NX1 PDU User Guide

NX1-PDU
LE14534AA
September 2024
Release 4.0.35

Contents

Introduction

NX1 PDU is an intelligent power distribution unit (PDU) that allows you to reboot remote servers and other network devices and/or to monitor power in the data center.

The intended use of NX1 PDU is distribution of power to information technology equipment such as computers and communication equipment where such equipment is typically mounted in an equipment rack located in an information technology equipment room.

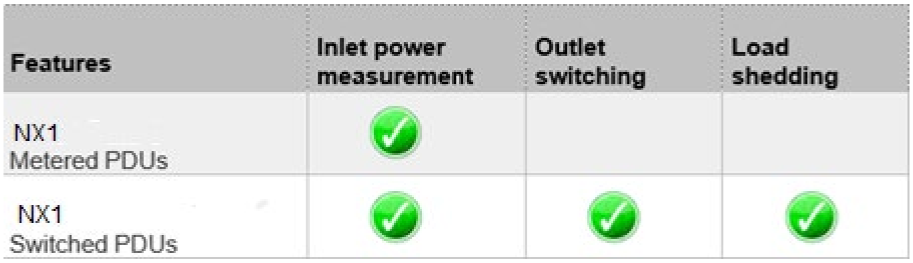
NX1 offers different types of NX1 PDU models -- some are outlet-switching capable, and some are not. With the outlet-switching function, you can recover systems remotely in the event of system failure and/or system lockup, eliminate the need to perform manual intervention or dispatch field personnel, reduce downtime and mean time to repair, and increase productivity.

In This Chapter

Available NX1 PDU Models

This Online Help mainly introduces two types of NX1 PDU models, both of which are inlet metered PDUs.

► *NX1 PDUs comparison in brief:*



Features	Inlet power measurement	Outlet switching	Load shedding
NX1 Metered PDUs	✓		
NX1 Switched PDUs	✓	✓	✓

Package Contents

The equipment and other material in the product package includes:

► *Zero U Products*

- One NX1 PDU
- 0U bracket pack and buttons for Zero U

► *1U Products*

- One NX1 PDU
- 1U bracket pack and screws

APIPA and Link-Local Addressing

NX1 PDU supports Automatic Private Internet Protocol Addressing (APIPA).

With APIPA, your NX1 PDU automatically configures a link-local IP address and a link-local host name when it cannot obtain a valid IP address from any DHCP server in the TCP/IP network.

Only IT devices connected to the same subnet can access the NX1 PDU using the link- local address/host name. Those in a different subnet cannot access it.

Exception: NX1 PDU in the Port Forwarding mode does not support APIPA.
Once the NX1 PDU can get a DHCP-assigned IP address, it stops using APIPA and the link- local address is replaced by the DHCP-assigned address.

► *„Scenarios where APIPA applies:*

- DHCP is enabled on the NX1 PDU, but no IP address is assigned to the NX1 PDU. This may be caused by the absence or malfunction of DHCP servers in the network.

  Note: Configuration by connecting the NX1 PDU to a computer using a network cable is an application of this scenario.

- The NX1 PDU previously obtained an IP address from the DHCP server, but the lease of this IP address has expired, and the lease cannot be renewed, or no new IP address is available.

► *„Link-local addressing:*

- IPv4 address:

Factory default is to enable IPv4 only. The link-local IPv4 address is 169.254.x.x/16, which ranges between 169.254.1.0 and 169.254.254.255.

- IPv6 address:

A link-local IPv6 address is available only after IPv6 is enabled on the NX1 PDU.

- Host name - pdu.local:

You can type https://pdu.local to access the NX1 PDU instead of typing the link-local IP address.

► *„Retrieval of the link-local address:*

- See Device Info (in Chapter Front Panel Display).

Before You Begin

Before beginning the installation, perform the following activities:

- Unpack the product and components
- Prepare the installation site
- Check the branch circuit rating
- Fill out the equipment setup worksheet

Unpacking the Product and Components

- Remove the NX1 PDU and other equipment from the box in which they were shipped.
- Compare the serial number of the equipment with the number on the packing slip located on the outside of the box and make sure they match.
- Inspect the equipment carefully. If any of the equipment is damaged or missing, contact Raritan Technical Support Department for assistance.
- Verify that all circuit breakers on the NX1 PDU are set to ON. If not, turn them ON.

  Or make sure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

Note: Not all models have overcurrent protectors.

Preparing the Installation Site

- Make sure the installation area is clean and free of extreme temperatures and humidity.

Note: If necessary, contact Raritan Technical Support for the maximum operating temperature for your model.

- Allow sufficient space around the NX1 PDU for cabling and outlet connections.
- Review Safety Instructions in this guide.

