCM2 devices to update.
- When there are device-specific settings involved for updating more than one BCM2 devices, you must upload two files. including one configuration file and one device list file.

► *To upload one configuration file only:*

1. Type the following curl command in the command line interface.

```
curl -k -F "config_file=@<config file>" https://<user>:<password>@<device IP>/cgi-bin/raw_config_update.cgi
```

Parameter	Description
<user>	Any user name that has the Administrator Privileges.
<password>	The password of the specified user name.
<device IP>	Hostname or IP address of the BCM2 whose raw configuration you want to upload.
<config file>	Filename of the configuration file. <ul style="list-style-type: none"><li>• For the syntax, see <i>config.txt</i> (on page ).</li></ul>

2. When the upload is completed successfully, the curl returns the code 0 (zero).

---

*Note: If the upload fails and curl returns other codes, see [Curl Upload Return Codes](#) (on page ).*

---

3. After several seconds, BCM2 reboots automatically. Changed settings take effect after the reboot process finishes.

► *To upload both configuration and device list files:*

1. Type the following curl command in the command line interface.

```
curl -k -F "config_file=@<config file>" -F "device_list_file=@<dev_list file>" https://<user>:<password>@<device IP>/cgi-bin/raw_config_update.cgi?match=<dev_col>
```

Parameter	Description
<user>, <password>, <device IP>, <config file>	Refer to the above table for explanation. <ul style="list-style-type: none"><li>• For device-specific settings in the &lt;config file&gt;, refer each device-specific configuration key to a specific column in the &lt;dev_list file&gt;. See <i>config.txt</i> (on page ).</li></ul>

Parameter	Description
<dev_list_file>	Filename of the device list file in CSV format. <ul style="list-style-type: none"> <li>For the content format, see <i>devices.csv</i> (on page ).</li> </ul>
<dev_col>	<dev_col> comprises "serial:" or "mac:" and the number of the column where the serial number or MAC address of each BCM2 is in the uploaded CSV file. This is the data based on which each device finds its device-specific settings. For example: <ul style="list-style-type: none"> <li>If the second column contains each device's serial number, the parameter is then <code>serial:2</code>.</li> <li>If the seventh column contains each device's MAC address, the parameter is then <code>mac:7</code>.</li> </ul>

2. BCM2 will reboot after Curl shows the return code 0. For details, refer to above steps 2 to 3.

► **Examples:**

- Upload of the configuration file only:

```
curl -k -F "config_file=@config.txt" https://admin:adm@192.168.84.114/cgi-bin/raw_config_download.cgi
```

- Upload of both configuration and device list files:

```
curl -k -F "config_file=@config.txt" -F "device_list_file=@devices.csv" https://admin:adm@192.168.84.114/cgi-bin/raw_config_download.cgi
```

### Curl Upload Return Codes

After performing raw configuration *Upload via Curl* (on page ), curl will return a code to indicate the result of the file upload.

Code	Description
0	Operation was successful.
1	An internal error occurred.
2	A parameter error occurred.
3	A raw configuration update operation is already running.
4	The file is too large.
5	Invalid raw configuration file provided.

Code	Description
6	Invalid device list file or match provided.
7	Device list file required but missing.
8	No matching entry in device list found.
9	Macro substitution error.
10	Decrypting value failed.
11	Unknown magic line.
12	Processing magic line failed.

## Bulk Configuration, Firmware Upgrade, or Backup/Restore via SCP

You can perform a SSH File Transfer Protocol (SFTP) or Secure Copy (SCP) command to update the firmware, do bulk configuration, or back up and restore the configuration.

---

Note: Because of security issues the SFTP (SSH File Transfer Protocol) should be used. SCP client in newer OpenSSH versions uses SFTP protocol by default. SCP is still supported and needs to be enabled.

---

### Firmware Update via SCP

Same as any firmware update, all user management operations are suspended and all login attempts fail during the SCP firmware update.

---

Warning: Do NOT perform the firmware upgrade over a wireless network connection.

---

#### ► To update the firmware via SCP:

1. Type the following SCP command and press Enter.

```
scp <firmware file> <user name>@<device ip>:/fwupdate
```

- *<firmware file>* is the firmware's filename. If the firmware file is not in the current directory, you must include the path in the filename.
  - *<user name>* is the "admin" or any user profile with the Firmware Update permission.
  - *<device ip>* is the IP address or hostname where you want to upload the specified file.
2. Type the password when prompted, and press Enter.
  3. The system transmits the specified firmware file to the device, and shows the transmission speed and percentage.
  4. When the transmission is complete, it shows the following message, indicating that the BCM2 starts to update its firmware now. Wait until the upgrade completes.

Starting firmware update. The connection will be closed now.

► *SCP example:*

```
scp pdu-px2-030410-44599.bin admin@192.168.87.50:/fwupdate
```

► *Windows PSCP command:*

PSCP in Windows works in a similar way to the SCP.

- `pscp <firmware file> <user name>@<device ip>:/fwupdate`

## Bulk Configuration via SCP

Like performing bulk configuration via the web interface, there are two steps with the bulk configuration using the SCP commands:

- a. Save a configuration from a source device.
- b. Copy the configuration file to one or multiple destination device.

Note: You can configure *device-specific* settings with the upload of raw configuration but not with the bulk configuration file.

► *To save the configuration via SCP:*

1. Type the following SCP command and press Enter.

```
scp <user name>@<device ip>:/bulk_config.txt <filename>
```

- *<user name>* is any user profile with Administrator Privileges.
  - *<device ip>* is the IP address or hostname of the device whose configuration you want to save.
  - *<filename>* is the custom filename you assign to the "bulk\_config.txt" of the source device.
2. Type the user password when prompted.
  3. The system saves the configuration to a file named "bulk\_config.txt."

► *To copy the configuration via SCP:*

1. Type the following SCP command and press Enter.

```
scp bulk_config.txt <user name>@<device ip>:/bulk_restore
```

- *<user name>* any user profile with Administrator Privileges
  - *<device ip>* is the IP address of the device whose configuration you want to copy.
2. Type the user password when prompted.
  3. The system copies the configuration included in the file "bulk\_config.txt" to another device, and displays the following message.

```
Starting restore operation. The connection will be closed now.
```

► *SCP examples:*

- Save operation:

```
scp admin@192.168.87.50:/bulk_config.txt today_config.txt
```

- Copy operation:

```
scp today_config.txt admin@192.168.87.47:/bulk_restore
```

For the linked units you can backup each unit by specifying the link id.

- Save operation:

```
scp admin@10.0.42.3:/backup_settings.txt/link_id=2 backup_settings.txt
```

- Copy operation:

```
scp backup_settings.txt admin@10.0.42.3:/settings_restore/link_id=2
```

► *Windows PSCP commands:*

PSCP in Windows works in a similar way to the SCP.

- Save operation:

```
pscp <user name>@<device ip>:/bulk_config.txt today_config.txt
```

- Copy operation:

```
pscp today_config.txt <user name>@<device ip>:/bulk_restore
```

## Backup and Restore via SCP

To back up ALL settings of a BCM2, including device-specific settings, you should perform the backup operation instead of the bulk configuration.

You can restore all settings to previous ones after a backup file is available.

► *To back up the settings via SCP:*

1. Type the following SCP command and press Enter.

```
scp <user name>@<device ip>:/backup_settings.txt
```

- <user name> is the "admin" or any user profile with Administrator Privileges
- <device ip> is the IP address or hostname of the BCM2 whose settings you want to back up.

2. Type the user password when prompted.

3. The system saves the settings from the BCM2 to a file named "backup\_settings.txt."

► *To restore the settings via SCP:*

1. Type the following SCP command and press Enter.

```
scp backup_settings.txt <user name>@<device ip>:/settings_restore
```

- *<user name>* is the "admin" or any user profile with Administrator Privileges
  - *<device ip>* is the IP address or hostname of the BCM2 whose settings you want to restore.
2. Type the user password when prompted.
  3. The system copies the configuration included in the file "backup\_settings.txt" to the BCM2, and displays the following message.

```
Starting restore operation. The connection will be closed now.
```

► *SCP examples:*

- Backup operation:  

```
scp admin@192.168.87.50:/backup_settings.txt
```
- Restoration operation:  

```
scp backup_settings.txt admin@192.168.87.50:/settings_restore
```

► *Windows PSCP commands:*

PSCP in Windows works in a similar way to the SCP.

- Backup operation:  

```
pscp <user name>@<device ip>:/backup_settings.txt
```
- Restoration operation:  

```
pscp backup_settings.txt <user name>@<device ip>:/settings_restore
```

## Downloading Diagnostic Data via SCP

You can download the diagnostic data via SCP.

► *To download the diagnostic data via SCP:*

1. Type one of the following SCP commands and press Enter.
  - *<user name>* is the "admin" or any user profile with Administrator Privileges or "Unrestricted View Privileges" privileges.
  - *<device ip>* is the IP address or hostname of the BCM2 whose data you want to download.
  - *<port>* is the current SSH/SCP port number, or the port number of a specific expansion device in the Port-Forwarding chain.
  - *<filename>* is the new filename of the downloaded file.

**Scenario 1: Use the default SCP port and default filename**

- SSH/SCP port is the default (22), and the accessed BCM2 is a standalone device.
- The diagnostic file's default filename "diag-data.zip" is wanted. Then add a dot (.) in the end of the SCP command as shown below.

```
scp <user name>@<device ip>:/diag-data.zip .
```

### Scenario 2: Specify a different SCP port but use the default filename

- SSH/SCP port is NOT the default (22), or the accessed BCM2 is a Port-Forwarding expansion device.
- The diagnostic file's default filename "diag-data.zip" is wanted. Then add a dot in the end of the SCP command as shown below.

```
scp -P <port> <user name>@<device ip>:/diag-data.zip .
```

### Scenario 3: Specify a new filename but use the default SCP port

- SSH/SCP port is the default (22), and the accessed BCM2 is a standalone device.
- Renaming the diagnostic file is wanted.

```
scp <user name>@<device ip>:/diag-data.zip <filename>
```

### Scenario 4: Specify a different SCP port and a new filename

- SSH/SCP port is NOT the default (22), or the accessed BCM2 is a Port-Forwarding expansion device.
- Renaming the diagnostic file is wanted.

```
scp -P <port> <user name>@<device ip>:/diag-data.zip <filename>
```

2. Type the password when prompted.
3. The system downloads the specified data from the BCM2 onto your computer.
  - If you do NOT specify a new filename in the command, such as Scenarios 1 or 2, the downloaded file's default name is "diag-data.zip."
  - If you specify a new filename in the command, such as Scenarios 3 or 4, the downloaded file is renamed accordingly.



► *SCP example:*

```
scp admin@192.168.87.50:/diag-data.zip .
```

► *Windows PSCP command:*

PSCP in Windows works in a similar way to the SCP.

- `pscp -P <port> <user name>@<device ip>:/diag-data.zip <filename>`

## Uploading or Downloading Raw Configuration Data

You can download the raw configuration data of a specific device for review, backup or modification.

After modifying or creating any raw configuration data, you can upload it to a specific device for changing its configuration. The uploaded raw configuration file can contain only partial configuration keys that you want to modify. Other settings that are not contained in the uploaded file will remain unchanged.

Syntax of the raw configuration data is completely the same as the syntax in the config.txt file. See config.txt.

---

**Warning: Some configuration keys in the downloaded raw configuration are commented out, and those must NOT be part of the configuration that will be uploaded to any device. See [Keys that Cannot Be Uploaded](#) (on page 459).**

---

► *To download raw configuration data:*

1. Type one of the following SCP commands and press Enter.

**Scenario 1: Use the default SCP port and default filename**

- SSH/SCP port is the default (22), and the accessed device is a standalone device.
- The raw configuration file's default filename "raw\_config.txt" is wanted. Then add a dot (.) in the end of the SCP command as shown below.

```
scp <user name>@<device ip>:/raw_config.txt .
```

**Scenario 2: Specify a different SCP port but use the default filename**

- SSH/SCP port is NOT the default (22), or the accessed device is a Port-Forwarding expansion device.
- The raw configuration file's default filename "raw\_config.txt" is wanted. Then add a dot in the end of the SCP command as shown below.

```
scp -P <port> <user name>@<device ip>:/raw_config.txt .
```

**Scenario 3: Specify a new filename but use the default SCP port**

- SSH/SCP port is the default (22), and the accessed device is a standalone device.
- Renaming the raw configuration file is wanted.

```
scp <user name>@<device ip>:/raw_config.txt <filename>
```

#### Scenario 4: Specify a different SCP port and a new filename

- SSH/SCP port is NOT the default (22), or the accessed device is a Port-Forwarding expansion device.
- Renaming the raw configuration file is wanted.

```
scp -P <port> <user name>@<device ip>:/raw_config.txt <filename>
```

- <user name> is the "admin" or any user profile with Administrator Privileges.
  - <device ip> is the IP address or hostname of the device whose data you want to download.
  - <port> is the current SSH/SCP port number, or the port number of a specific link unit device in the Port-Forwarding chain.
  - <filename> is the new filename of the downloaded file.
2. Type the password when prompted.
  3. The system downloads the specified data from the device onto your computer.
    - If you do NOT specify a new filename in the command, such as Scenarios 1 or 2, the downloaded file's default name is "raw\_config.txt."
    - If you specify a new filename in the command, such as Scenarios 3 or 4, the downloaded file is renamed accordingly.

#### ► To upload raw configuration data:

1. Type one of the following SCP commands and press Enter.

##### Scenario 1: Only one device to configure, with the default SCP port

- SSH/SCP port is the default (22), and the accessed device is a standalone device.
- There is only one device to configure so a CSV file for device-specific settings is NOT needed.

```
scp <config file> <user name>@<device ip>:/raw_config_update
```

##### Scenario 2: Only one device to configure, with a non-default SCP port

- SSH/SCP port is NOT the default (22), or the accessed device is a Port-Forwarding expansion device.
- There is only one device to configure so a CSV file for device-specific settings is NOT needed.

```
scp -P <port> <config file> <user name>@<device ip>:/raw_config_update
```

##### Scenario 3: Multiple device to configure, with the default SCP port

- SSH/SCP port is the default (22), and the accessed device is a standalone device.
- There are multiple devices to configure so a CSV file for device-specific settings is needed during the upload.

```
scp <dev_list file> <config file> <user name>@<device ip>:/  
raw_config_update/match=<col>
```

##### Scenario 4: Multiple device to configure, with a non-default SCP port

- SSH/SCP port is NOT the default (22), or the accessed device is a Port-Forwarding expansion device.
- There are multiple devices to configure so a CSV file for device-specific settings is needed during the upload.

```
scp -P <port> <dev_list file> <config file> <user name>@<device ip>:/  
raw_config_update/match=<dev_col>
```

- `<config file>` is the filename of the custom raw configuration that you want to upload.
- `<user name>` is the "admin" or any user profile with Administrator Privileges.
- `<device ip>` is the IP address or hostname of the device where you want to upload the specified file.
- `<port>` is the current SSH/SCP port number, or the port number of a specific expansion device in the Port-Forwarding chain.
- `<dev_list file>` is the name of the CSV file for configuring multiple device with device-specific settings. For this file's format, see `devices.csv`.
  - For device-specific settings in the `<config file>`, refer each device-specific configuration key to a specific column in the `<dev_list file>`. See `config.txt`.
- `<dev_col>` comprises "serial:" or "mac:" and the number of the column where the serial number or MAC address of each device is in the uploaded CSV file. This is the data based on which each device finds its device-specific settings.

For example:

- If the second column contains each device's serial number, the parameter is then `serial:2`.
- If the seventh column contains each device's MAC address, the parameter is then `mac:7`.

#### ► *SCP examples:*

- Raw configuration download example --  

```
scp admin@192.168.87.50:/raw_config.txt config.txt
```
- Raw configuration upload example with the configuration file only --  

```
scp config.txt admin@192.168.87.50:/raw_config_update
```
- Raw configuration upload example with both configuration and device list files --  

```
scp devices.csv config.txt admin@192.168.87.50:/raw_config_update/  
match=serial:2
```

#### ► *Windows PSCP commands:*

PSCP in Windows works in a similar way to the SCP.

- `pscp -P <port> <user name>@<device ip>:/raw_config.txt <filename>`
- `pscp -P <port> <CSV file> <config file> <user name>@<device ip>:/raw_config_update/match=<col>`

#### ► *Alternative of bulk configuration via SCP:*

Both methods of uploading 'bulk configuration' file or 'raw configuration' file via SCP can serve the purpose of bulk configuration. The only difference is that you can configure *device-specific* settings with the upload of raw configuration but not with the 'bulk configuration' file.

### Keys that Cannot Be Uploaded

The raw configuration downloaded from any BCM2 contains a few configuration keys that are commented out with either syntax below.

These configuration keys cannot be part of the configuration that you will upload to any BCM2. That is, they should be either not available or remain commented out in the configuration file you will upload.

<b>Comment syntax</b>	<b>Description</b>
#INTERNAL#	Internal use only. They are NOT user configurable settings.
#OLD/INVALID#	These keys are old or invalid ones.

## Remote Authentication Examples

### In This Chapter

LDAP Configuration Illustration. . . . .	461
RADIUS Configuration Illustration. . . . .	466
Cisco ISE Xerus TACACS+ Authentication. . . . .	480

### LDAP Configuration Illustration

This section provides an LDAP example for illustrating the configuration procedure using Microsoft Active Directory® (AD). To configure LDAP authentication, four main steps are required:

- a. Determine user accounts and roles (groups) intended for the device
- b. Create user groups for the device on the AD server
- c. Configure LDAP authentication on the device
- d. Configure roles on the device

---

**Important: TLS is used 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.**

---

#### Step A. Determine User Accounts and Roles

Determine the user accounts and roles (groups) that are authenticated for accessing the device. In this example, we will create two user roles with different permissions. Each role (group) will consist of two user accounts available on the AD server.

User roles	User accounts (members)
PX_User	usera
	pxuser2
PX_Admin	userb
	pxuser

Group permissions:

- The PX\_User role will have neither system permissions nor outlet permissions.
- The PX\_Admin role will have full system and outlet permissions.

#### Step B. Configure User Groups on the AD Server

You must create the groups (roles) for the BCM2 on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups (roles) for the BCM2 are named *PX\_Admin* and *PX\_User*.
- User accounts *pxuser*, *pxuser2*, *usera* and *userb* already exist on the AD server.