Checking the Branch Circuit Rating

The rating of the branch circuit supplying power to the PDU shall be in accordance with national and local electrical codes.

Filling Out the Equipment Setup Worksheet

An Equipment Setup Worksheet is provided in this Guide. Use this worksheet to record the model, serial number, and use of each IT device connected to the PDU.

As you add and remove devices, keep the worksheet up-to-date.

Rack Mounts and Locking Outlets

This chapter describes how to rack mount a NX1 PDU and describes locking outlet options.

In This Chapter

Rackmount Safety Guidelines

In NX1 products which require rack mounting, follow these precautions:

- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the Power Distribution Units.
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, to the branch circuit.

Circuit Breaker Orientation Limitation

Usually a PDU can be mounted in any orientation. However, when mounting a PDU with circuit breakers, you must obey these rules:

- Circuit breakers CANNOT face down. For example, do not horizontally mount a Zero U PDU with circuit breakers on the ceiling.
- If a rack is subject to shock in environments such as boats or airplanes, the PDU CANNOT be mounted upside down. If installed upside down, shock stress reduces the trip point by 10%.

Note: If normally the line cord is down, upside down means the line cord is up.

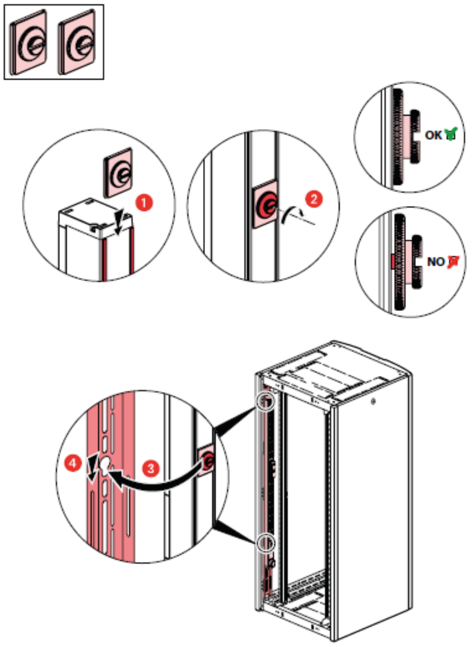
Rack Mounting Solutions

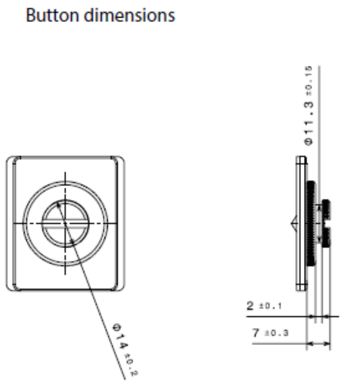
The Zero-U NX1 PDU is delivered with 2 different sets for mounting in a rack.

Set of 2 buttons

Use the set of 2 buttons for screwless fixing.

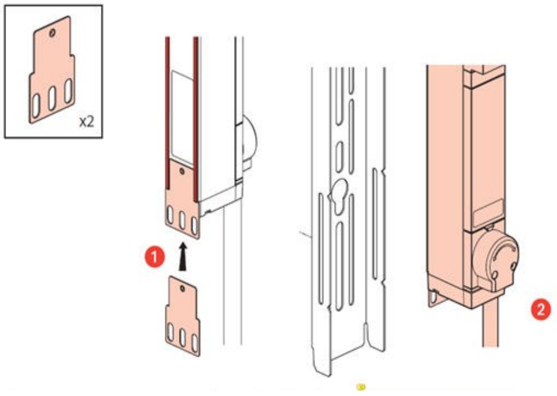
The height of the fixing centre can be set at any point along the full height of the PDU by sliding the button slots into the groove on the rear of the PDU. Tighten using a screwdriver.

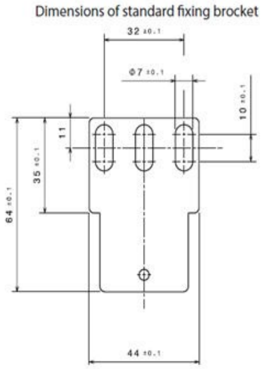




Set of 2 standard fixing brackets

Use the set of 2 standard brackets for screw-fixing (screws not included).



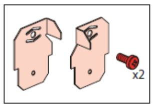


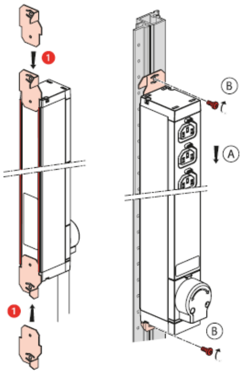
OPTION: Brackets for Nexpand Racks

Screw-fixing (2 screws included).