► *To configure user groups on the AD server:*

1. On the AD server, create new groups -- *PX\_Admin* and *PX\_User*.

---

*Note: Refer to the documentation or online help accompanying Microsoft AD for detailed instructions.*

---

2. Add the *pxuser2* and *usera* accounts to the *PX\_User* group.
3. Add the *pxuser* and *userb* accounts to the *PX\_Admin* group.
4. Verify whether each group comprises correct users.



## Step C. Configure LDAP Authentication on the BCM2

You must enable and set up LDAP authentication properly on the BCM2 to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See *Wired Network Settings and Role of a DNS Server*.
- 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*.
2. In the *LDAP Servers* section, click *New* to add an LDAP/LDAPS server.
3. Provide the BCM2 with the information about the AD server.

Field/setting	Do this...
IP address / hostname	Type the domain name <code>techadssl.com</code> or IP address <code>192.168.56.3</code> . <ul style="list-style-type: none"> <li>Without the 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 encryption is enabled.</li> </ul>
Copy settings from existing LDAP server	Leave the checkbox deselected unless the new LDAP server's settings are similar to any existing LDAP settings.
Type of LDAP server	Select "Microsoft Active Directory."
Security	Select "None" since the TLS encryption is not applied in this example.
Port (None/StartTLS)	Ensure the field is set to <code>389</code> .
Port (TLS), CA certificate	Skip the two fields since the TLS encryption is not enabled.
Anonymous bind	Select this checkbox because anonymous bind is used.
Bind DN, Bind password, Confirm bind password	Skip the three fields because of anonymous bind.
Base DN for search	Type <code>dc=techadssl,dc=com</code> as the starting point where your search begins on the AD server.
Login Name Attribute	Ensure the field is set to <code>sAMAccountName</code> because the LDAP server is Microsoft Active Directory.
User entry object class	Ensure the field is set to <code>user</code> 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 <code>techadssl.com</code> .

### Add LDAP Server

IP address/hostname: 192.168.52.55

Copy settings from existing LDAP server

Select LDAP Server: ▼

Type of LDAP server: Microsoft Active Directory ▼

Security: None ▼

Port (None/StartTLS): 389

Port (TLS): 636

Enable verification of LDAP server certificate

CA certificate: not set Show Remove

Browse... Certificate file

Allow expired and not yet valid certificates

Anonymous bind

Bind DN:

Bind password:

Confirm bind password:

Base DN for search: techadssl.dc-com

Login Name Attribute: sAMAccountName

User entry object class: user

User search subfilter:

Active Directory domain: techadssl.com

Test Connection

Note: LDAP authenticated users will see units from Default Preferences.

✕ Cancel ✓ Add Server

1. Click Add Server. The LDAP server is saved.
2. In the Authentication Type field, select LDAP.
3. Click Save. The LDAP authentication is activated.

---

Note: If the BCM2 clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, may be considered expired. To ensure proper synchronization, administrators should configure the BCM2 and the LDAP server to use the same NTP server(s).

---



## Step D. Configure Roles on the BCM2

A role on the BCM2 determines the system and outlet permissions. You must create the roles whose names are identical to the user groups created for the BCM2 on the AD server or authorization will fail. Therefore, we will create the roles named *PX\_User* and *PX\_Admin* on the PDU.

In this illustration, we assume:

- Users assigned to the *PX\_User* role can view settings only, but they can neither configure BCM2 nor access the outlets.
- Users assigned to the *PX\_Admin* role have the Administrator Privileges so they can both configure BCM2 and access the outlets.

### ► To create the *PX\_User* role with appropriate permissions assigned:

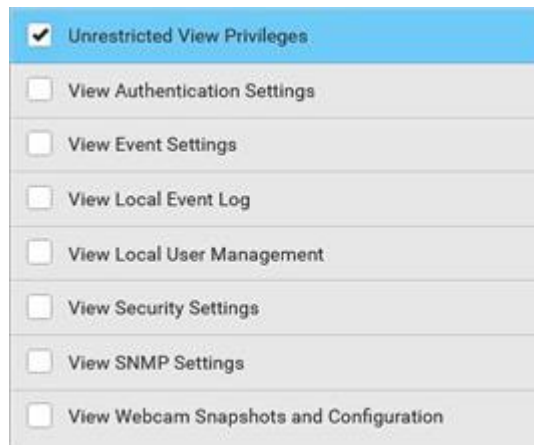
1. Choose User Management > Roles.

2. Click  to add a new role.

a. Type *PX\_User* in the Role Name field.

b. Type a description for the *PX\_User* role in the Description field. In this example, we type "View PX settings" to describe the role.


c. In the Privileges list, select Unrestricted View Privileges, which includes all View permissions. The Unrestricted View Privileges permission lets users view all settings without the capability to configure or change them.



<input checked="" type="checkbox"/>	Unrestricted View Privileges
<input type="checkbox"/>	View Authentication Settings
<input type="checkbox"/>	View Event Settings
<input type="checkbox"/>	View Local Event Log
<input type="checkbox"/>	View Local User Management
<input type="checkbox"/>	View Security Settings
<input type="checkbox"/>	View SNMP Settings
<input type="checkbox"/>	View Webcam Snapshots and Configuration



d. Click Save.

3. The *PX\_User* role is created.

Role Name ▲	Description
Admin	System defined administrator role including all privileges. 
Operator	Predefined operator role.
PX_User	View PX settings


4. Keep the Roles page open to create the PX\_Admin role.

► To create the PX\_Admin role with full permissions assigned:

1. Click   to add another role.
  - a. Type PX\_Admin in the Role Name field.
  - b. Type a description for the PX\_Admin role in the Description field. In this example, we type "Includes all PX privileges" to describe the role.
  - c. In the Privileges list, select Administrator Privileges. The Administrator Privileges allows users to configure or change all BCM2 settings.



- d. Click Save.
2. The PX\_Admin role is created.

Role Name ▲	Description
Admin	System defined administrator role including all privileges. 
Operator	Predefined operator role.
PX_Admin	Includes all PX privileges
PX_User	View PX settings

## 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 FreeRADIUS server.

The following steps are required for any RADIUS authentication:

1. Configure RADIUS authentication on the BCM2. See Adding Radius Servers.
2. Configure roles on the BCM2. See Creating Roles.
3. Configure BCM2 user credentials and roles on your RADIUS server.
  - To configure using standard attributes, see *Standard Attributes* (on page ).
  - To configure using vendor-specific attributes, see *Vendor-Specific Attributes* (on page ).

Note that we assume that the NPS is running on a Windows 2008 system in the NPS illustrations.

## Standard Attributes

The RADIUS standard attribute "Filter-ID" is used to convey the group membership, that is, roles.

- If a user has multiple roles, configure multiple standard attributes for this user.
- The syntax of a standard attribute is:

```
Raritan:G{role-name}
```

### FreeRADIUS Standard Attribute Illustration

With standard attributes, NO dictionary files are required. You simply add all user data, including user names, passwords, and roles, in the following FreeRADIUS path.

```
/etc/raddb/users
```

#### ► *Presumptions in the illustration:*

- User name = `steve`
- Steve's password = `test123`
- Steve's roles = `Admin` and `SystemTester`

#### ► *To create a user profile for "steve" in FreeRADIUS:*

1. Go to this location: `/etc/raddb/users`.
2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"  
Filter-ID = "Raritan:G{Admin}",  
Filter-ID = "Raritan:G{SystemTester}"
```

## Vendor-Specific Attributes

You must specify the following properties when using a RADIUS vendor-specific attribute (VSA).

- Vendor code = `13742`
- Vendor-assigned attribute number = `26`
- Attribute format = `String`

The syntax of the vendor-specific attribute for specifying one or multiple roles is:

Raritan:G{role-name1 role-name2 role-name3}

For configuration on NPS, see *NPS VSA Illustration* (on page ).

For configuration on FreeRADIUS, see *FreeRADIUS VSA Illustration* (on page ).

## NPS VSA Illustration

To configure Windows 2008 NPS with the *vendor-specific attribute*, you must:

- a. Add your BCM2 to NPS. See *Step A: Add Your BCM2 as a RADIUS Client* (on page ).
- b. On the NPS, configure connection request policies and the vendor-specific attribute. See *Step B: Configure Connection Policies and Vendor-Specific Attributes* (on page ).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See *AD-Related Configuration* (on page ).

### Step A: Add Your BCM2 as a RADIUS Client

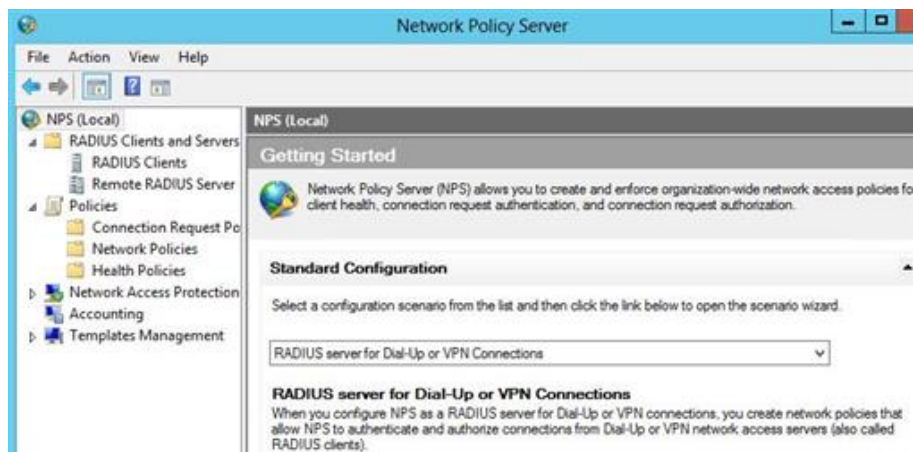
The RADIUS implementation on the BCM2 follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

#### ► *Presumptions in the illustration:*

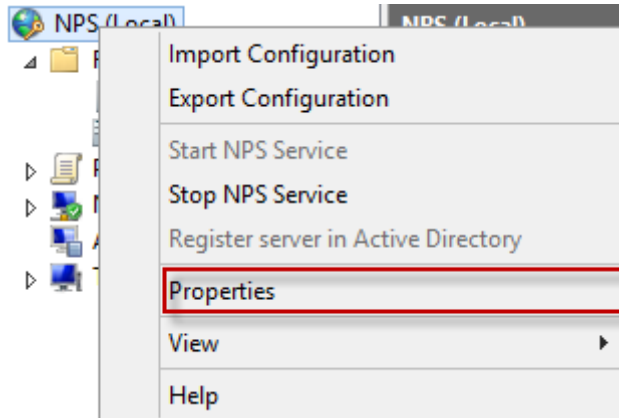
- IP address of your BCM2 = 192.168.56.29
- RADIUS authentication port specified for BCM2: 1812
- RADIUS accounting port specified for BCM2: 1813

#### ► *To add your BCM2 to the RADIUS NPS:*

1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.



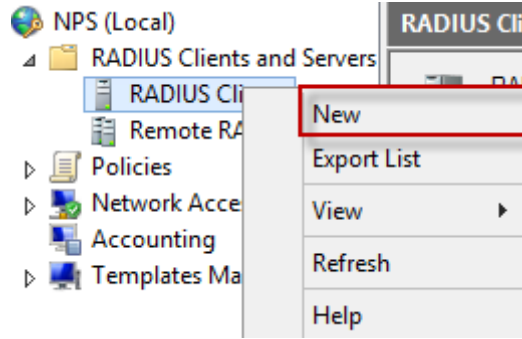
2. Right-click NPS (Local), and select Properties.



Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your BCM2. In this example, they are 1812 and 1813. Then close this dialog.



3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.



4. Do the following to add your BCM2 to NPS:
  - a. Verify the "Enable this RADIUS client" checkbox is selected.
  - b. Type a name for identifying your BCM2 in the "Friendly name" field.
  - c. Type *192.168.56.29* in the "Address (IP or DNS)" field.
  - d. Select *RADIUS Standard* in the "Vendor name" field.
  - e. Select the *Manual* radio button.
  - f. Type the shared secret in the "Shared secret" and "Confirm shared secret" fields. The shared secret must be the same as the one specified on your BCM2.



5. Click OK.

## Step B: Configure Connection Policies and Vendor-Specific Attributes

You need to configure the following for connection request policies:

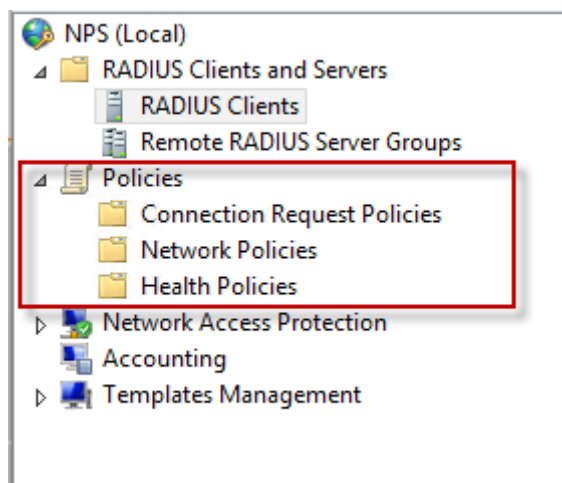
- IP address or host name of the BCM2
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

### ► *Presumptions in the illustration:*

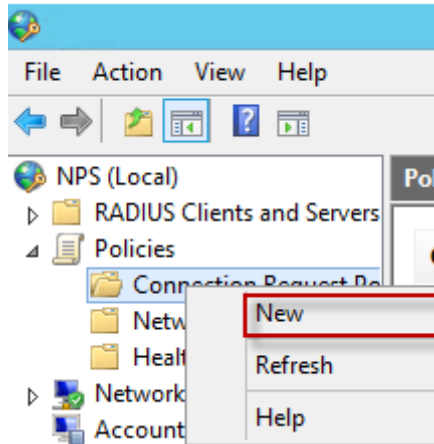
- IP address of your BCM2 = 192.168.56.29
- Local NPS server is used
- RADIUS protocol selected on your BCM2 = CHAP
- Existing roles of your BCM2 = Admin, User and SystemTester

### ► *Illustration:*

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.

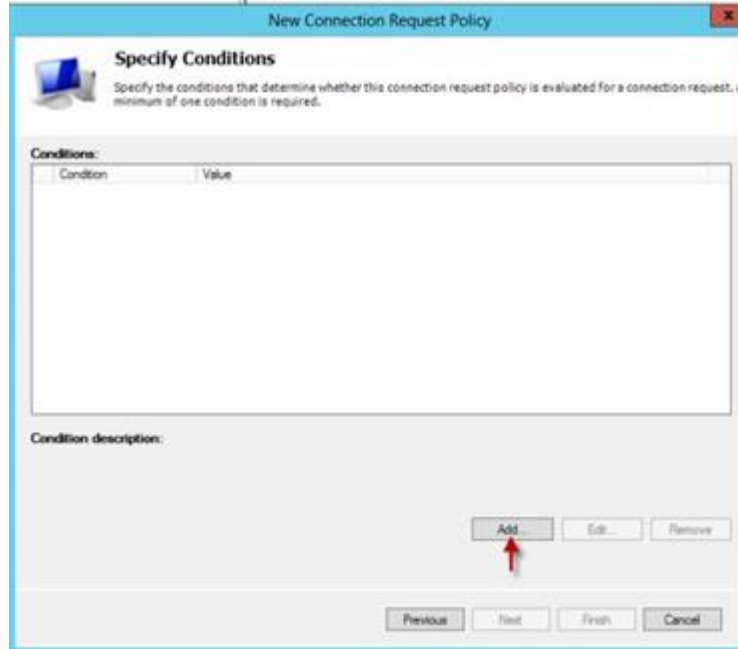


3. Type a descriptive name for identifying this policy in the "Policy name" field.
  - You can leave the "Type of network access server" field to the default -- Unspecified.

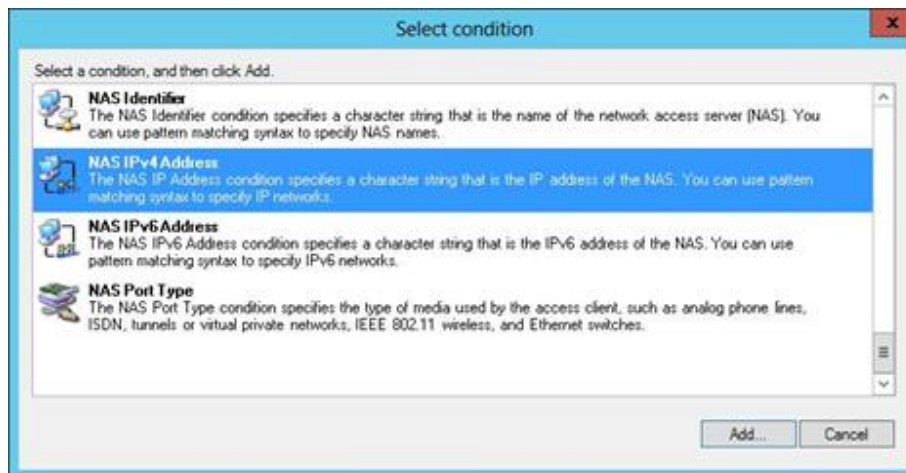


4. Click Next to show the "Specify Conditions" screen. Click Add.

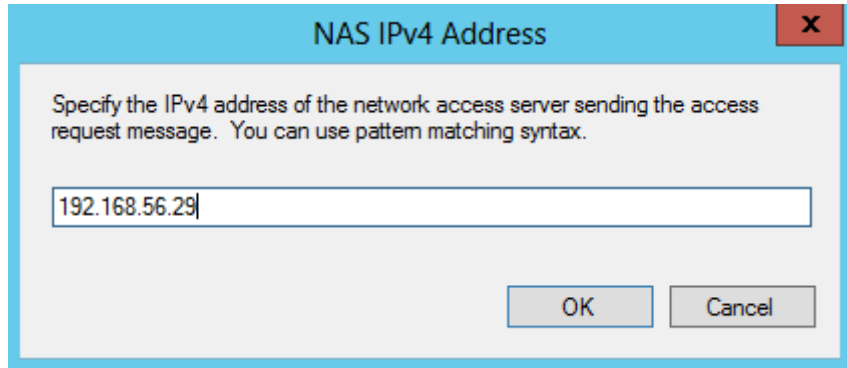




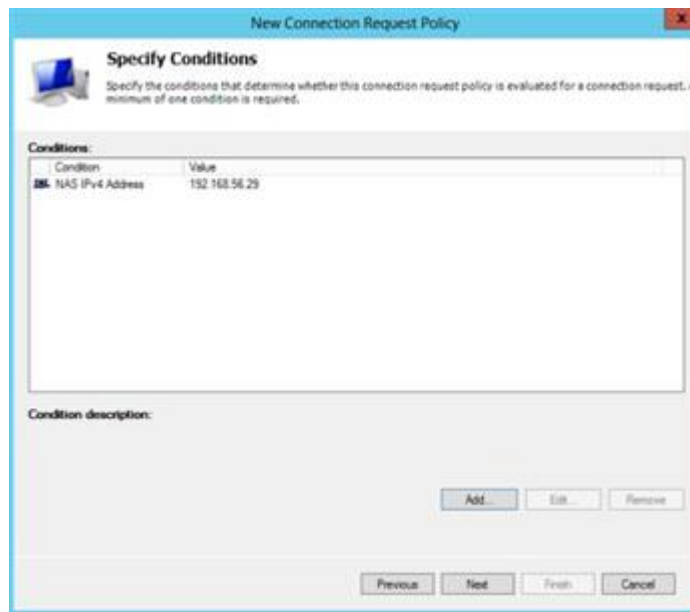
5. The "Select condition" dialog appears. Click Add.



6. The NAS IPv4 Address dialog appears. Type the BCM2 IP address -- 192.168.56.29, and click OK.



7. Click Next in the New Connection Request Policy dialog.

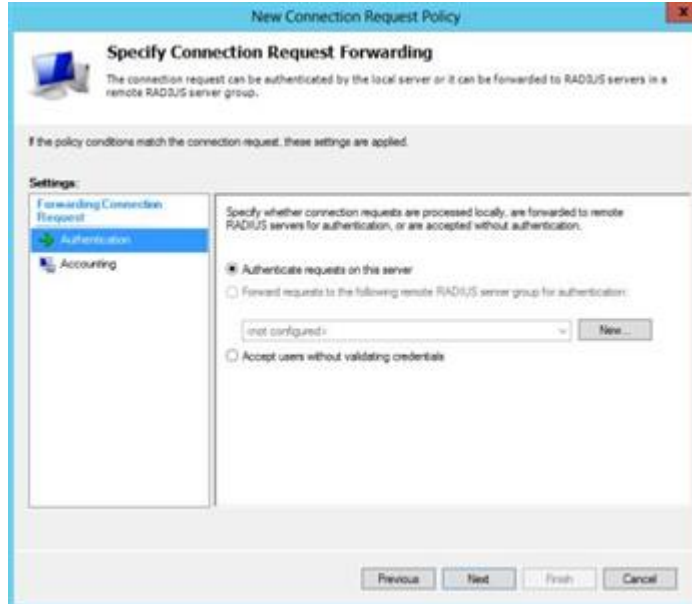


8. Select "Authenticate requests on this server" because a local NPS server is used in this example. Then click Next.

---

*Note: Connection Request Forwarding options must match your environment.*

---

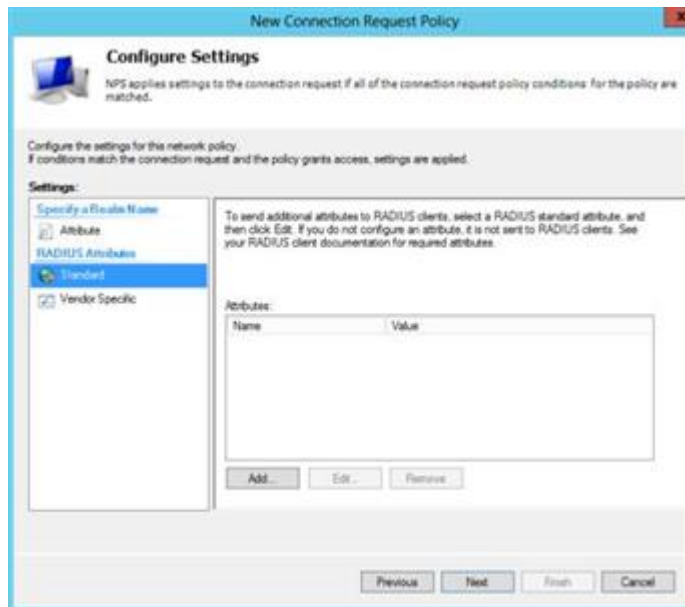


9. When the system prompts you to select the authentication method, select the following two options:
  - Override network policy authentication settings
  - CHAP -- the BCM2 uses "CHAP" in this example

---

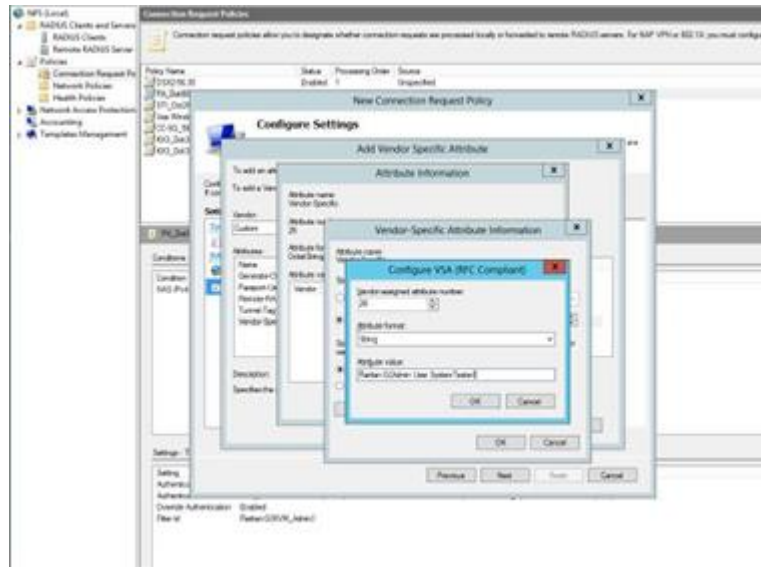
*Note: If your BCM2 uses PAP, then select "PAP."*

---



10. Select Vendor Specific to the left of the dialog, and click Add. The Add Vendor Specific Attribute dialog appears.
11. Select Custom in the Vendor field, and click Add. The Attribute Information dialog appears.

12. Click Add, and the Vendor-Specific Attribute Information dialog appears.
  13. Click "Enter Vendor Code" and type 13742.
  14. Select "Yes, it conforms" to indicate that the custom attribute conforms to the RADIUS Request For Comment (RFC).
  15. 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 'Admin,' 'User' and 'SystemTester' are specified inside the curved brackets {}.
- Note that multiple roles are separated with a space.



16. Click OK.

### FreeRADIUS VSA Illustration

A vendor-specific dictionary file is required for the vendor-specific-attribute configuration on FreeRADIUS. Therefore, there are two major configuration steps.

- a. Use a dictionary to define the Raritan vendor-specific attribute
- b. Add all user data, including user names, passwords, and roles

► *Presumptions in the illustration:*

- Raritan attribute = Raritan-User-Roles
- User name = steve
- Steve's password = test123
- Steve's roles = Admin, User and SystemTester

► *Step A -- define the vendor-specific attribute in FreeRADIUS:*

1. Go to this location: `/etc/raddb/dictionary`.
2. Type the following in the Raritan dictionary file.