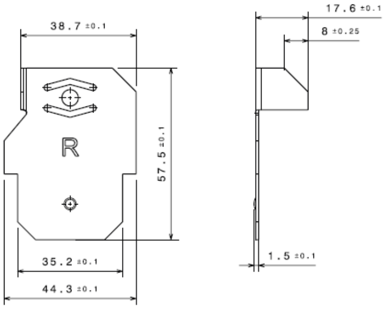
Ref. 981227 Set of 2 brackets (for 1 PDU)

Ref. 981228 Set of 20 brackets (for 10 PDUs)





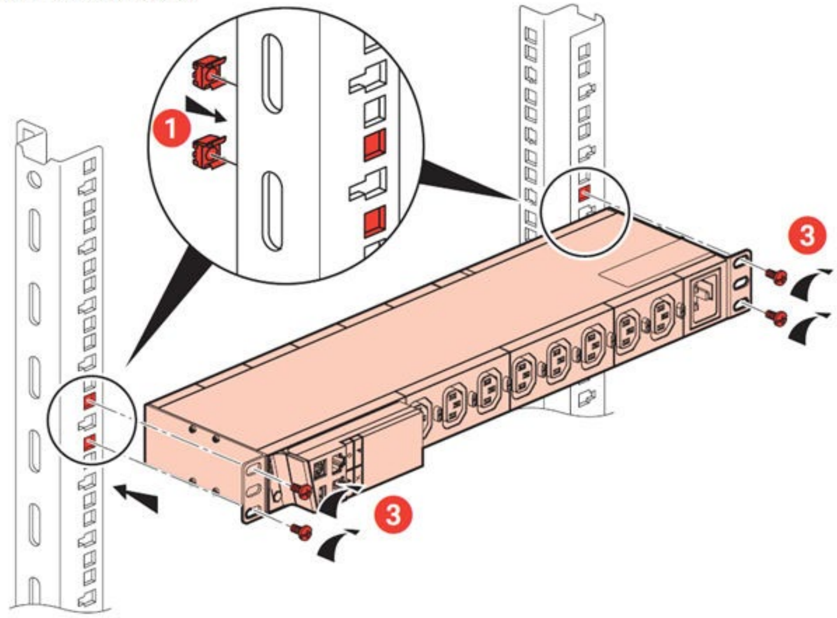
Dimensions of NEXPAND fixing bracket



19” horizontal PDUs

The 19'' horizontal NX1 PDU is delivered with screws and cage nuts to be mounted on 19'' uprights.

Delivered with 4 screws and 4 cage nuts.

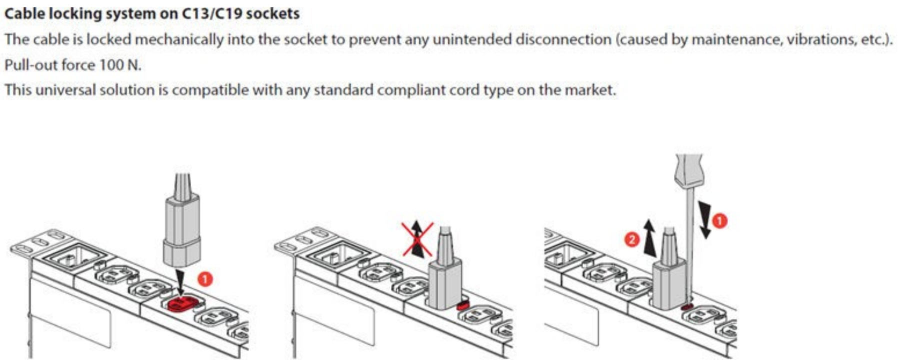


Locking Outlets

Some NX1 Smart PDUs are implemented with C13 and/or C19 locking outlets.

Locking outlets help secure the connection of power cords from your IT equipment to NX1 PDU.

A locking outlet has a button on it. Such outlets do not require any special power cords to achieve the locking purpose.



Cable locking system on C13/C19 sockets

The cable is locked mechanically into the socket to prevent any unintended disconnection (caused by maintenance, vibrations, etc.).

Pull-out force 100 N.

This universal solution is compatible with any standard compliant cord type on the market.

Initial Installation and Configuration

This chapter explains how to install your NX1 PDU and configure it for network connectivity.

Connecting the PDU to a Power Source

- Verify that all circuit breakers on the NX1 PDU are set to ON. If not, turn them ON.

Or make sure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

Note: Not all models have overcurrent protectors.

- Connect each NX1 PDU to an appropriately rated branch circuit. Refer to the label or nameplate affixed to your NX1 PDU for appropriate input ratings or range of ratings.