```
VENDOR Raritan 13742
BEGIN-VENDOR Raritan
ATTRIBUTE Raritan-User-Roles 26 string
END-VENDOR Raritan
```

► *Step B -- create a user profile for "steve" in FreeRADIUS:*

1. Go to this location: `/etc/raddb/users`.
2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Raritan-PDU-User-Roles = "Raritan:G{Admin User SystemTester}"
```

## AD-Related Configuration

When RADIUS authentication is intended, make sure you also configure the following settings related to Microsoft Active Directory (AD):

- Register the NPS server in AD
- Configure remote access permission for users in AD

The NPS server is registered in AD only when NPS is configured for the FIRST time and user accounts are created in AD.

If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

- Store password using reversible encryption

---

**Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.**

---

► *To register NPS:*

1. Open the NPS console.
2. Right-click NPS (Local) and select "Register server in Active Directory."

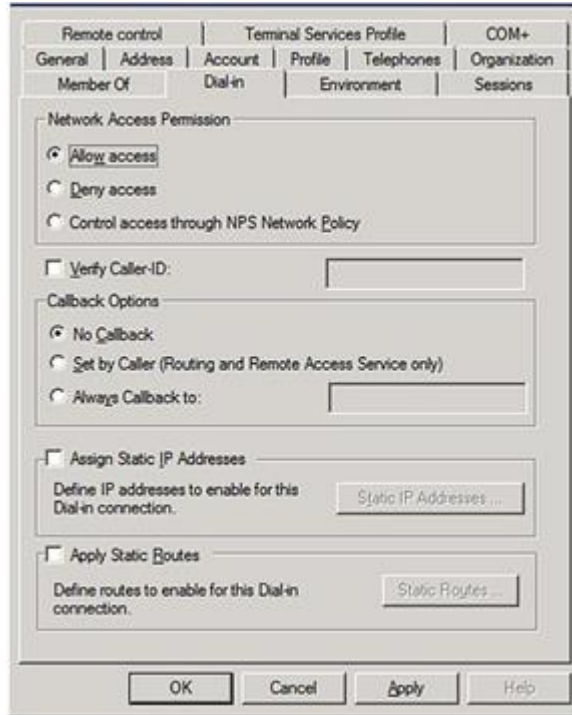


3. Click OK, and then OK again.



► *To grant BCM2 users remote access permission:*

1. Open Active Directory Users and Computers.
2. Open the properties dialog of the user whom you want to grant the access permission.
3. Click the Dial-in tab and select the "Allow access" checkbox.



► *To enable reversible encryption for CHAP authentication:*

1. Open Active Directory Users and Computers.
2. Open the properties dialog of the user that you want to configure.
3. Click the Account tab and select the "Store password using reversible encryption" checkbox.



## Cisco ISE Xerus TACACS+ Authentication

### ► *Configuring Cisco ISE 2.1.x for authenticating TACACS+ users on the Xerus Platform*

Xerus performs authorization through the user's membership in local roles. You must create a local role on Xerus and matching role (case sensitive) on Cisco ISE.

### ► *Configure TACACS+ on Xerus:*

1. Log in to BCM2 with an administrative account.
2. Select Access Device Settings > Security > TACACS+ and add the Cisco ISE running the TACACS+ server. Select the Type of TACACS+ authentication types (ASCII/PAP/CHAP/MS-CHAP) as appropriate and match the TACACS+ server.



TACACS+ Servers

Access Order	IP Address/Hostname	Port	Authentication Type
1	192.168.56.6	49	MS-CHAP

Modify TACACS+ Server

IP address/hostname: 192.168.56.6

Type of TACACS+ authentication: MS-CHAP

Warning: No security protocol is activated.

Port: 49

Enable Accounting:

Timeout: 10

Retries: 3

Shared secret: [Redacted]

Confirm shared secret: [Redacted]

Test Connection

Note: TACACS+ authenticated users will see units from Default Preferences.

3. Create Roles with appropriate permissions by accessing User Management > Roles > and clicking on

Add Role 

New Role

Settings

Role name: PDU\_Admin

Description: [Empty]

Privileges

Select privilege to add to role. Be aware some privileges may require additional arguments.

Acknowledge Alarms

Administrator Privileges

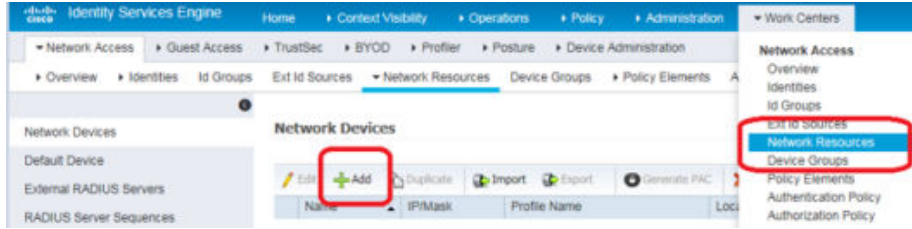
Change Asset Strip Configuration

► *Configure Cisco ISE:*

**Add the Xerus device to Cisco ISE server:**

1. Access Cisco ISE Web URL <https://x.x.x.x/admin> and log in with administrative credentials.
2. Select Access Work Centers tab > Network Access > Network Resources. On Network Devices click


 Add

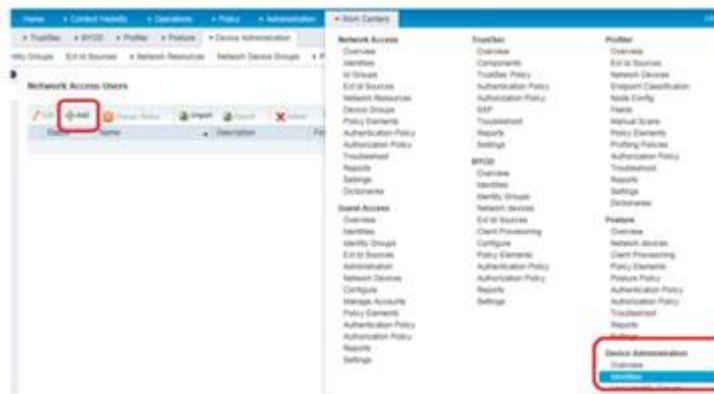


3. Configure Name, Description, IP Address/Range, enable the TACACS Authentication Settings option, set Shared secret, and click Submit to save changes. Be sure to enable Enable Single Connect Mode option and select the TACACS Draft Compliance Single Connect Support radio button.

### Create/Edit Users:

Note: If your environment already has user accounts or configured with external identity source (AD/ LDAP), you may skip this step.

1. Access Work Centers > Device Administration > Identities > and click  to add a user.



Network Access Users List - Overview

**Network Access User**

Name:

Status:  Enabled

Email:

**Passwords**

Password Type: Internal Users

**User Information**

First Name:

Last Name:

**Account Options**

Description:

Change password on next login:


**Account Disable Policy**

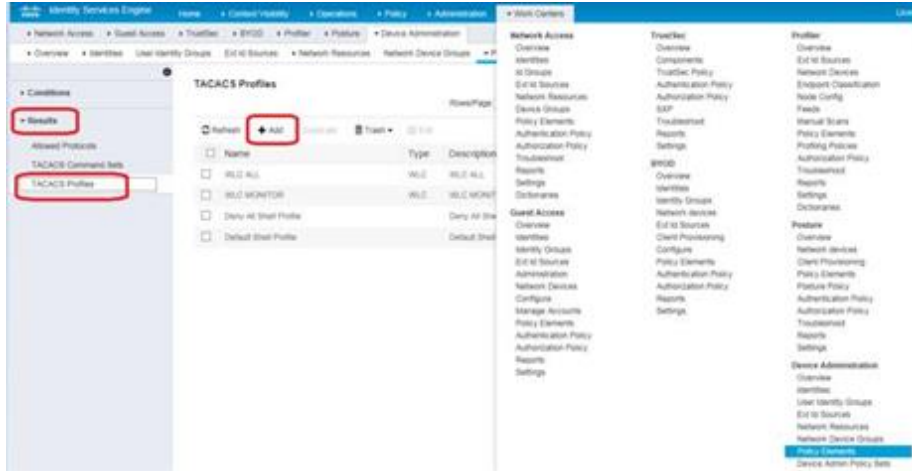
Disable account if date exceeds:


**User Groups**


### Create TACACS Profile Policy Element:

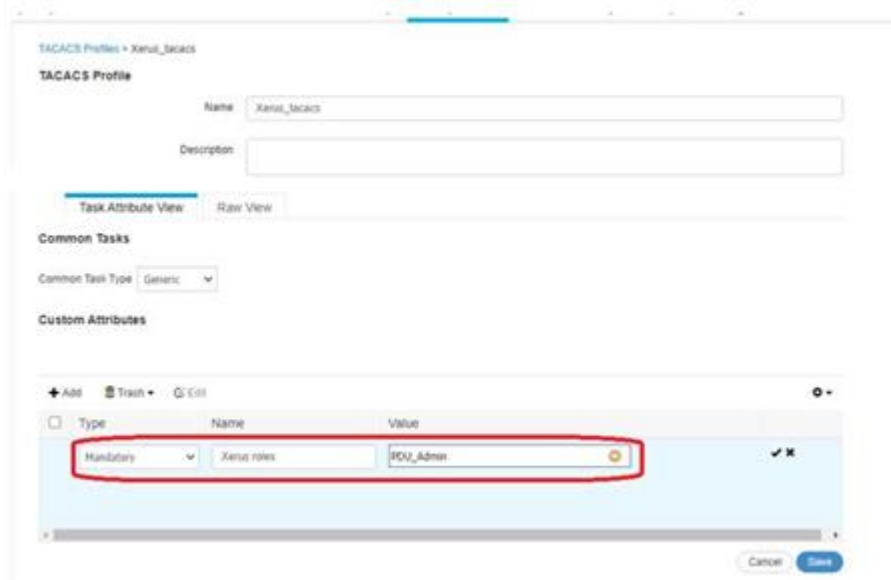
1. On Access Work Centers tab>select Device Administration > Policy Elements > Results >TACACS

Profiles and click  to add a profile.



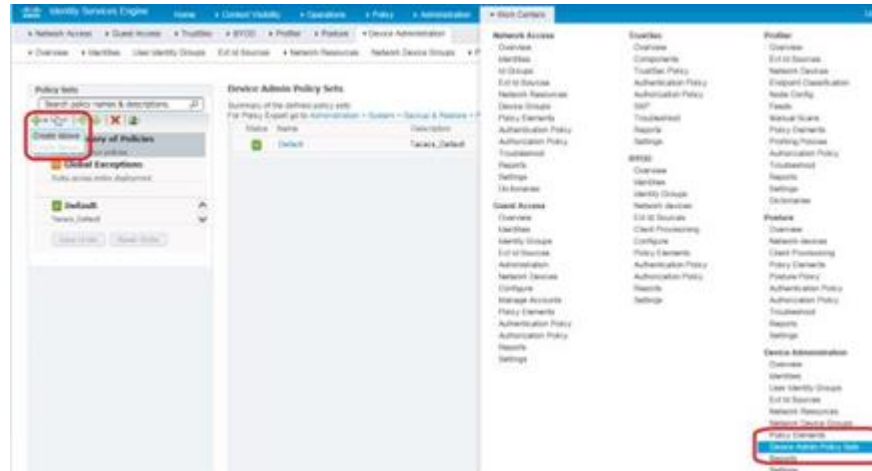
2. Enter Policy Name and click  under Custom Attributes section. Then, from the Type drop-down, select option Mandatory, Attribute Name as Xerus:roles and value PDU\_Admin where

PDU\_Admin is the role name created locally on Xerus. (Case sensitive) then Click on  to add attribute then click Submit to save changes.



### Configure/Create Device Admin Policy Set

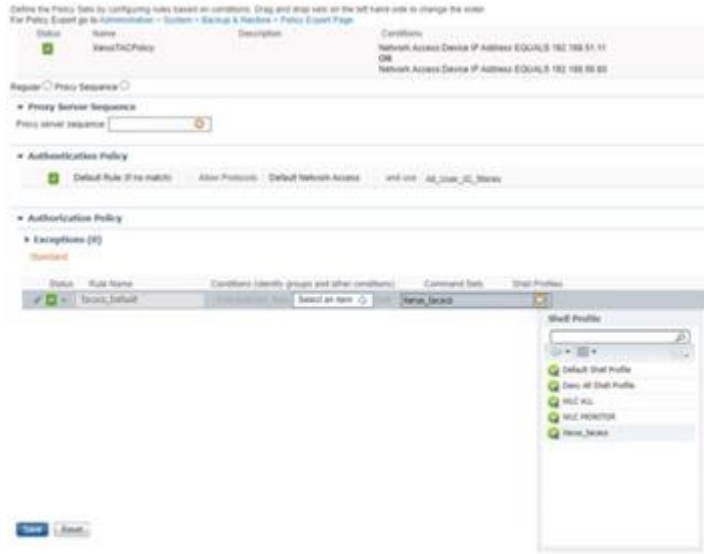
1. On the Work Centers tab, click Device Administration > Device Admin Policy Sets. Click  to create a new policy set in left pane. New Policy Set 1 will be created



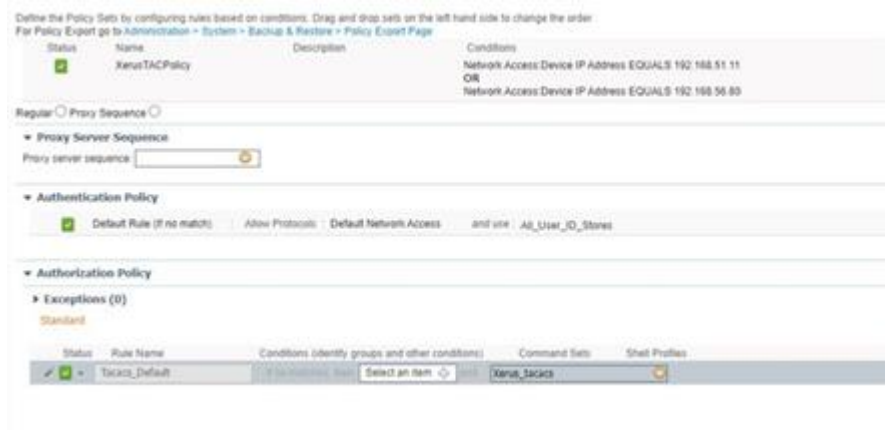
2. Click Edit, enter the Name, Description, and Condition (optional), and click Done. Authentication Policy is optional unless it is explicitly required for security guidelines.



3. Create the required Authorization Policy. Next, click Edit, specify a drop-down / under Command Sets, select the profile created earlier, and then click Done to save changes.




4. Click  or  to save changes.



► **Troubleshooting Tips**

Logs, and ISE reports are great references to troubleshoot the issues with configuration.

1. Verify from Live Logs under Operations> TACACS that the correct Authorization Policy is applied.

Click the Details icon  to see more information. Alternatively Choose Work Centers > Device Administration > Reports > ISE Reports.

Logged Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy	Group Profile	Network Device	Network Device
Sep 14, 2022 11:52:11.878 AM	Success		Xerus	Authentication	XerusTACPolicy == Default == Default	XerusTACPolicy == Tacacs_Default	Xerus_tacacs	Xerus_30	192.168.56.80
Sep 14, 2022 11:52:11.864 AM	Success		Xerus	Authentication	XerusTACPolicy == Default == Default	XerusTACPolicy == Tacacs_Default	Xerus_tacacs	Xerus_30	192.168.56.80
Sep 14, 2022 11:51:01.506 AM	Success		Xerus	Authentication	XerusTACPolicy == Default == Default	XerusTACPolicy == Tacacs_Default	Xerus_tacacs	Xerus_30	192.168.56.80
Sep 14, 2022 11:51:01.475 AM	Success		Xerus	Authentication	XerusTACPolicy == Default == Default	XerusTACPolicy == Tacacs_Default	Xerus_tacacs	Xerus_30	192.168.56.80
Sep 14, 2022 11:50:34.373 AM	Success		Xerus	Authentication	XerusTACPolicy == Default == Default	XerusTACPolicy == Tacacs_Default	Xerus_tacacs	Xerus_30	192.168.56.80
Sep 14, 2022 11:50:34.327 AM	Success		Xerus	Authentication	XerusTACPolicy == Default == Default	XerusTACPolicy == Tacacs_Default	Xerus_tacacs	Xerus_30	192.168.56.80
Sep 14, 2022 11:49:38.125 AM	Success		Xerus	Authentication	XerusTACPolicy == Default == Default	XerusTACPolicy == Tacacs_Default	Xerus_tacacs	Xerus_30	192.168.56.80
Sep 14, 2022 11:49:38.111 AM	Success		Xerus	Authentication	XerusTACPolicy == Default == Default	XerusTACPolicy == Tacacs_Default	Xerus_tacacs	Xerus_30	192.168.56.80

2. User authorization may fail on Xerus if an incorrect policy is applied, considering the following options.
- Moving policy higher up in the order (in case of multiple policy sets).
  - More appropriate conditions in policy coupled with device type and location when adding Xerus as a network device in Cisco ISE.

## Updating the LDAP Schema

### In This Chapter

Returning User Group Information. . . . .	488
Setting the Registry to Permit Write Operations to the Schema. . . . .	488
Creating a New Attribute. . . . .	489
Adding Attributes to the Class. . . . .	490
Updating the Schema Cache. . . . .	492
Editing rciusergroup Attributes for User Members. . . . .	492

### Returning User Group Information

Use the information in this section to return User Group information (and assist with authorization) once authentication is successful.

#### From LDAP/LDAPS

When an LDAP/LDAPS authentication is successful, the BCM2 determines the permissions for a given user based on the permissions of the user's . Your remote LDAP server can provide these user names by returning an attribute named as follows:

rciusergroup                      attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute.

In addition, for Microsoft® Active Directory®, the standard LDAP memberOf is used.

#### From Microsoft Active Directory

---

Note: This should be attempted only by an experienced Active Directory® administrator.

---

Returning user information from Microsoft's® Active Directory for Windows 2000® operating system server requires updating the LDAP/LDAPS schema. See your Microsoft documentation for details.

1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

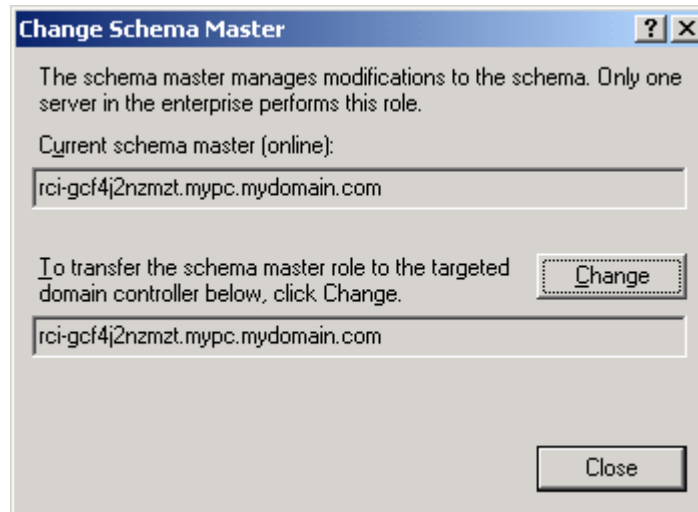
### Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.



► *To permit write operations to the schema:*

1. Right-click the Active Directory® Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.



2. Select the "Schema can be modified on this Domain Controller" checkbox. Optional
3. Click OK.

## Creating a New Attribute

► *To create new attributes for the rcigroup class:*

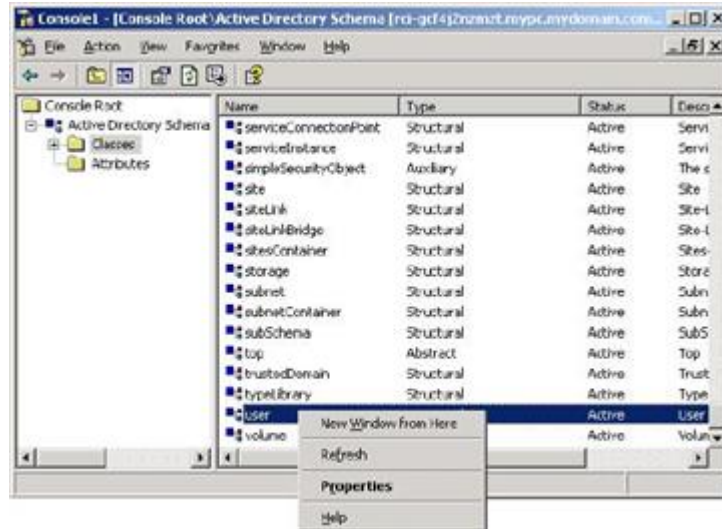
1. Click the + symbol before Active Directory® Schema in the left pane of the window.
2. Right-click Attributes in the left pane.
3. Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.

4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
9. Type *1* in the Minimum field.
10. Type *24* in the Maximum field.
11. Click OK to create the new attribute.

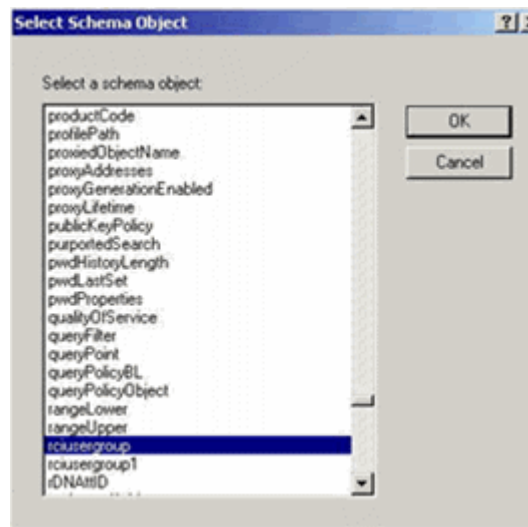
## Adding Attributes to the Class

### ► *To add attributes to the class:*

1. Click Classes in the left pane of the window.
2. Scroll to the user class in the right pane and right-click it.



3. Choose Properties from the menu. The user Properties dialog appears.
4. Click the Attributes tab to open it.
5. Click Add.
6. Choose rcusergroup from the Select Schema Object list.



7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

## Updating the Schema Cache

► *To update the schema cache:*

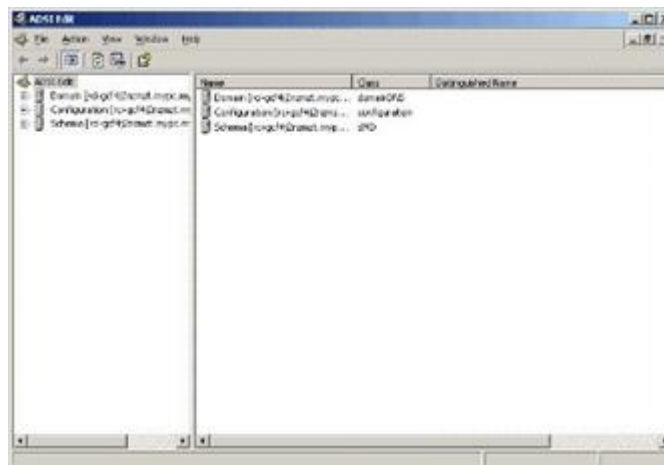
1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

## Editing rcusergroup Attributes for User Members

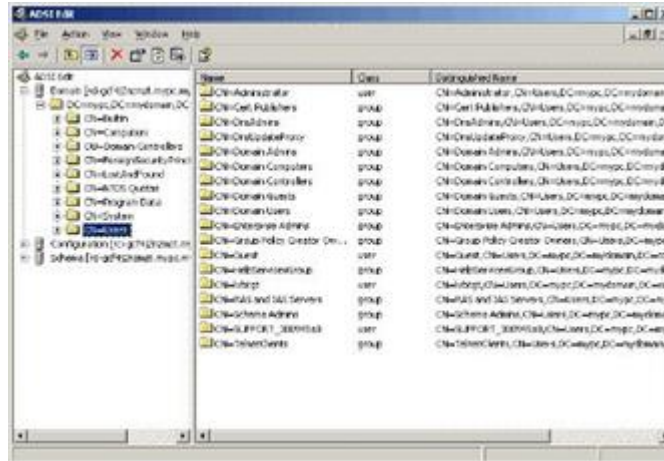
To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

► *To edit the individual user attributes within the group rcusergroup:*

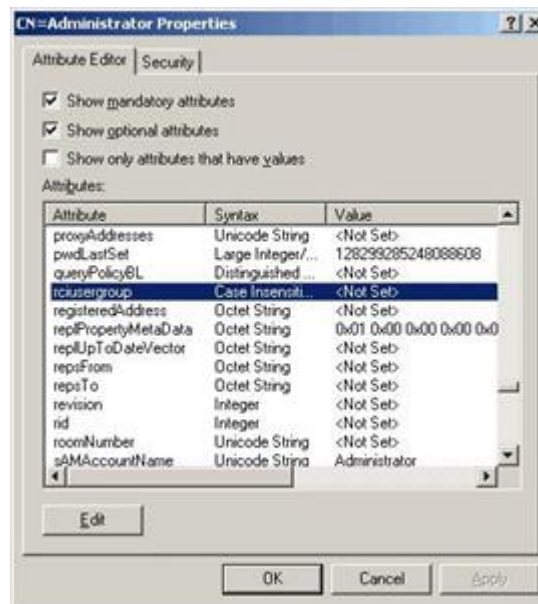
1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.
3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.



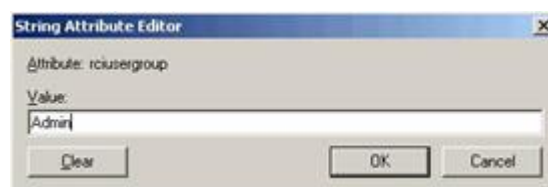
4. Open the Domain.
5. In the left pane of the window, select the CN=Users folder.



6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.
7. Click the Attribute Editor tab if it is not already open. Choose rcusergroup from the Attributes list.



8. Click Edit. The String Attribute Editor dialog appears.
9. Type the user (created in the BCM2) in the Edit Attribute field. Click OK.



## Additional Xerus Information - Assorted Products

### In This Chapter

Reserving IP Addresses in DHCP Servers. . . . .	494
Sensor Threshold Settings. . . . .	496
Default Voltage and Current Thresholds. . . . .	503
Altitude Correction Factors. . . . .	504
Unbalanced Current Calculation. . . . .	505
Ways to Probe Existing User Profiles. . . . .	506
Role of a DNS Server. . . . .	506
Installing the USB-to-Serial Driver (Optional). . . . .	506
Device-Specific Settings. . . . .	507
TLS Certificate Chain. . . . .	508

### Reserving IP Addresses in DHCP Servers

Xerus uses the product serial number as the client identifier in the DHCP request. To successfully reserve an IP address in a DHCP server, use the device's serial number as the unique ID instead of the MAC address.

Since all network interfaces can be simultaneously enabled and configured with diverse static IP addresses, the client identifier of each network interface is different. The main difference is the absence/presence of a suffix, which is the interface name added to the end of the serial number. The table below lists the client identifiers of all network interfaces.

Interface	Client identifier
ETH1	serial number
ETH2	serial number plus the uppercase suffix "-ETH2"
WIRELESS	serial number plus the uppercase suffix "-WIRELESS"
BRIDGE	serial number

You can reserve the IP addresses of more than one interfaces in the DHCP server if preferred. Note that you must choose/configure the bridge interface if your device is set to the bridging mode.

---

**Important: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.**

---

### Reserving IP in Windows

To reserve the IP address of any network interface in the Windows DHCP server, you must convert that interface's client identifier into *hexadecimal* ASCII codes.

In the following illustration, it is assumed that the serial number is PEG1A00003.

► *Windows IP address reservation illustration:*

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETH1	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH2	PEG1A00003-ETH2 = 50 45 47 31 41 30 30 30 30 33 2D 45 54 48 32 <ul style="list-style-type: none"> <li>• The suffix comprising the dash symbol and the word "ETH2" is also converted.</li> </ul>
WIRELESS	PEG1A00003-WIRELESS = 50 45 47 31 41 30 30 30 30 33 2D 57 49 52 45 4C 45 53 53 <ul style="list-style-type: none"> <li>• The suffix comprising the dash symbol and the word "WIRELESS" is also converted.</li> </ul>
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. In your DHCP server, go to the New Reservation dialog, and enter the converted ASCII codes without spaces.

For example, to reserve the ETH1 interface's IP address, enter the following data in the dialog.

Field	Data entered
IP address	The IP address you want to reserve.
MAC address	The following ASCII codes. 50454731413030303033
Other fields	Configure as needed.

## Reserving IP in Linux

There are two methods to reserve the IP address of any network interface in the standard Linux DHCP server (ISC DHCP server):

- Convert an interface's client identifier into *hexadecimal* ASCII codes.
- Use an interface's original client identifier without converting it into ASCII codes.

In the following illustrations, it is assumed that the BCM2 serial number is PEG1A00003, and the IP address you want to reserve is 192.168.20.1.