Note: When a NX1 PDU powers up, it proceeds with the power-on self test and software loading for a few moments.

- When the software has completed loading, the outlet LEDs show a steady color and the front panel display illuminates. Note that outlet LEDs are only available on some PDU models.

Connecting the NX1 PDU to Your Network

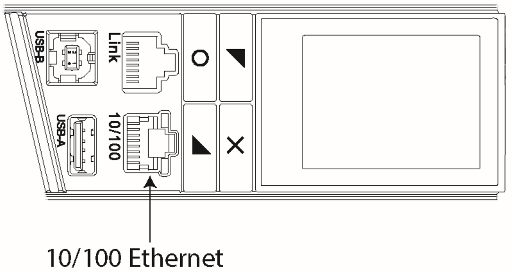
To remotely administer the NX1 PDU, you must connect the NX1 PDU to your local area network (LAN).

Ethernet port of NX1 PDU must be enabled for the described connection to work properly, which has been enabled per default.

► *„To make a wired connection:*

- Connect a standard network patch cable to the Ethernet port on the NX1 PDU.
- Connect the other end of the cable to your LAN.

Below illustrates the Ethernet port on Zero U models.



Configuring the NX1 PDU

You can initially configure the NX1 PDU via one of the following:

- A TCP/IP network that supports DHCP
- A computer physically connected to the NX1 PDU

► *„Configuration via a DHCP-enabled network:*

- Connect the NX1 PDU to a DHCP IPv4 network. See Connecting the NX1 PDU to Your Network.
- Retrieve the DHCP-assigned IPv4 address. Use the front panel LCD display to retrieve it.
- Launch a web browser to configure the NX1 PDU.

► *„Configuration via a connected computer:*

- Connect the NX1 PDU to a computer.
- Use the connected computer to configure the NX1 PDU via the command line or web interface.
- Web interface: Launch the web browser on the computer, and type the link-local IP address or pdu.local to access the NX1 PDU. For link-local IP address retrieval see Device Info.

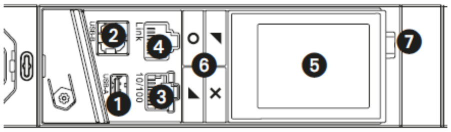
Tip: To configure a number of NX1 PDUs quickly, see Bulk Configuration Methods.

Connecting the NX1 PDU to a Computer

The NX1 PDU can be connected to a computer for configuration via one of the following ports.

- Ethernet port
- USB-B port

The following diagram illustrates a PDU's ports.



1) USB-A port: to connect a USB Flash drive or to cascade NODE PDUs for sharing network connection

2) USB-B port: to cascade NODE PDUs for sharing network connection or to establish a USB connection between a computer and the PDU for using the Command Line Interface (CLI).

3) ETH 10/100 Port – Network connection

4) Link RJ45 port: RS485 port for cascading of BASE units (see user guide)

5) Front panel display: to view PDU metering data and outlet information (on select models)

6) Control buttons for LED display: Navigate the local menu

7) NODE controller disconnection button: Physically disconnect the NODE controller from its base

To use the command line interface (CLI) for configuration, establish a USB connection.

To use a web browser for configuration, make a network connection to the computer. The NX1 PDU is automatically configured with the following link-local addressing in any network without DHCP available:

- https://169.254.x.x (where x is a number)
- https://pdu.local

Establish one of the following connections to a computer. Ethernet port of NX1 PDU must be enabled for the described connection to work properly, which has been enabled per default.

► *„ Direct network connection:*

- Connect one end of a standard network patch cable to the 10/100 Ethernet port of the NX1 PDU.
- Connect the other end to a computer's Ethernet port.
- On the connected computer, launch a web browser to access the NX1 PDU, using either link-local addressing: pdu.local or 169.254.x.x.

► *„ USB connection:*

- A USB-to-serial driver is required in Windows®. Install this driver before connecting the USB cable.
- Connect a USB cable between a computer's USB-A port and the USB-B port of NX1 PDU.
- Perform initial network configuration via CLI.
  Initial network configuration via CLI Sample:

These sample commands set up the ETHERNET interface with static IP address, gateway, and DNS server settings.

```
#config

config:# network bridge enabled false

config:# network ipv4 interface ETHERNET enabled true

config:# network ipv4 interface ETHERNET configMethod static

config:# network ipv4 interface ETHERNET address 192.168.56.80/24

config:# network ipv4 interface ETHERNET gateway 192.168.56.128

config:# network dns firstServer 1.1.1.1 secondServer 1.0.0.1

config:# network ethernet Ethernet speed 100Mbps duplexMode full

config:# apply
```

Note: Not all serial-to-USB converters work properly with the NX1 PDU so Raritan does not introduce the use of such converters.