► *Illustration with ASCII code conversion:*

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETH1	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH2	PEG1A00003-ETH2 = 50 45 47 31 41 30 30 30 30 33 2D 45 54 48 32 <ul style="list-style-type: none"> <li>• The suffix comprising the dash symbol and the word "ETH2" is also converted.</li> </ul>

Interface	Client identifier conversion
WIRELESS	PEG1A00003-WIRELESS = 50 45 47 31 41 30 30 30 30 33 2D 57 49 52 45 4C 45 53 53 <ul style="list-style-type: none"> <li>The suffix comprising the dash symbol and the word "WIRELESS" is also converted.</li> </ul>
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. Separate the converted ASCII codes with a colon, and a prefix "00:" must be added to the beginning of the converted codes.

For example, the *converted* client identifier of the ETH1 interface looks like the following:

```
00:50:45:47:31:41:30:30:30:30:33
```

3. Now enter the converted client identifier with the following syntax.

```
host mypx {
option dhcp-client-identifier = 00:50:45:47:31:41:30:30:30:30:33;
fixed-address 192.168.20.1;
}
```

► *Illustration without ASCII code conversion:*

1. Use the original client identifier of the desired network interface. DO NOT convert them into ASCII codes.
2. A prefix "\000" must be added to the beginning of the client identifier.

For example, the client identifier of the ETH1 interface looks like the following:

```
\000PEG1A00003
```

3. Now enter the original client identifier with the following syntax. The client identifier is enclosed in quotation marks.

```
host mypx {
option dhcp-client-identifier = "\000PEG1A00003";
fixed-address 192.168.20.1;
}
```

## Sensor Threshold Settings

This section explains the thresholds settings for a numeric sensor.

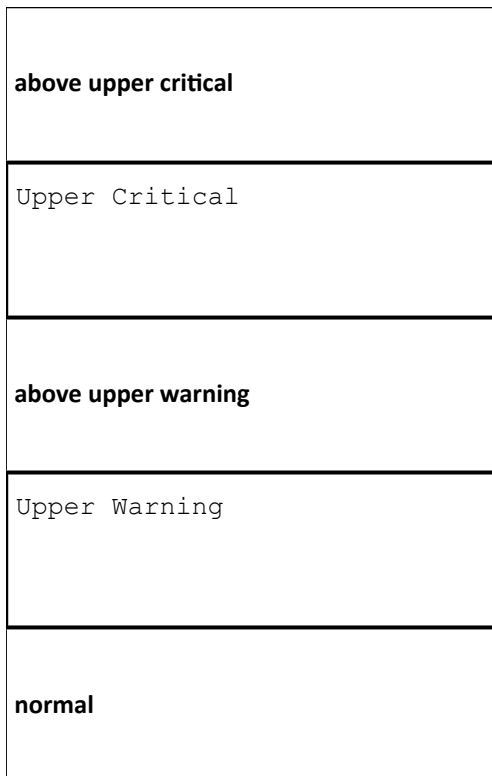


Lower critical	<input checked="" type="checkbox"/>	10	
Lower warning	<input checked="" type="checkbox"/>	20	
Upper warning	<input checked="" type="checkbox"/>	30	
Upper critical	<input checked="" type="checkbox"/>	40	
Deassertion hysteresis		1	
Assertion timeout		0	Samples

## Thresholds and Sensor States

A numeric sensor has four thresholds: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

The threshold settings determine how many sensor states are available for a certain sensor and the range of each sensor state. The diagram below shows how each threshold relates to each state.



Lower Warning
<b>below lower warning</b>
Lower Critical
<b>below lower critical</b>

► *Available sensor states:*

The more thresholds are enabled for a sensor, the more sensor states are available for it. The "normal" state is always available regardless of whether any threshold is enabled.

For example:

- When a sensor only has the Upper Critical threshold enabled, it has two sensor states: normal and above upper critical.
- When a sensor has both the Upper Critical and Upper Warning thresholds enabled, it has three sensor states: normal, above upper warning, and above upper critical.

States of "above upper warning" and "below lower warning" are warning states to call for your attention.

States of "above upper critical" and "below lower critical" are critical states that require you to immediately handle.

► *Range of each available sensor state:*

The value of each enabled threshold determines the reading range of each available sensor state.

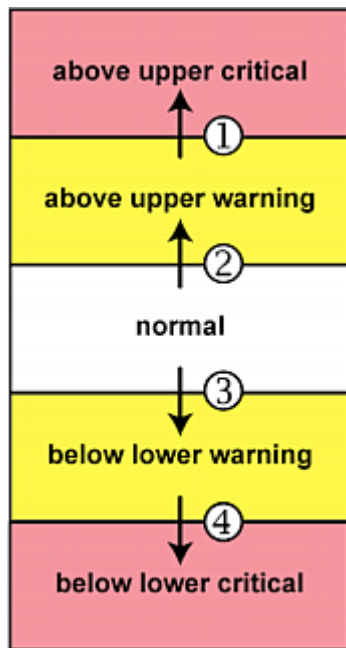
### "To Assert" and Assertion Timeout

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

► *To assert a state:*

To assert a state is to announce a new, "worse" state.

Below are bad state changes that cause the BCM2 to assert.



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

► *Assertion Timeout:*

Lower Critical	<input checked="" type="checkbox"/>	0	
Lower Warning	<input checked="" type="checkbox"/>	0	
Upper Warning	<input checked="" type="checkbox"/>	0	
Upper Critical	<input checked="" type="checkbox"/>	0	
Deassertion Hysteresis		0	
Assertion Timeout		0	Samples

In the threshold settings, the Assertion Timeout field postpones the "assertion" action. It determines how long a sensor must remain in the "worse" new state before the BCM2 triggers the "assertion" action. If that sensor changes its state again within the specified wait time, the BCM2 does NOT assert the worse state.

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

---

Note: For most sensors, the measurement unit in the "Assertion Timeout" field is sample. Sensors are measured every second, so the timing of a sample is equal to a second. Raritan's BCM2 is an exception to this, with a sample of 3 seconds.

---

► *How "Assertion Timeout" is helpful:*

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

### Assertion Timeout Example for Temperature Sensors

*Assumption:*

```
Upper Warning threshold is enabled.  
Upper Warning = 25 (degrees Celsius)  
Assertion Timeout = 5 samples (that is, 5 seconds)
```

When a temperature sensor's reading exceeds 25 degrees Celsius, moving from the "normal" range to the "above upper warning" range, the BCM2 does NOT immediately announce this warning state. Instead it waits for 5 seconds, and then does either of the following:

- If the temperature remains above 25 degrees Celsius in the "above upper warning" range for 5 seconds, the BCM2 performs the "assertion" action to announce the "above upper warning" state.
- If the temperature drops below 25 degrees Celsius within 5 seconds, the BCM2 does NOT perform the "assertion" action.

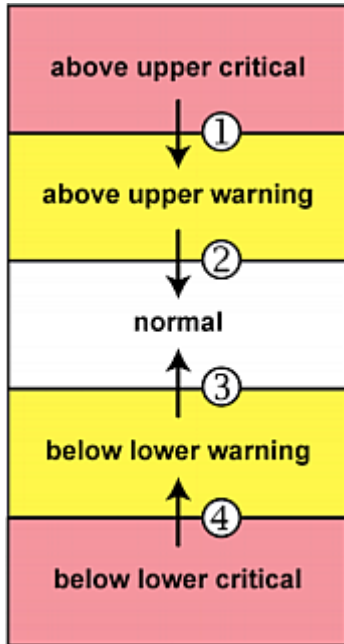
### "To De-assert" and Deassertion Hysteresis

After the BCM2 asserts a worse state for a sensor, it may de-assert that state later on if the readings improve.

► *To de-assert a state:*

To de-assert a state is to announce the end of the previously-asserted worse state.

Below are good state changes that cause the BCM2 to de-assert the previous state.



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

► *Deassertion Hysteresis:*

Lower Critical	<input checked="" type="checkbox"/>	0	
Lower Warning	<input checked="" type="checkbox"/>	0	
Upper Warning	<input checked="" type="checkbox"/>	0	
Upper Critical	<input checked="" type="checkbox"/>	0	
<b>Deassertion Hysteresis</b>		0	
Assertion Timeout		0	Samples

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

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

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

For example, if Deassertion Hysteresis = 2, then the deassertion level of each threshold is either "+2" or "-2" as illustrated below.

Threshold value	Deassertion value
Upper Critical = 33	Deassertion level = 31 <ul style="list-style-type: none"> <li>• <math>33 - 2 = 31</math></li> </ul>
Upper Warning = 25	Deassertion level = 23 <ul style="list-style-type: none"> <li>• <math>25 - 2 = 23</math></li> </ul>
Lower Critical = 10	Deassertion level = 12 <ul style="list-style-type: none"> <li>• <math>10 + 2 = 12</math></li> </ul>
Lower Warning = 18	Deassertion level = 20 <ul style="list-style-type: none"> <li>• <math>18 + 2 = 20</math></li> </ul>

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

---

Note: The difference between Upper Warning and Lower Warning must be at least "two times" of the deassertion value.

---

► *How "Deassertion Hysteresis" is helpful:*

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

### Deassertion Hysteresis Example for Temperature Sensors

*Assumption:*

```
Upper Warning threshold is enabled.
Upper Warning = 20 (degrees Celsius)
Deassertion Hysteresis = 3 (degrees Celsius)
"Deassertion" level = 20-3 = 17 (degrees Celsius)
```

When the BCM2 detects that a temperature sensor's reading drops below 20 degrees Celsius, moving from the "above upper warning" range to the "normal" range, either of the following may occur:

- If the temperature falls between 20 and 17 degrees Celsius, the BCM2 does NOT perform the "deassertion" action.
- If the temperature drops to 17 degrees Celsius or lower, the BCM2 performs the "deassertion" action to announce the end of the "above upper warning" state.

## Default Voltage and Current Thresholds

The following are factory-default voltage and current thresholds. There are no default values set for *lower* current thresholds because lower thresholds are not useful.

Availability of diverse thresholds depends on the capability of the model you purchased.

### ► *Single-phase inlets or outlets:*

- RMS voltage:

Threshold	Default value
Lower critical	-6% of minimum rating
Lower warning	-3% of minimum rating
Upper warning	+3% of maximum rating
Upper critical	+6% of maximum rating
Hysteresis	2V

- RMS current:

Threshold	Default value
Upper warning	65% of rating
Upper critical	80% of rating
Hysteresis	1A

### ► *Multi-phase inlets or outlets:*

- Line-Line RMS voltage:

Threshold	Default value
Lower critical	-6% of minimum rating
Lower warning	-3% of minimum rating
Upper warning	+3% of maximum rating

Threshold	Default value
Upper critical	+6% of maximum rating
Hysteresis	2V

- Line RMS current:

Threshold	Default value
Upper warning	65% of rating
Upper critical	80% of rating
Hysteresis	1A

- Unbalanced current:

Threshold	Default value
Upper critical	10% -- disabled by default
Upper warning	5% -- disabled by default
Hysteresis	2%

► *Overcurrent protectors which aims to protect the PDU's outlets:*

- OCP RMS current:

Threshold	Default value
Upper critical	80% of OCP rating
Upper warning	65% of OCP rating
Hysteresis	1A

► *Total residual current:*

<i>Threshold</i>	<i>Default value</i>
<i>Upper critical</i>	<i>30mA</i>
<i>Hysteresis</i>	<i>15mA</i>

## 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

## Unbalanced Current Calculation

Unbalanced current information is available on 3-phase models only. This section explains how BCM2 calculates the unbalanced current percentage.

### ► Calculation:

1. Calculate the average current of all 3 lines.

$$\text{Average current} = (L1+L2+L3) / 3$$

2. Calculate each line's current unbalance by having each line current subtracted and divided with the average current.

$$L1 \text{ current unbalance} = (L1 - \text{average current}) / \text{average current}$$

$$L2 \text{ current unbalance} = (L2 - \text{average current}) / \text{average current}$$

$$L3 \text{ current unbalance} = (L3 - \text{average current}) / \text{average current}$$

3. Determine the maximum absolute value among three lines' current unbalance values.

$$\text{Maximum} (|L1 \text{ current unbalance}|, |L2 \text{ current unbalance}|, |L3 \text{ current unbalance}|)$$

4. Convert the maximum value to a percentage.

$$\text{Unbalanced load percent} = 100 * \text{maximum current unbalance}$$

### ► Example:

- Each line's current:  
L1 = 5.5 amps  
L2 = 5.2 amps

L3 = 4.0 amps

- Average current:  $(5.5+5.2+4.0) / 3 = 4.9$  amps
- L1 current unbalance:  $(5.5 - 4.9) / 4.9 = 0.1224$
- L2 current unbalance:  $(5.2 - 4.9) / 4.9 = 0.0612$
- L3 current unbalance:  $(4.0 - 4.9) / 4.9 = -0.1837$
- Maximum current unbalance:  
Maximum ( $|0.1224|$ ,  $|0.0612|$ ,  $|-0.1837|$ ) = 0.1837
- Current unbalance converted to a percentage:  
 $100 * (0.1837) = 18\%$

## Ways to Probe Existing User Profiles

This section indicates available ways to query existing user accounts on the BCM2.

- With SNMP v3 activated, you get the "user unknown" error when the user name used to authenticate does not exist.
- Any user with the permission to view event rules can query all local existing users via JSON RPC.
- Any user with the permission to view the event log may get information about existing users from the log entries.
- Any authenticated users can query currently-existing connection sessions, including Webcam-Live-Preview sessions, which show a list of associated user names.

## Role of a DNS Server

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

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

For information on external authentication, see Setting Up External Authentication.

## Installing the USB-to-Serial Driver (Optional)

The BCM2 can emulate a USB-to-serial converter over a USB connection. A USB-to-serial driver named "Dominion PX2 Serial Console" is required for Microsoft® Windows® operating systems.

Download the Windows driver for USB serial console from the Raritan website's *Support page* ([www.raritan.com/support](http://www.raritan.com/support)). The downloaded driver's name is *dominion-serial-setup-<n>.exe*, where <n> represents the file's version number.

There are two ways to install this driver: automatic and manual installation. Automatic driver installation is highly recommended.

► *Automatic driver installation in Windows® :*

1. Make sure the BCM2 is NOT connected to the computer via a USB cable.
2. Run `dominion-serial-setup-<n>.exe` on the computer and follow online instructions to install the driver.

---

*Note: If any Windows security warning appears, accept it to continue the installation.*

---

3. Connect the BCM2 to the computer via a USB cable. The driver is automatically installed.

► *Manual driver installation in Windows® :*

1. Make sure the BCM2 has been connected to the computer via a USB cable.
2. The computer detects the new device and the "Found New Hardware Wizard" dialog appears.
  - If this dialog does not appear, choose Control Panel > System > Hardware > Device Manager, right-click the *Dominion PX2 Serial Console*, and choose Update Driver.
3. Select the option of driver installation from a specific location, and then specify the location where both *dominion-serial.inf* and *dominion-serial.cat* are stored.

---

*Note: If any Windows security warning appears, accept it to continue the installation.*

---

4. Wait until the installation is complete.

---

Note: If the BCM2 enters the disaster recovery mode when the USB serial driver is not installed yet, it may be shown as a 'GPS camera' in the Device Manager on the computer connected to it.

---

► *In Linux:*

No additional drivers are required, but you must provide the name of the tty device, which can be found in the output of the "dmesg" after connecting the BCM2 to the computer. Usually the tty device is `"/dev/ttyACM#" or "/dev/ttyUSB#,"` where # is an integer number.

For example, if you are using the kermit terminal program, and the tty device is `"/dev/ttyACM0,"` perform the following commands:

```
> set line /dev/ttyACM0
```

```
> Connect
```

## Device-Specific Settings

A bulk configuration file will NOT contain any device-specific information like the following list.

For further information, simply open the built-in bulk profile for a detailed list of 'excluded' settings.

- Device name
- SNMP system name, contact and location
- Part of network settings (IP address, gateway, netmask and so on)
- Device logs
- Names, states and values of environmental sensors and actuators
- TLS certificate
- Server monitoring entries
- Asset strip names and rack unit names
- Outlet names and states

## TLS Certificate Chain

A TLS server sends out a certificate to any client attempting to connect to it. The receiver determines whether a TLS server can be trusted by verifying that server's certificate, using the certificate (chain) stored on the receiver.

Therefore, to successfully connect to a TLS server, you must upload a valid certificate or (partial) certificate chain to the receiver.

The uploaded certificate (chain) must contain all missing certificates "related to" that TLS server's certificate in some way. Otherwise, the connection made to that TLS server will fail.

- For information on how the uploaded certificate (chain) is related to a TLS server's certificate, see *What is a Certificate Chain* (on page ).
- For an example of creating and uploading a TLS certificate to BCM2, see *Illustration - GMAIL SMTP Certificate Chain* (on page ).

## What is a Certificate Chain

---



---

If you are familiar with a certificate chain, you can ignore this topic and refer to *Illustration - GMAIL SMTP Certificate Chain* (on page ).

---



---

A certificate or a chain of certificates is used for trusting a TLS server that you want to connect.

The receiver, such as BCM2, can trust a TLS server only after an appropriate certificate (chain) which is "related to" that TLS server's certificate is uploaded to the receiver.

### ► *How a certificate chain is generated:*

To explain how a TLS server's certificate is "related to" the certificate (chain) that is uploaded to the receiver, we assume that there are three "related" certificates.

- Certificate C. The certificate issued to the TLS server you want to connect.  
'Certificate C' is issued by the certificate authority (CA) entity called 'Issuer B'.
- Certificate B. The certificate issued to 'Issuer B'.

'Certificate B' is issued by a CA entity called 'Issuer A', and it is an intermediate certificate.

- Certificate A. The self-signed certificate issued by Issuer A. Issuer A is a root CA.

The above three certificates form a certificate path, which is called the "certificate chain".



Each certificate in the chain is the issuer certificate of the certificate that follows it. That is, A is the issuer certificate of B, and B is the issuer certificate of C.

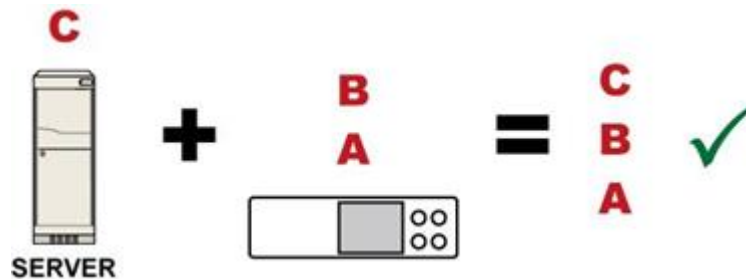
---

Note: In fact many certificate chains may comprise only the root certificate and a TLS server's certificate and do not have any intermediate certificate(s) like 'Certificate B' involved. Or some chains may contain more than one intermediate certificates.

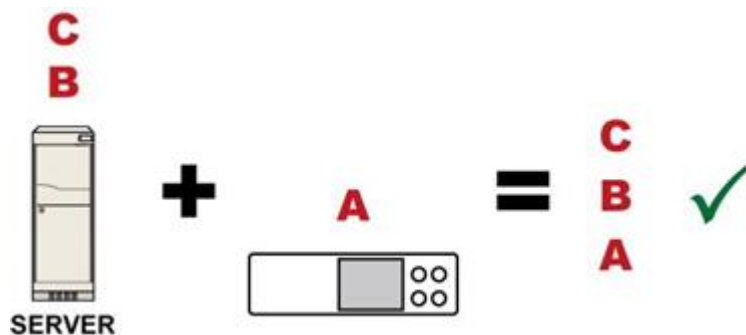
---

► *Certificate (chain) that you must upload to the receiver, such as BCM2:*

Because the TLS server provides only 'Certificate C', you need to upload a file containing the missing certificates of the chain (that is, 'Certificate A' and 'Certificate B') to the receiver.



In reality some servers may provide a partial (or even a full) certificate chain instead of a single server certificate. If your server provides a partial certificate chain containing 'Certificate B' and 'Certificate C', then you only need to upload 'Certificate A' to the receiver. If the server has a full certificate chain containing Certificates 'A', 'B', and 'C', then you also need to upload the root certificate 'A'.

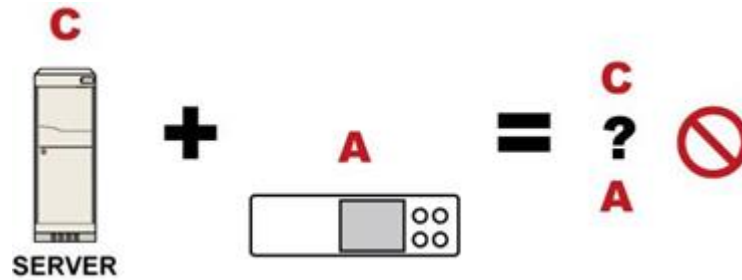


---

Warning: The certificate (chain) uploaded to the receiver must always contain the ROOT certificate even though the TLS server provides the root certificate. When uploading a (partial) chain onto the BCM2, it means you trust each certificate in the chain to certify the authenticity of certificates a server sends to BCM2. Therefore, at least the root certificate must be authentic, issued by a CA you trust, and downloaded from that CA over a secure channel. Never implicitly trust a root certificate that is sent by the server which you want to connect to. It could have been created by an attacker.

---

If either certificate 'A' or 'B' is missing in the certificate file uploaded to the receiver, the connection to the wanted TLS server will fail.



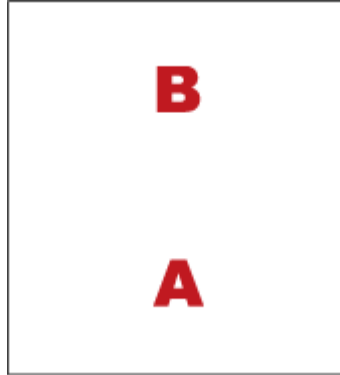
For BCM2, if any required certificate is missing, a certificate error message similar to the following is shown on the BCM2 web interface.



It is NOT recommended to upload the server certificate to the receiver except when it is a self-signed certificate. Using self-signed server certificates is also not recommended and may not even work in all cases.

► *Order of the chain in the certificate file:*

The order of a certificate chain's content in the certificate file uploaded to the receiver must look like the following.



- The top is the final intermediate certificate of the chain "B" if you have to upload a partial chain.
- The bottom is always the root certificate "A".
- When copying multiple certificates to a single file, make sure you also copy the lines of BEGIN CERTIFICATE and END CERTIFICATE from each certificate.

## Illustration - GMAIL SMTP Certificate Chain

---

---

If you will apply your company's SMTP service to BCM2, ignore this GMAIL illustration topic. Simply contact your IT department to retrieve the appropriate certificate (chain) file and upload it to the BCM2.

---

---

This section illustrates the upload of a TLS "root" certificate for using the "gmail.com" SMTP service.

Unlike normal TLS websites, where you can easily find its server certificate by using a Web browser, the method to find an SMTP server's certificate is more difficult, which requires appropriate tools and sufficient technical knowledge. For example, you may have to use the openssl command as illustrated below to retrieve the certificate of the GMAIL SMTP server.

► **Step 1 -- Find the certificate(s) the SMTP server has:**

1. Issue the following command in the appropriate command line application.
  - In the following example command, we assume the server "smtp.gmail.com" provides the SMTP service. You can change the server name, port number, command or even the tool as needed.

```
openssl s_client -showcerts -connect smtp.gmail.com:465
```

---

*Alternative: To view the certificate chain instead of all certificates, you can remove the "-showcerts" option from the above command.*

---

1. Information that shows the certificates the SMTP server has is displayed.

```
.  
. .  
Certificate chain  
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=smtp.gmail.com
```

```

i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIEdjCCA16gAwIBAgIIbzO9vIL2OXcwDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
.
.
YHKKJH96sSNC+6dLpOOoRritL5z+jn2WFLcQkL2mRoWQi6pYTzPyXB4D
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIIEKDCCAxCGAwIBAgIQAhJYiw+lmnd+8Fe2Yn3zANBgkqhkiG9w0BAQsFADEBC
.
.
MqO5tzHpCvX2HzLc
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDftCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
.
.
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=sntp.gmail.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
.
.
.

```

2. Onscreen information under the title 'Certificate chain' indicates that there are three issuers and three certificates on this server.
  - Each line beginning with the letter "i" indicates an issuer. They are:



- *Google Internet Authority G2*
  - *GeoTrust Global CA*
  - *Equifax Secure Certificate Authority*
  - Each certificate begins with the line "BEGIN CERTIFICATE" and ends with the line "END CERTIFICATE".
  - The topmost certificate is the server certificate.
3. The section titled "Server certificate" indicates that the issuer (CA) *Google Internet Authority G2* issues the server certificate.
  4. As the server has the server certificate and two intermediate certificates, we conclude that this server sends a partial certificate chain to the receiver.
  5. Check whether the issuer "Equifax Secure Certificate Authority" is the root CA.
    - If yes, you only need to upload the root certificate self-signed by *Equifax Secure Certificate Authority* to BCM2.
    - If not, you need to find all missing issuer certificates, including the root certificate, and upload them to BCM2.

► *Step 2 -- Find and download the content of missing issuer certificate(s):*

1. View the name of the issuer (CA) at the bottom. In this example, this issuer is 'Equifax Secure Certificate Authority'.
2. Use the issuer's name 'Equifax Secure Certificate Authority' to search for its certificate on the Internet, and then download or copy the content from an authentic source, which is usually its official website.

---

*Important: To prevent the downloaded certificate from being modified or manipulated, you must secure the download with TLS via a trusted certificate.*

---

3. As it is found the Equifax Secure Certificate Authority's certificate is self signed by 'Equifax Secure Certificate Authority', which indicates it is the root CA, there are no more missing certificates to search for.

► *Step 3 -- Upload the missing certificate(s) to BCM2:*

1. Paste the root certificate's content into a plain text file that will be uploaded to BCM2.
  - Content copying must include the lines of "BEGIN CERTIFICATE" and "END CERTIFICATE".
2. Save that file as a *.pem*, *.crt* or *.cer* file. In this example, it is named as "my-root.pem."
3. Upload the file "my-root.pem" to BCM2 for using the GMAIL SMTP service.

---

Note: If your SMTP server requires the upload of a certificate file comprising multiple certificates, make sure the order of these certificates is correct in the file. See *What is a Certificate Chain* (on page ).

---

► **IMPORTANT NOTE:**

If your SMTP server provides a full certificate chain, you should be suspicious whether any attacker fakes the certificate chain and doubt whether the root certificate on that server is authentic. It is **STRONGLY** recommended to download the root certificate from an authentic source, which is usually the root CA's website, rather than from the server you want to connect.

### Xerus Product Integration

This section contains information about possible integrations of Xerus products with other Legrand, Raritan, Server Technology, or third-party products to provide diverse power solutions. Not all Xerus products support all integrations.

## Connecting a PDU to a Dominion KVM or Serial Device

Some Xerus- firmware PDUs can be integrated with Raritan KVM or Serial devices.

► *PDU connection via Feature port (only for PX2, PX3 or PX3TS devices)*

Raritan PX series rack PDUs can be connected to the Dominion device using the D2CIM-PWR CIM.

► *To connect the rack PDU:*

1. Connect a Raritan KX3 KVM switch to the "FEATURE" port of the rack PDU using a D2CIM-PWR CIM and CAT5 cable. For example, set up as KX3 <-> CAT5 cable <-> D2CIM-PWR CIM <-> "FEATURE" port of the PX4 PDU. or set up as KX3 <-> CAT5 cable <-> D2CIM-PWR CIM <-> "FEATURE" port of the PRO4X PDU.

---

Note: PX2, PX3 or PX3TS series has RJ-45 "FEATURE" port.

---

1. Attach an AC power cord to the target server and an available rack PDU outlet.
2. Connect the rack PDU to an AC power source.
3. Power on the device.

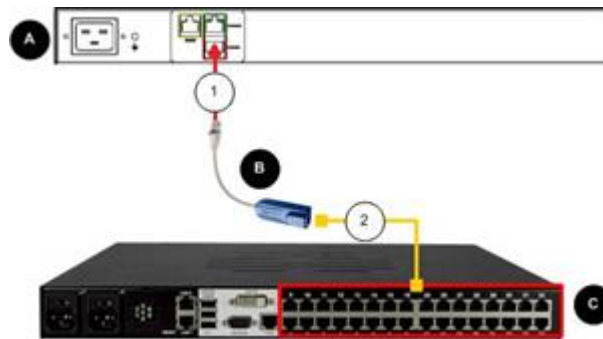







Diagram key

	Rack PDU
	D2CIM-PWR
	KX III
	D2CIM-PWR to rack PDU connection
	D2CIM-PWR to KX III target device port via Cat5 cable

► *PDU connection via USB port (only for PRO4X and PX4 devices)*

PRO3X, PRO4X and PX4 devices do not have a feature port, so the connection to a Power CIM peer can be achieved through an USB dongle (DSER-PWR-USB-G4, DKX3-PWR-USB-G4 and DSER-CLI-USB-G4) and a USB-A port. You can use SNMP protocol to communicate to the Raritan KVM or serial devices.

---

Note: Power CIM peer stands for either a Raritan KVM switch (KX2, KX3 via D2CIM-PWR) or a Raritan serial switch (SX2, KSX2).

---

► *To connect PX4 or PRO4X*

1. You can connect a Raritan KX3 KVM Switch via Power CIM DKX3-PWR-USB-G4 or via Power CIM DSER-CLI-USB-G4 for a CLI connection or Power CIM DSER-PWR-USB for a serial device. Listed here are the several ways devices can be connected via power CIMs.
  - To connect a Raritan KX3 KVM Switch to one of the PDU's USB-A ports use a CAT5 cable and a Power CIM (DKX3-PWR-USB-G4 USB dongle). For example, set up as KX3 <-> CAT5 cable <-> DKX3-PWR-USB-G4 <-> PX4 PDU USB-A or set up as KX3 <-> CAT5 cable <-> DKX3-PWR-USB-G4 <-> PRO4X PDU USB-A.
  - To connect a Raritan KX3 KVM Switch and DSAM module to one of the PDU's USB-A ports use a CAT5 cable and a Power CIM (DSER-CLI-USB-G4 dongle) For example, set up as KX3 <-> DSAM <-> CAT5 <-> DSER-CLI-USB-G4 <-> PX4 PDU USB-A or set up as KX3 <-> DSAM <-> CAT5 <-> DSER-CLI-USB-G4 <-> PRO4X PDU USB-A.
  - To connect a PC using a USB port requires a DSER-CLI-USB-G4 dongle, a USB-to-Serial adapter, and a Cisco cable. For example, set up as PC <-> USB-to-serial adapter <-> Cisco cable <-> DSER-CLI-USB-G4 <-> PX4 PDU USB-A or set up as PC <-> USB-to-serial adapter <-> Cisco cable <-> DSER-CLI-USB-G4 <-> PRO4X PDU USB-A.

► *Only for PX4*

- To connect a PC with a Serial port requires a DSER-CLI-USB-G4 dongle and a Cisco cable. For example, set up as PC serial port <-> Cisco cable <-> DSER-CLI-USB-G4 <-> PX4 PDU USB-A.
- To connect a Serial Console Server, such as the Raritan SX2 to one of the PX4's USB-A ports use a CAT5 cable and a DSER-PWR-USB-G4 USB dongle. For example, set up as Serial Console Server (such as the SX2) <-> CAT5 cable <-> DSER-PWR-USB-G4 <-> PX4 PDU USB-A.

► *Only for PRO4X*

- To access a serial device you can connect a Raritan DSAM Serial Access Module (DSAM) directly to the PRO4X PDU's USB-A port, and the serial device would then connect directly to an available RJ45 port on the DSAM module. NOTE: This functionality requires Xerus Firmware 4.0.20 or later.

1. Attach an AC power cord to the target server and an available the PDU outlet.
2. Connect the PDU to an AC power source.
3. Power on the device.

## Power IQ Configuration

Sunbird's Power IQ is a software application that collects and manages the data from different PDUs installed in your server room or data center. With this software, you can:

- Do bulk configuration for multiple PDUs
- Name outlets on different PDUs
- Switch on/off outlets on outlet-switching capable PDUs

For more information on Power IQ, refer to the Power IQ online help on the Sunbird website: <http://support.sunbirdcim.com>.

## Connecting a Modbus RTU Device or Bus

If connecting the Modbus RTU devices to Xerus PDU and enabling the Modbus Gateway feature, the Modbus TCP clients on your network will be able to communicate with those Modbus RTU devices attached to Xerus PDU.

► *To use the Modbus Gateway feature:*

1. Connect a Modbus RTU device, or a Modbus bus with multiple RTU devices, to the Xerus PDU via two adapters described below.

- a. Connect an isolated RS485-to-RS232 adapter to the Modbus RTU device or Modbus bus.
  - b. Connect an RS232-to-USB adapter (using FTDI's FT232 chip) to the RS485-to-RS232 adapter.
  - c. Connect the RS232-to-USB adapter to the USB-A port on the Xerus PDU.
2. On the Xerus PDU, enable and properly configure the Modbus Gateway feature. See Changing Modbus Settings.

► *Communications between Modbus TCP and RTU devices:*

- The Xerus PDU acts only as a message gateway for the Modbus TCP client. Messages from the Modbus TCP client(s) are passed through the Xerus PDU to the connected Modbus RTU devices or Modbus bus.
- The Modbus RTU devices on the bus are identified with their Modbus RTU addresses using the Modbus unit identifier addresses in the Modbus TCP protocol. If the Modbus TCP client does not support unit identifier addressing, refer to Changing Modbus Settings.
- The Xerus PDU supports communications to multiple Modbus RTU devices. Note that the connected Modbus RTU devices are invisible to the Xerus PDU.

## dcTrack

Sunbird's dcTrack<sup>®</sup> is a product that allows you to manage the data center. The BCM2 is categorized as a power item in dcTrack.

You can use dcTrack to:

- Record and manage the data center infrastructure and assets
- Monitor the electrical consumption of the data center
- Track environmental factors in the data center, such as temperature and humidity
- Optimize the data center growth

For more information on dcTrack, refer to the online help accessible from the dcTrack application, or user documentation available on the Sunbird's website: <http://support.sunbirdcim.com>.

## Asset Management Strips and dcTrack

If any asset strips are connected to the BCM2, the BCM2 can transmit their information to Sunbird's dcTrack. Add the BCM2 to dcTrack, and also add each IT item where an asset tag is attached to dcTrack.

If SNMP is enabled, event information can be transmitted to dcTrack. Specifically, Sunbird's Power IQ detects when an asset tag is connected or disconnected from an asset strip. Power IQ then generates a connection or disconnection event. When dcTrack polls Power IQ, the connection/disconnection events are pulled into dcTrack, and displayed in the dcTrack Web Client.

► *To poll and display asset management events in dcTrack*

- The BCM2 that the asset strip is connected to must exist in dcTrack.
- Each IT item connected to the asset strip via an asset tag must exist in dcTrack.

You do not need to manually enter the asset tag IDs for IT items that already exist in dcTrack as long as these items are in the Installed status.

Plug the item's asset tag into an asset strip that is connected to the BCM2 that exists in dcTrack. dcTrack automatically assigns the asset tag ID to the existing IT item.

## Third Party Licenses

This appendix contains third party licenses for software used by Xerus that require including the license in documentation.

For information on open source software, see [raritan.com/about-us/legal/open-source-software-statement](http://raritan.com/about-us/legal/open-source-software-statement)

## In This Chapter

Licenses - Angular. . . . .	519
Licenses - Bind9. . . . .	528
Licenses - Clish. . . . .	534
Licenses - Dropbear. . . . .	539
Licenses - FreeType. . . . .	541
Licenses - IW. . . . .	543
Licenses - JSON-C. . . . .	543
Licenses - LIBTIRPC. . . . .	544
Licenses - LIBXML2. . . . .	544
Licenses - Mbus. . . . .	544
Licenses - Net-SNMP. . . . .	545
Licenses - Open LDAP. . . . .	550
Licenses - OpenSSL. . . . .	552
Licenses - Wireless-RegDB. . . . .	553
Licenses - WPA Supplicant and Hostapd. . . . .	554

## Licenses - Angular

@angular-devkit/build-angular

MIT

The MIT License

Copyright (c) 2017 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@angular-devkit/core

MIT

The MIT License

Copyright (c) 2017 Google, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@angular/animations

MIT

@angular/cdk

MIT

The MIT License

Copyright (c) 2021 Google LLC.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.



THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@angular/common

MIT

@angular/core

MIT

@angular/forms

MIT

@angular/material

MIT

The MIT License

Copyright (c) 2021 Google LLC.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@angular/platform-browser

MIT

@angular/router

MIT

@babel/runtime

MIT

MIT License

Copyright (c) 2014-present Sebastian McKenzie and other contributors Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@ctrl/nginx-chartjs

MIT

MIT License

Copyright (c) Scott Cooper <scctcper@gmail.com>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

@ngx-translate/core

MIT

chart.js

MIT

The MIT License (MIT)

Copyright (c) 2018 Chart.js Contributors

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

core-js

MIT

Copyright (c) 2014-2021 Denis Pushkarev

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

regenerator-runtime

MIT

MIT License

Copyright (c) 2014-present, Facebook, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

rxjs

Apache-2.0

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

#### TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

##### 1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual,

worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made,

use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable

by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and

do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other

Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

#### END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[ ]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright (c) 2015-2018 Google, Inc., Netflix, Inc., Microsoft Corp. and contributors

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.

tslib

OBSD

Copyright (c) Microsoft Corporation.

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

zone.js

MIT

The MIT License

Copyright (c) 2010-2020 Google LLC. <https://angular.io/license>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Licenses - Bind9

Copyright (C) 2004-2016 Internet Systems Consortium, Inc. ("ISC")

Copyright (C) 1996-2003 Internet Software Consortium.

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions of this code release fall under one or more of the following Copyright notices. Please see individual source files for details.

For binary releases also see: OpenSSL-LICENSE.

Copyright (C) 1996-2001 Nominum, Inc.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

-----  
Copyright (C) 1995-2000 by Network Associates, Inc.

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC AND NETWORK ASSOCIATES DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

-----



Copyright (C) 2002 Stichting NLnet, Netherlands, stichting@nlnet.nl.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND STICHTING NLNET DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL STICHTING NLNET BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The development of Dynamically Loadable Zones (DLZ) for Bind 9 was conceived and contributed by Rob Butler.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ROB BUTLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ROB BUTLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

-----  
Copyright (c) 1987, 1990, 1993, 1994

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

-----  
Copyright (C) The Internet Society 2005. This version of this module is part of RFC 4178; see the RFC itself for full legal notices.

(The above copyright notice is per RFC 3978 5.6 (a), q.v.)

-----  
Copyright (c) 2004 Masarykova universita

(Masaryk University, Brno, Czech Republic)

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---

Copyright (c) 1997 - 2003 Kungliga Tekniska Hogskolan  
(Royal Institute of Technology, Stockholm, Sweden).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---

Copyright (c) 1998 Doug Rabson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright ((c)) 2002, Rice University

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* Neither the name of Rice University (RICE) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided by RICE and the contributors on an "as is" basis, without any representations or warranties of any kind, express or implied including, but not limited to, representations or warranties of non-infringement, merchantability or fitness for a particular purpose. In no event shall RICE or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

---

Copyright (c) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED "AS IS" AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---

Copyright 2000 Aaron D. Gifford. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) AND CONTRIBUTOR(S) ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) OR CONTRIBUTOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---

Copyright (c) 1998 Doug Rabson.

Copyright (c) 2001 Jake Burkholder.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

-----  
Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

-----  
Copyright (c) 1999-2000 by Nortel Networks Corporation

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NORTEL NETWORKS DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NORTEL NETWORKS BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

-----  
Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved.

By using this file, you agree to the terms and conditions set forth below.

LICENSE TERMS AND CONDITIONS

The following License Terms and Conditions apply, unless a different license is obtained from Japan Network Information Center ("JPNIC"), a Japanese association, Kokusai-Kogyo-Kanda Bldg 6F, 2-3-4 Uchi-Kanda, Chiyoda-ku, Tokyo 101-0047, Japan.

1. Use, Modification and Redistribution (including distribution of any modified or derived work) in source and/or binary forms is permitted under this License Terms and Conditions.
2. Redistribution of source code must retain the copyright notices as they appear in each source code file, this License Terms and Conditions.
3. Redistribution in binary form must reproduce the Copyright Notice, this License Terms and Conditions, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the "Copyright Notice" refers to the following language:  
"Copyright (c) 2000-2002 Japan Network Information Center. All rights reserved."
4. The name of JPNIC may not be used to endorse or promote products derived from this Software without specific prior written approval of JPNIC.
5. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY JPNIC "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL JPNIC BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

-----  
Copyright (C) 2004 Nominet, Ltd.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINET DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

-----  
Portions Copyright RSA Security Inc.

License to copy and use this software is granted provided that it is identified as "RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki)" in all material mentioning or referencing this software.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki)" in all material mentioning or referencing the derived work.

RSA Security Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

-----  
Copyright (c) 1996, David Mazieres <dm@uun.org>

Copyright (c) 2008, Damien Miller <djm@openbsd.org>

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

-----  
Copyright (c) 2000-2001 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:  
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.OpenSSL.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [licensing@OpenSSL.org](mailto:licensing@OpenSSL.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.OpenSSL.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

-----  
Copyright (c) 1995, 1997, 1998 The NetBSD Foundation, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Licenses - Clish

This package contains code which is copyrighted to multiple sources. The initial public release of this software was developed by Graeme McKerrill whilst in the employment of 3Com Europe Ltd.

Copyright (c) 2005, 3Com Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* Neither the name of 3Com Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Newport Networks Ltd.

The 0.6-0.7 releases of this software was developed by Graeme Mckerrell whilst in the employment of Newport Networks Ltd.

As well as enhancing the existing code the following new modules were developed.

Copyright (c) 2005,2006, Newport Networks Ltd

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* Neither the name of Newport Networks Ltd nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

tinycl

Yves Berquin

As of release 0.6 the tinycl library is included (unchanged) as part of the distribution.

tinycl (v2.5.1)

<http://www.sourceforge.net/projects/tinycl>

Original file by Yves Berquin.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

GNU binutils

As of release 0.7.1 libbfd can be used to resolve symbols for stacktraces. This feature can be turned off if linking with GPL code is problematic, using "configure --without-gpl".

The Binary File Descriptor library is part of GNU binutils

<http://www.gnu.org/software/binutils/>

The following file is licensed under the GPLv2.

This file is part of the CLISH project <http://clish.sourceforge.net/>

The code in this file is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2

This code is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Derived from addr2line.c in the GNU binutils package by Ulrich.Lauther@mchp.siemens.de

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.



Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

## GNU GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### END OF TERMS AND CONDITIONS

## Licenses - Dropbear

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2015 Matt Johnston

Portions copyright (c) 2004 Mihnea Stoenescu

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

=====

sshpty.c is taken from OpenSSH 3.5p1,

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

curve25519-donna:

/\* Copyright 2008, Google Inc.

\* All rights reserved.

\*

\* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

\*

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

\* curve25519-donna: Curve25519 elliptic curve, public key function

\* <http://code.google.com/p/curve25519-donna/>

\* Adam Langley <agl@imperialviolet.org>

\* Derived from public domain C code by Daniel J. Bernstein <djb@cr.yp.to>

\* More information about curve25519 can be found here

\* <http://cr.yp.to/ecdh.html>

\* djb's sample implementation of curve25519 is written in a special assembly language called qhasm and uses the floating point registers.

\* This is, almost, a clean room reimplementaion from the curve25519 paper. It uses many of the tricks described therein. Only the crecip function is taken from the sample implementation.

## Licenses - FreeType

The FreeType Project LICENSE

2006-Jan-27

Copyright 1996-2002, 2006 by

David Turner, Robert Wilhelm, and Werner Lemberg

Introduction

=====

The FreeType Project is distributed in several archive packages; some of them may contain, in addition to the FreeType font engine, various tools and contributions which rely on, or relate to, the FreeType Project.

This license applies to all files found in such packages, and which do not fall under their own explicit license. The license affects thus the FreeType font engine, the test programs, documentation and makefiles, at the very least.

This license was inspired by the BSD, Artistic, and IJG (Independent JPEG Group) licenses, which all encourage inclusion and use of free software in commercial and freeware products alike. As a consequence, its main points are that:

o We don't promise that this software works. However, we will be interested in any kind of bug reports. ('as is' distribution)

o You can use this software for whatever you want, in parts or full form, without having to pay us. ('royalty-free' usage)

o You may not pretend that you wrote this software. If you use it, or only parts of it, in a program, you must acknowledge somewhere in your documentation that you have used the FreeType code. ('credits')

We specifically permit and encourage the inclusion of this software, with or without modifications, in commercial products.

We disclaim all warranties covering The FreeType Project and assume no liability related to The FreeType Project.

Finally, many people asked us for a preferred form for a credit/disclaimer to use in compliance with this license. We thus encourage you to use the following text:

Portions of this software are copyright <year> The FreeType Project ([www.freetype.org](http://www.freetype.org)). All rights reserved.

Please replace <year> with the value from the FreeType version you actually use.

Legal Terms

=====

## 0. Definitions

-----

Throughout this license, the terms 'package', 'FreeType Project', and 'FreeType archive' refer to the set of files originally distributed by the authors (David Turner, Robert Wilhelm, and Werner Lemberg) as the 'FreeType Project', be they named as alpha, beta or final release.

'You' refers to the licensee, or person using the project, where 'using' is a generic term including compiling the project's source code as well as linking it to form a 'program' or 'executable'.

This program is referred to as 'a program using the FreeType engine'.

This license applies to all files distributed in the original FreeType Project, including all source code, binaries and documentation, unless otherwise stated in the file in its original, unmodified form as distributed in the original archive.

If you are unsure whether or not a particular file is covered by this license, you must contact us to verify this.

The FreeType Project is copyright (C) 1996-2000 by David Turner, Robert Wilhelm, and Werner Lemberg. All rights reserved except as specified below.

### 1. No Warranty

-----

THE FREETYPE PROJECT IS PROVIDED 'AS IS' WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL ANY OF THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY DAMAGES CAUSED BY THE USE OR THE INABILITY TO USE, OF THE FREETYPE PROJECT.

### 2. Redistribution

-----

This license grants a worldwide, royalty-free, perpetual and irrevocable right and license to use, execute, perform, compile, display, copy, create derivative works of, distribute and sublicense the FreeType Project (in both source and object code forms) and derivative works thereof for any purpose; and to authorize others to exercise some or all of the rights granted herein, subject to the following conditions:

- o Redistribution of source code must retain this license file ('FTL.TXT') unaltered; any additions, deletions or changes to the original files must be clearly indicated in accompanying documentation. The copyright notices of the unaltered, original files must be preserved in all copies of source files.

- o Redistribution in binary form must provide a disclaimer that states that the software is based in part of the work of the FreeType Team, in the distribution documentation. We also encourage you to put an URL to the FreeType web page in your documentation, though this isn't mandatory.

These conditions apply to any software derived from or based on the FreeType Project, not just the unmodified files. If you use our work, you must acknowledge us. However, no fee need be paid to us.

### 3. Advertising

-----

Neither the FreeType authors and contributors nor you shall use the name of the other for commercial, advertising, or promotional purposes without specific prior written permission.

We suggest, but do not require, that you use one or more of the following phrases to refer to this software in your documentation or advertising materials: 'FreeType Project', 'FreeType Engine', 'FreeType library', or 'FreeType Distribution'.

As you have not signed this license, you are not required to accept it. However, as the FreeType Project is copyrighted material, only this license, or another one contracted with the

authors, grants you the right to use, distribute, and modify it. Therefore, by using, distributing, or modifying the FreeType Project, you indicate that you understand and accept all the terms of this license.

### 4. Contacts

-----

There are two mailing lists related to FreeType:

o freetype@nongnu.org

Discusses general use and applications of FreeType, as well as future and wanted additions to the library and distribution. If you are looking for support, start in this list if you haven't found anything to help you in the documentation.

o freetype-devel@nongnu.org

Discusses bugs, as well as engine internals, design issues, specific licenses, porting, etc.

Our home page can be found at <http://www.freetype.org>

## Licenses - IW

Copyright (c) 2007, 2008 Johannes Berg

Copyright (c) 2007 Andy Lutomirski

Copyright (c) 2007 Mike Kershaw

Copyright (c) 2008-2009 Luis R. Rodriguez

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## Licenses - JSON-C

Copyright (c) 2009-2012 Eric Haszlakiewicz

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

-----  
Copyright (c) 2004, 2005 Metaparadigm Pte Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Licenses - LIBTIRPC

Copyright (c) Copyright (c) Bull S.A. 2005 All Rights Reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Licenses - LIBXML2

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Licenses - Mbus

Copyright (c) 2002-2003, 2013-2019 Victor Antonovich (v.antonovich@gmail.com)

Copyright (c) 2011 Andrew Denysenko <nitr0@seti.kr.ua>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.



2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Licenses - Net-SNMP

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,

DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2013, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 10: Lennart Poettering copyright notice (BSD-like) -----

Copyright 2010 Lennart Poettering

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Part 11: IETF copyright notice (BSD) -----

Copyright (c) 2013 IETF Trust and the persons identified as authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of Internet Society, IETF or IETF Trust, nor the names of specific contributors, may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 12: Arista Networks copyright notice (BSD) ----

Copyright (c) 2013, Arista Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Arista Networks, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 13: VMware, Inc. copyright notice (BSD) -----

Copyright (c) 2016, VMware, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of VMware, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 14: USC/Information Sciences Institute copyright notice (BSD) -----

Copyright (c) 2017-2018, Information Sciences Institute

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Information Sciences Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Licenses - Open LDAP

Copyright 1998-2019 The OpenLDAP Foundation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP Public License.

A copy of this license is available in the file LICENSE in the top-level directory of the distribution or, alternatively, at <http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by other parties and/or subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3 distribution. Information concerning this software is available at <<http://www.umich.edu/~dirsvcs/ldap/ldap.html>>.

This work also contains materials derived from public sources. Additional information about OpenLDAP can be obtained at <<http://www.openldap.org/>>.

Portions Copyright 1998-2012 Kurt D. Zeilenga.

Portions Copyright 1998-2006 Net Boolean Incorporated.

Portions Copyright 2001-2006 IBM Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted only as authorized by the OpenLDAP

Public License.

Portions Copyright 1999-2008 Howard Y.H. Chu.

Portions Copyright 1999-2008 Symas Corporation.

Portions Copyright 1998-2003 Hallvard B. Furuseth.

Portions Copyright 2007-2011 Gavin Henry.

Portions Copyright 2007-2011 Suretec Systems Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that this notice is preserved. The names of the copyright holders may not be used to endorse or promote products derived from this software without their specific prior written permission. This software is provided "as is" without express or implied warranty.

Portions Copyright (c) 1992-1996 Regents of the University of Michigan.

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

## Licenses - OpenSSL

### LICENSE ISSUES

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts.

#### OpenSSL License

Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This product includes cryptographic software written by Eric Young  
([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Original SSLeay License

-----

Copyright (C) 1995-1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com))



All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public License.]

## Licenses - Wireless-RegDB

Copyright (c) 2008, Luis R. Rodriguez <mcgrof@gmail.com>

Copyright (c) 2008, Johannes Berg <johannes@sipsolutions.net>

Copyright (c) 2008, Michael Green <Michael.Green@Atheros.com>

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## Licenses - WPA Supplicant and Hostapd

Copyright (c) 2002-2019, Jouni Malinen <j@w1.fi> and contributors

All Rights Reserved.

These programs are licensed under the BSD license (the one with advertisement clause removed).

If you are submitting changes to the project, please see CONTRIBUTIONS file for more instructions.

This package may include either wpa\_supplicant, hostapd, or both. See README file respective subdirectories (wpa\_supplicant/README or hostapd/README) for more details.

Source code files were moved around in v0.6.x releases and compared to earlier releases, the programs are now built by first going to a subdirectory (wpa\_supplicant or hostapd) and creating build configuration (.config) and running 'make' there (for Linux/BSD/cygwin builds).

### License

This software may be distributed, used, and modified under the terms of BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name(s) of the above-listed copyright holder(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

# Index

"

"To Assert" and Assertion Timeout 498, 71

"To De-assert" and Deassertion Hysteresis 500, 72

8

802.1x Security Overview 121

A

A Note about Firmware Upgrade Time 255

A Note about Infinite Loop 226

A Note about Untriggered Rules 227

Action Group 202

Actuator Configuration Commands 399

Actuator Control Operations 407

Actuator Information 294

Adding a Firewall Rule 348

Adding a Monitored Device 400

Adding a Radius Server 386

Adding a Role-Based Access Control Rule 360

Adding an LDAP Server 380

Adding Attributes to the Class 490

Adding LDAP/LDAPS Servers 162

Adding Radius Servers 165

Adding TACACS+ Server 389

Adding TACACS+ Servers 167

Adding, Removing or Swapping Cascaded Devices 141

Additional Xerus Information - Assorted Products 494

AD-Related Configuration 477

Alarm 201

All Privileges 375

Altitude Correction Factors 504

Appendices 412

Assertion Timeout Example for Temperature Sensors 500

Asset Management Commands 404

Asset Management Strips and dcTrack 517

Asset Management Tag List 232

Asset Management Tag Log 234

Asset Strip Automatic Firmware Upgrade 108

Asset Strip Management 405

Asset Strip Settings 295

Asset Strips 100

Authentication Commands 378

Authentication Settings 295

Automatic and Manual Modes 39

Automatic Management of Sensors 85

Automatically Completing a Command 292

Available Actions 199

B

Backup and Restore of Device Settings 260

Backup and Restore via SCP 454

BCM2 Rear Panel Connectors and Controls 14

BCM2 Series Hardware Installation 10

Blade Slot 297

Branch Circuit Details 43

Branch Circuits 41

Built-in Rules and Rule Configuration 176

Bulk Configuration 255

Bulk Configuration or Firmware Upgrade via DHCP (TFTP/HTTPS) 429

Bulk Configuration Restrictions 256

Bulk Configuration via SCP 453

Bulk Configuration, Firmware Upgrade, or Backup/Restore via SCP 451

Bulk Configuration/Upgrade Procedure 429

C

Card Readers 278

Cascading Modes Overview 135

Change Load Shedding State 202

Changing a User's Password 366

Changing HTTP(S) Settings 143

Changing Measurement Units 371

Changing Modbus Settings 148

Changing SSH Settings 147

Changing Storage Settings 270  
 Changing Telnet Settings 148  
 Changing the Device Name 313  
 Changing the LAN Duplex Mode 324  
 Changing the LAN Interface Speed 324  
 Changing the Modbus Configuration 341  
 Changing the Role(s) 370  
 Changing the Sensor Description 394  
 Changing the Sensor Name 392  
 Changing the SSH Configuration 338  
 Changing the Telnet Configuration 337  
 Changing Your Own Password 373  
 Changing Your Password 49  
 Checking Lua Scripts States 246  
 Checking the Accessibility of NTP Servers 346  
 Cisco ISE Xerus TACACS+ Authentication 480  
 Clearing Diagnostic Log for Network Connections 311  
 Clearing Event Log 311  
 Clearing Information 311  
 Closing a Local Connection 290  
 Collected Data 249  
 Command History 297  
 Commands for Environmental Sensors 397  
 Common Network Settings 120  
 config.txt 422  
 Configuration Files 418  
 Configuration Files for Linking 425  
 Configuration Files for Linking: Port-Forwarding Cascade Example 426  
 Configuration or Firmware Upgrade with a USB Drive 417  
 Configure DSAM Serial Ports 95  
 Configure Panel Branch Circuits 36  
 Configure Panel Mains Circuit 36  
 Configure Power Meter 35  
 Configure Thresholds 69  
 Configuring Data Push Settings 229  
 Configuring DNS Parameters 322  
 Configuring Environmental Sensors' Default Thresholds 395  
 Configuring IPv4 Parameters 314  
 Configuring IPv6 Parameters 318  
 Configuring Login Settings 168  
 Configuring Network Services 142  
 Configuring NTP Server Settings 285  
 Configuring Password Policy 169  
 Configuring Power Meters and Branch Circuit Monitors 34  
 Configuring Security Settings 151  
 Configuring SMTP Settings 146  
 Configuring SNMP Settings 144  
 Configuring the Cascading Mode 335  
 Configuring the Device and Network 312  
 Configuring the Serial Port 241  
 Configuring Webcams and Viewing Live Images 266  
 Connect to DSAM Serial Targets in the Web Interface 97  
 Connect to DSAM Serial Targets via SSH 99  
 Connecting a Modbus RTU Device or Bus 516  
 Connecting a PDU to a Dominion KVM or Serial Device 514  
 Control Buttons 39  
 Controller Wiring to Meters 19, 32  
 Copying an Existing Authentication Server's Settings 383  
 Creating a New Attribute 489  
 Creating a Role 374  
 Creating a Self-Signed Certificate 159  
 Creating a TLS Certificate or CSR 157  
 Creating a User Profile 365  
 Creating Configuration Files via Mass Deployment Utility 426  
 Creating IP Access Control Rules 152  
 Creating Role Based Access Control Rules 154  
 Creating Roles 114  
 Creating Users 109  
 Curl Upload Return Codes 450  
 Current Transformer (CT) Wiring 17  
 Customizing Bulk Configuration Profiles 257  
  