Bulk Configuration Methods

If you have to set up multiple NX1 PDUs, you can use one of the following configuration methods to save your time.

► *A bulk configuration file downloaded from NX1 PDU:*

- Requirement: All NX1 PDUs to configure are of the same model and firmware.
- Procedure: First finish configuring one NX1 PDU. Then download the bulk configuration file from it and copy this file to all of the other NX1 PDUs.

► *A TFTP server:*

- Requirement: DHCP is enabled in your network and a TFTP server is available.
- Procedure: Prepare special configuration files, which must include fwupdate.cfg, and copy them to the root directory of the TFTP server. Re-boot all NX1 PDUs after connecting them to the network.

► Curl command:

- Requirement: Two files are required -- one is a configuration file in TXT and the other is a devices list file in CSV. See config.txt and devices.csv.
- Procedure: Upload both files to all of NX1 PDUs one by one, using the appropriate curl command.

► *SCP or PSCP command:*

- Requirement: Two files are required -- one is a configuration file in TXT and the other is a devices list file in CSV.

- Procedure: Upload both files to all of NX1 PDUs one by one, using the appropriate SCP or PSCP command.

► *A USB flash drive:*

- Requirement: A FAT32- or supperfloppy-formatted USB flash drive containing two special configuration files and one devices list file is required.
- Procedure: Plug this USB drive into the NX1 PDU. When a happy smiley is shown on the front panel display, press and hold one of the control buttons on the front panel until the display turns blank.

Deploying Link Chains with IP Cascading

NODE units can be cascaded through their USB Ports under the same IP via the Port Forwarding mode or a different IP using the Bridging mode. See next Chapter Cascading Multiple NX1 PDUs via USB for Sharing Ethernet Connectivity.

A total of 8 NODE units can be cascaded in a single link chain. The first unit in a cascade will act as the primary device. Only the primary device must be physically connected to the LAN.

Additionally, each NODE unit in a cascade can downstream up to 31 BASE units in their own link chain through RS485. Max length: 250m in total and 30m between each PDU.

Cascading Multiple NX1 PDUs via USB for Sharing Ethernet Connectivity

You can have multiple NX1 NODE PDUs share one Ethernet connection by cascading them via the USB interface.

The first one in the cascade is the primary unit and all the other devices follow it in the cascade. Only the primary unit is physically connected to the LAN.

Each device in the cascade is accessible over the network, with Port-Forwarding cascading mode or Bridging cascading mode activated on the primary unit.

- Port Forwarding: Each device in the cascading chain is accessed with the same IP address(es) but with a different port number assigned.
- Bridging mode: Each device in the cascading chain is accessed with a different IP address within the LAN subnet.

► *„Basic cascading restrictions:*

- All NX1 PDU in the chain must run compatible firmware versions, which are Firmware v4.0.30 or later.
- The cascading mode of all devices in the chain must be the same.
- Do NOT connect cascaded units other than primary to the LAN.

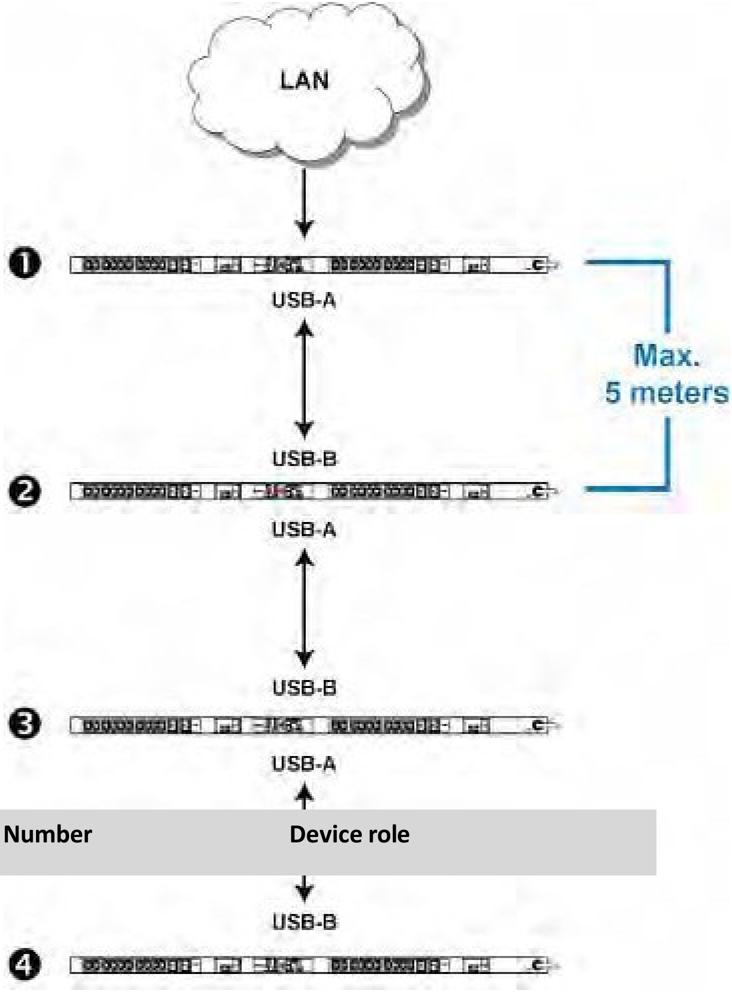
► *„Troubleshooting:*

When a networking issue occurs, check the cascading connection and/or software settings of all devices in the chain.

Cascading All Devices via USB

You must set the cascading mode before establishing the chain.

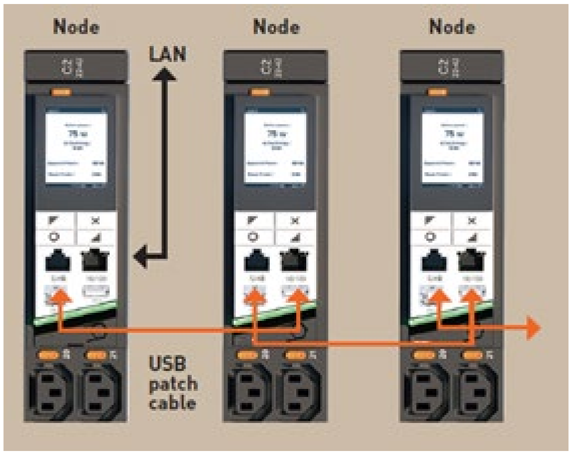
Any certified USB 2.0 cable up to 5 meters (16 feet) long can be used. Both cascading modes support a maximum of 16 devices in a chain. The following diagram illustrates NX1 PDUs cascaded via USB.



Number	Device role
❶	Primary unit
❷	Link unit 1
❸	Link unit 2
❹	Link Unit 3

► *„To cascade NX1 PDUs via USB:*

- Make sure all of NX1 PDUs are running firmware version 4.0.30 or later.
- Choose the appropriate one as the primary unit.
- Log in to all devices one by one and select the same cascading mode.
- Set the cascading mode of all devices to Port Forwarding. Make sure the cascading role and downstream interface are also set correctly.
- Connect the primary unit to the LAN, using a standard network patch cable (CAT5e or higher).
- Connect the USB-A port of the primary unit device to the USB-B port of an additional NX1 PDU via a USB cable. This additional device is Link Unit 1.
- Connect Link Unit 1's USB-A port to the USB-B port of an additional NX1 PDU via another USB cable. The second additional device is Link Unit 2.
- Repeat the same step to connect more link units. You can cascade up to 15 link units.
- Only the primary unit’s network settings should be configured.