**D**  
 Dashboard - Alarms 57  
 Dashboard - Alerted Sensors 56

Dashboard - Power Meter History 58  
Dashboard - Power Meters 55  
Data Encryption in 'config.txt' 427  
Data Push Format Examples 231  
Date and Time Settings 298  
dcTrack 517  
Deassertion Hysteresis Example for Temperature Sensors 502  
Default Measurement Units 298  
Default Voltage and Current Thresholds 503  
Deleting a Firewall Rule 352  
Deleting a Monitored Device 401  
Deleting a Role 378  
Deleting a Role-Based Access Control Rule 363  
Deleting a User Profile 372  
Determining the Authentication Method 379  
Device Configuration 297  
Device Configuration Commands 312  
Device Configuration/Upgrade Procedure 417  
Device Information 249  
Device Settings 118  
devices.csv 424  
Device-Specific Settings 507  
DHCP IPv4 Configuration in Linux 444  
DHCP IPv4 Configuration in Windows 431  
DHCP IPv6 Configuration in Linux 445  
DHCP IPv6 Configuration in Windows 439  
Diagnostic Log for Network Connections 130  
Different CLI Modes and Prompts 289  
DIN Rail Mounting PMM + PMB 27  
Door Access 173  
Door Status and Control 276  
Download via Curl 447  
Download via Web Browsers 447  
Downloading Diagnostic Data via SCP 455  
Downloading Diagnostic Information 261  
Downloading SNMP MIB 283  
DSAM CLI Commands 98  
DSAM Connection 94  
DSAM LED Operation 94

## E

EAP CA Certificate Example 329  
Editing or Deleting a Rule/Action 221  
Editing or Deleting IP Access Control Rules 153  
Editing or Deleting Ping Monitoring Settings 238  
Editing or Deleting Role Based Access Control Rules 156  
Editing or Deleting Roles 116  
Editing or Deleting Users 113  
Editing rcusergroup Attributes for User Members 492  
Enable Modbus Access 63  
Enabling and Configuring SNMP 280  
Enabling or Disabling 802.11n High Throughput 331  
Enabling or Disabling a User Profile 367  
Enabling or Disabling data backup 314  
Enabling or Disabling Data Logging 313  
Enabling or Disabling Front Panel Actuator Control 364  
Enabling or Disabling Front Panel Beeper-Sound Control 365  
Enabling or Disabling Front Panel Outlet Switching 364  
Enabling or Disabling Service Advertising 343  
Enabling or Disabling Strong Passwords 356  
Enabling or Disabling the LAN Interface 323  
Enabling or Disabling the Restricted Service Agreement 352  
Enabling Redfish Services 150  
Enabling Service Advertising 151  
Enabling the Restricted Service Agreement 170  
Environmental Sensor Configuration Commands 392  
Environmental Sensor Default Thresholds 301  
Environmental Sensor Information 300  
Environmental Sensor Package Information 307  
Equipment Maintenance and Service 11, 21  
Equipment Setup Worksheet Sample 413  
Ethernet (Wired) Interface Settings 121  
Event Log 298  
Event Rules and Actions 175  
Example - Actuator Naming 400

Example - Asset Management 405  
 Example - Baud Rate 406  
 Example - Creating a Role 378  
 Example - Default Upper Thresholds for Temperature 397  
 Example - Ping Command 412  
 Example - Server Settings Changed 403  
 Example - Turning On a Specific Actuator 408  
 Example -Time Configuration 346  
 Example: Ping Monitoring and SNMP Notifications 239  
 Existing Roles 302  
 Existing User Profiles 302  
 Export Readings as CSV 74  
 External Beeper 108, 203

**F**

Finding the Sensor's Serial Number 84  
 Firewall Control 347  
 Firmware Update via SCP 451  
 Firmware Upgrade via USB 428  
 Forcing a Password Change 367  
 Forcing the Device Detection Mode 406  
 FreeRADIUS Standard Attribute Illustration 467  
 FreeRADIUS VSA Illustration 476  
 From LDAP/LDAPS 488  
 From Microsoft Active Directory 488  
 Front Panel Permissions 303  
 Front Panel Settings 240  
 Full Disaster Recovery 255  
 fwupdate.cfg 418

**H**

Hardware Installation 10  
 Hardware Issue Detection 262  
 How Long a Link Remains Accessible 269

**I**

Identifying Snapshots Folders on Remote Servers 271  
 Identifying the Sensor Position and Channel 84  
 Idle Timeout 355

Illustration - GMAIL SMTP Certificate Chain 511  
 Illustrations of Adding LDAP Servers 382  
 Individual Sensor/Actuator Pages 87  
 Installation and Initial Configuration 10  
 Installing a CA-Signed Certificate 159  
 Installing or Downloading Existing Certificate and Key 161  
 Installing the USB-to-Serial Driver (Optional) 506  
 Internal Beeper 203  
 Introduction to the Web Interface 50  
 IP Configuration 304  
 IPv4-Only or IPv6-Only Configuration 304

**K**

Keys that Cannot Be Uploaded 459

**L**

LDAP Configuration Illustration 461  
 LDAP Settings 379  
 Legrand 11, 21  
 Licenses - Angular 519  
 Licenses - Bind9 528  
 Licenses - Clish 534  
 Licenses - Dropbear 539  
 Licenses - FreeType 541  
 Licenses - IW 543  
 Licenses - JSON-C 543  
 Licenses - LIBTIRPC 544  
 Licenses - LIBXML2 544  
 Licenses - Mbus 544  
 Licenses - Net-SNMP 545  
 Licenses - Open LDAP 550  
 Licenses - OpenSSL 552  
 Licenses - Wireless-RegDB 553  
 Licenses - WPA Supplicant and Hostapd 554  
 Log an Event Message 203  
 Log Rows 232  
 Logging in to CLI 287  
 Logging out of CLI 290  
 Login and Configuration 33  
 Login and Logout 48  
 Login Limitation 354

Login, Logout and Password Change 48  
Logout 50  
Lowercase Character Requirement 357  
Lua Scripts 243

## M

Maintenance 249  
Managed vs Unmanaged Sensors/Actuators 81  
Managing Firewall Rules 348  
Managing One Sensor or Actuator 85  
Managing Role-Based Access Control Rules 360  
Manually Starting or Stopping a Script 245  
Maximum Password History 358  
Maximum Password Length 356  
Menu 52  
Meter Controller Connectors and Controls 15  
Minimum Password Length 356  
Miscellaneous 247  
Modifying a Firewall Rule 350  
Modifying a Monitored Device's Settings 401  
Modifying a Role 377  
Modifying a Role-Based Access Control Rule 362  
Modifying a User Profile 366  
Modifying a User's Personal Data 366  
Modifying an Existing LDAP Server 383  
Modifying an Existing Radius Server 387  
Modifying an Existing TACACS+ Server 390  
Modifying Firewall Control Parameters 347  
Modifying or Deleting a Script 247  
Modifying or Deleting Bulk Configuration Profiles 259  
Modifying Role-Based Access Control Parameters 359  
Modifying SNMPv3 Settings 368  
Monitoring Server Accessibility 234  
Multi-Command Syntax 292

## N

Network Configuration 303  
Network Configuration Commands 314  
Network Connections Diagnostic Log 307  
Network Diagnostics 261, 303

Network Interface Settings 306  
Network Service Settings 306  
Network Settings 119  
Network Troubleshooting in Diagnostic Mode 410  
NPS VSA Illustration 468  
Numeric Character Requirement 357

## O

Optional Parameters 381

## P

Panel Branch Circuits Operations 67  
Panel Layout 33  
Panel Mains Circuit Management 67  
Panel Wiring Example 18  
Panels 41  
Password Aging 354  
Password Aging Interval 355  
Performing Bulk Configuration 258  
Peripheral Devices Configuration Commands 403  
Peripheral Devices Settings 307  
Peripherals 43, 76  
Permissions 117  
Placeholders for Custom Messages 217  
PM Series Hardware Installation: PMC-1000, PMC-1001, PMM-1000, PMB-1960, PMMC-1000 19  
PMB Branch Circuit Wiring 30  
PMC Power Metering Controller 59  
PMM Power Wiring 30  
PMMC Power Wiring 31  
Port Forwarding Examples 139  
Port Number Syntax 137  
Power CIM 109  
Power IQ Configuration 516  
Power Meter (PMM) Connectors and Controls 24  
Power Meter Branch Monitor (PMB) Connectors 25  
Power Meter Controller (PMC) iX6/iX7 27  
Power Meter Management 63  
Power Meter with Controller (PMMC) 25  
Power Meters 40, 61

Product Models 10  
Product Overview 11  
Product Overview - PM Series Power Meters 21  
Product Specification 23  
Product Specifications 12  
Push Out Sensor Readings 204

## Q

Querying Available Parameters for a Command 291  
Querying DNS Servers 410  
Quick Access to a Specific Page 54

## R

Rack Unit Configuration (Tag Ports) 405  
Rack Unit Settings of an Asset Strip 309  
RADIUS Configuration Illustration 466  
Radius Settings 386  
Raw Configuration Upload and Download 446  
Rebooting 263  
Record Snapshots to Webcam Storage 205  
Regaining Access with HSTS and Expired Certificate 144  
Reliability Data 308  
Reliability Error Log 308  
Reliability Hardware Failures 309  
Remote Authentication Examples 461  
Removing an Existing LDAP Server 386  
Removing an Existing Radius Server 388  
Removing an Existing TACACS+ Server 391  
Removing the Uploaded Certificate or Private Key 330  
Requirements for Prometheus and Grafana 248  
Reserving IP Addresses in DHCP Servers 494  
Reserving IP in Linux 495  
Reserving IP in Windows 494  
Resetting All Settings to Factory Defaults 264  
Resetting the BCM2 408  
Resetting to Factory Defaults 409  
Restarting the BCM2 408  
Restricted Service Agreement 352  
Retrieving Energy Usage 286

Retrieving Previous Commands 291  
Returning User Group Information 488  
Role Configuration Commands 374  
Role of a DNS Server 506  
Role-Based Access Control 359

## S

Safety Information 8, 10, 19  
Sample Environmental-Sensor-Level Event Rule 225  
Sample Event Rules 222  
Sample Inlet-Level Event Rule 224  
Sample Outlet-Level Event Rule 222  
Sample PDU-Level Event Rule 222  
Scan Power Meters 34  
Scheduling an Action 214  
Security Configuration Commands 347  
Security Settings 310  
Send an SNMP Notification 210  
Send Email 206  
Send Sensor Report 207  
Send Sensor Report Example 214  
Send SMS Message 208  
Send Snapshots via Email 209  
Sending Links to Snapshots or Videos 268  
Sensor Descriptors for Inlet Active Power 231  
Sensor Log 231  
Sensor Threshold Settings 496  
Sensor/Actuator Location Example: X, Y, Z Coordinates 92  
Sensor/Actuator States 82  
Serial Access With Dominion Serial Access Module 93  
Serial Port Configuration Commands 405  
Serial Port Settings 311  
Server Reachability Configuration Commands 400  
Server Reachability Information 310  
Server Reachability Information for a Specific Server 310  
Server Status Checking or Power Control 237  
Setting Data Logging 227  
Setting Data Logging Measurements Per Entry 313



Setting Default Measurement Units 118, 373

Setting Ethernet EAP Parameters 326

Setting IPv4 Static Routes 317

Setting IPv6 Static Routes 321

Setting LAN Interface Parameters 323

Setting Log Capacity 313

Setting Network Service Parameters 336

Setting Power Thresholds 68

Setting Redfish Service 342

Setting the Alarmed to Normal Delay for DX2-passive infrared sensor 394

Setting the Automatic Daylight Savings Time 345

Setting the Baud Rates 405

Setting the BSSID 334

Setting the Cascading Mode 134

Setting the Date and Time 171

Setting the Ethernet Authentication Method 325

Setting the HTTP Port 336

Setting the HTTPS Port 337

Setting the IPv4 Address 316

Setting the IPv4 Configuration Mode 314

Setting the IPv4 Gateway 316

Setting the IPv4 Preferred Host Name 315

Setting the IPv6 Address 320

Setting the IPv6 Configuration Mode 318

Setting the IPv6 Gateway 320

Setting the IPv6 Preferred Host Name 319

Setting the LAN MTU 325

Setting the PSK 331

Setting the Registry to Permit Write Operations to the Schema 488

Setting the SNMP Configuration 339

Setting the SSID 330

Setting the Time Zone 345

Setting the Wireless Authentication Method 331

Setting the Wireless MTU 335

Setting the X Coordinate 393

Setting the Y Coordinate 393

Setting the Z Coordinate 393

Setting Up a TLS Certificate 157

Setting Up External Authentication 161

Setting Wireless EAP Parameters 332

Setting Wireless Parameters 330

Setting Your Preferred Measurement Units 117

Showing Information 294

Showing Network Connections 411

Shut down a Server and Control its Power 204

Single Login Limitation 354

SmartLock 273

SmartLock and Card Reader 272

SNMP Gets and Sets 284

SNMP Sets and Thresholds 285

SNMPv2c Notifications 282

SNMPv3 Notifications 280

Sorting a List 54

Special Character Requirement 358

Special Configuration and Upgrade Methods 417

Specifying the Agreement Contents 353

Specifying the CC Sensor Type 392

Specifying the SSH Public Key 372

Standard Attributes 467

Start or Stop a Lua Script 211

Static Route Examples 131

Static Route Interface Names 133

Step A. Determine User Accounts and Roles 461

Step A: Add Your BCM2 as a RADIUS Client 468

Step B. Configure User Groups on the AD Server 461

Step B: Configure Connection Policies and Vendor-Specific Attributes 471

Step C. Configure LDAP Authentication on the BCM2 462

Step D. Configure Roles on the BCM2 465

Strong Passwords 356

Supported Web Browsers and Mobile Devices 48

Switch Outlet Group 212

Switch Outlets 212

Switch Peripheral Actuator 213

Switching Off an Actuator 407

Switching On an Actuator 407

Syslog Message 213

System and USB Requirements 418

## T

TACACS+ Settings 389  
Testing the Network Connectivity 411  
TFTP/HTTPS Requirements 430  
The ? Command for Showing Available Commands 290  
The MIB File 284  
Third Party Licenses 519  
Thresholds and Sensor States 497  
Time Configuration Commands 343  
Tips for Using the CLI 290  
TLS Certificate Chain 508  
Tracing the Route 412

## U

Unbalanced Current Calculation 505  
Unblocking a User 408  
Updating the Firmware 253  
Updating the LDAP Schema 488  
Updating the Schema Cache 492  
Upgrade Guidelines for Existing Cascading Chains 255  
Upgrade Matrix 254  
Upload via Curl 448  
Uploading or Downloading Raw Configuration Data 457  
Uploading Raw Configuration 448  
Uppercase Character Requirement 357  
User Blocking 355  
User Configuration Commands 365  
User Interfaces Showing Default Units 118  
User Management 109  
Using Default Thresholds 394  
Using Prometheus and Grafana 248  
Using SNMP 280  
Using the BCM2's Display 38  
Using the Command Line Interface 287  
Using the Web Interface 48

## V

Vendor-Specific Attributes 467  
View DSAM Serial Ports 95

Viewing Connected Users 250  
Viewing Firmware Update History 255  
Viewing the Dashboard 54  
Viewing the Panel Data 64  
Viewing the Power Meter Data 61  
Viewing, Downloading, Deleting Locally-Saved Snapshots 269  
Viewing, Pausing, Resuming or Clearing the Local Event Log 252  
Voltage and Current Measurement Wiring 29  
Voltage Measurement and Power Wiring 15

## W

Ways to Probe Existing User Profiles 506  
Webcam Management 265  
What is a Certificate Chain 508  
Windows NTP Server Synchronization Solution 172  
Wireless Network Settings 126  
With an Analog Modem 289  
With HyperTerminal 287  
With SSH or Telnet 288  
Writing or Loading a Lua Script 243

## X

Xerus Default Log Messages for All Products 180  
Xerus Product Integration 514

## Y

Yellow- or Red-Highlighted Sensors 80

## Z

Z Coordinate Format 92