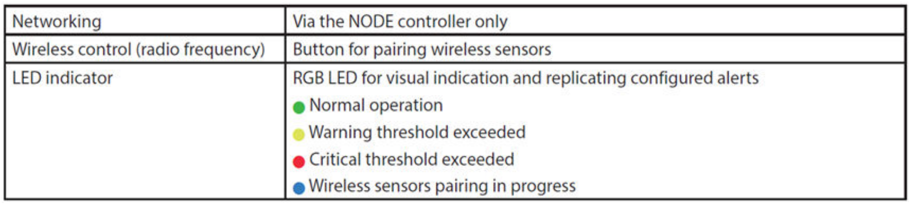


Cascading Multiple NX1 PDUs via RS485 for Sharing Ethernet Connectivity

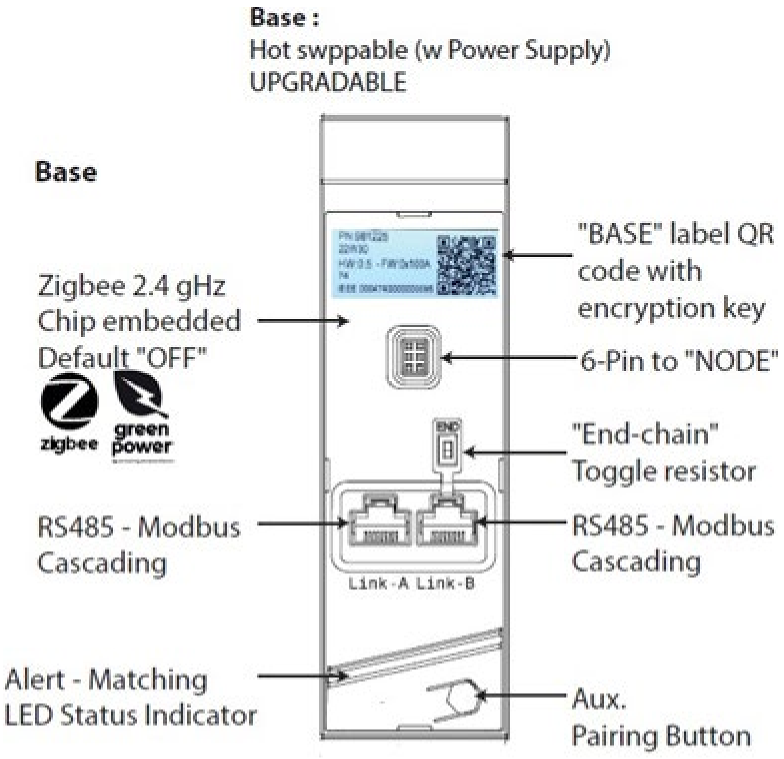
The NX1 PDU without controller is referred to as a BASE unit. Additionally, a NODE controller module can be purchased and connected to the BASE unit to turn it into a NODE unit.

► *„BASE Unit*

A BASE unit describes the NX1 PDU without any additional features. It can be upgraded to a NODE unit by plugging a NODE controller module into the BASE unit.



Networking	Via the NODE controller only
Wireless control (radio frequency)	Button for pairing wireless sensors
LED indicator	RGB LED for visual indication and replicating configured alerts 🟢 Normal operation 🟡 Warning threshold exceeded 🔴 Critical threshold exceeded 🔵 Wireless sensors pairing in progress


Base :
Hot swppable (w Power Supply)
UPGRADABLE
Base
"BASE" label QR code with encryption key
Zigbee 2.4 gHz Chip embedded Default "OFF"
zigbee
green power
6-Pin to "NODE"
END
"End-chain" Toggle resistor
RS485 - Modbus Cascading
RS485 - Modbus Cascading
Link-A Link-B
Alert - Matching LED Status Indicator
Aux. Pairing Button

► *„NODE Unit*

A NODE unit consists of the BASE NX1 PDU and a NODE controller module that has been connected to the PDU. The NODE controller module is equipped with a LCD display.

Physical Deployment recommendations

The units must be connected in a downward stream, meaning that each BASE unit must have only one upstream and downstream device connected through RS485 at a time.

Do not physically connect any other than the first device in a link chain to the network.
Do not connect two BASE units through both Link A and Link B port simultaneously.

For the last device within a link chain, the position of the Link-B Port switch should always be toggled to "END". The Link-B port switch of all other devices within the link chain must be toggled to the opposite position.

Pairing Base units to a Node in a RS485 link chain

A NODE unit can be paired with a maximum of 31 BASE units through a RS485 link chain.

The NODE unit will act as the IP Controller device in a link chain. It must be the only device that is physically connected to the LAN. A NODE unit must not be linked to any upstream device and always remain the first device in a RS485 link chain.

A BASE unit must not be linked to more than one downstream or upstream device at once through

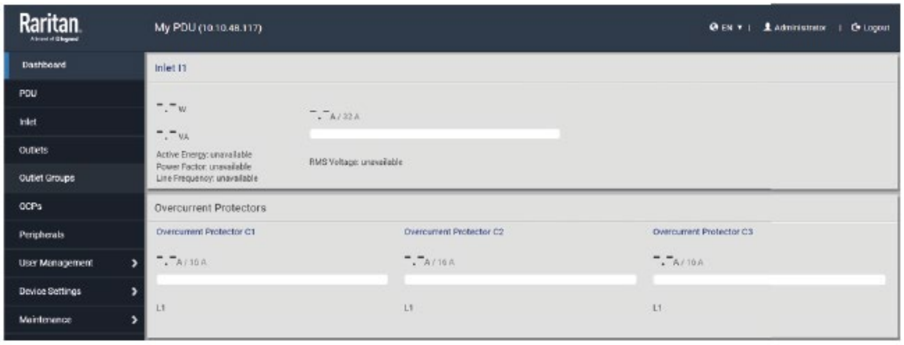
RS485.

Adding and Removing Base Units in a Link Chain

To connect a BASE unit to a link chain, the NODE unit must be deployed as Gateway.

► *Adding a BASE unit to the link chain*

1) Power on the BASE unit.
2) Attach one end of the RS485 cable to the LINK A port of the BASE unit.
3) Attach the other end to the RS485 Link port of the NODE unit.
4) Log in to the web interface of the PDU.
5) Go to PDU.



-.- W

-.- VA

Active Energy: unavailable
Power Factor: unavailable
Line Frequency: unavailable

-.- A / 32 A

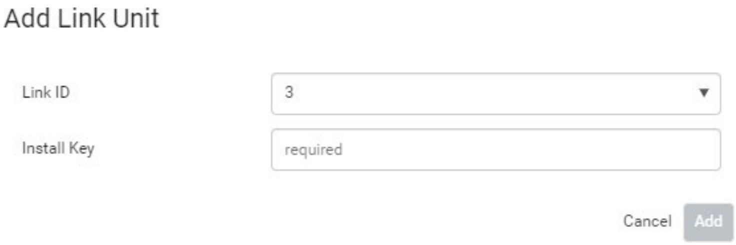
RMS Voltage: unavailable

Overcurrent Protector C1: -.- A / 10 A, L1

Overcurrent Protector C2: -.- A / 16 A, L1

Overcurrent Protector C3: -.- A / 16 A, L1

6) Select "Add Link PDU" in the Link PDUs column.



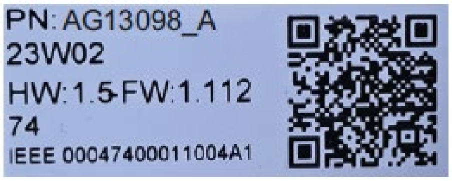
Add Link Unit

Link ID: 3

Install Key: required

7) Select a Link ID for the new device.
8) Enter the Install Key based on the QR Code label on the BASE. You can read the QR Code using a smartphone or a QR code scanner:

Example of key reading for the below QR code



PN: AG13098_A
23W02
HW: 1.5 FW: 1.112
74
IEEE 00047400011004A1

G$K:AG13098_A
$I:1C6C181EA0C12DB304A3110100E59DD1090% Z$A:00047400011004A1%
M:23W02
$HW:1.5
$FW:1.112

3 different formats are accepted.
In our example:

- Full key

G$K:981225$I:1C6C181EA0C12DB304A3110100E59BDD1090%
Z$A:00047400011004A1%M:23W02$HW:1.5$FW:1.11

- Reduce key with CRC

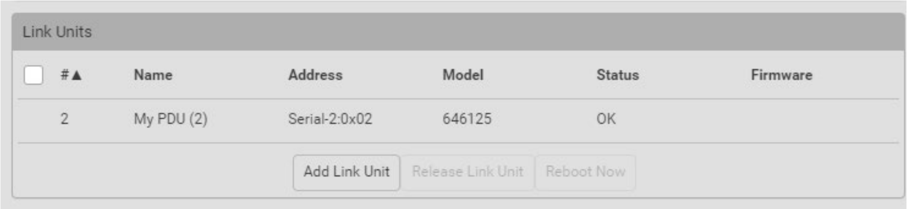
1C6C181EA0C12DB304A3110100E59BDD1090

- Only key

1C6C181EA0C12DB304A3110100E59BDD

9) Click "Add" to add the BASE unit to the link chain.

On success, the added unit will be listed in the table of the Link Units column.



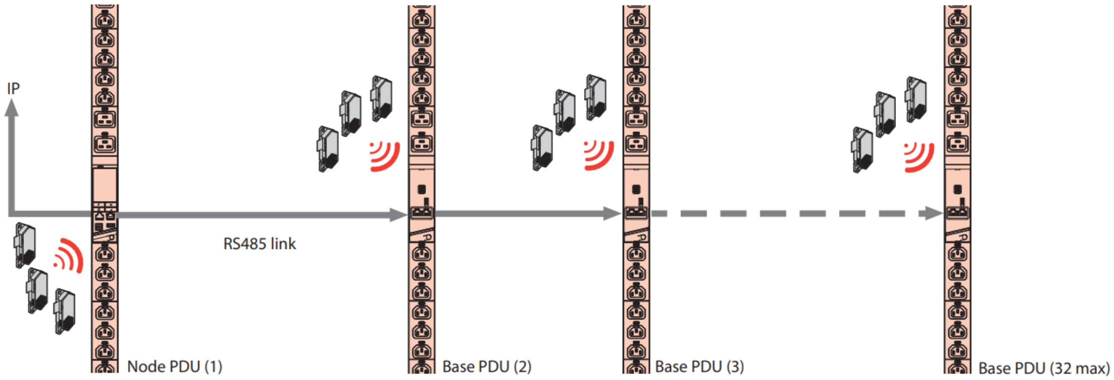
Link Units

□	#▲	Name	Address	Model	Status	Firmware
	2	My PDU (2)	Serial-2:0x02	646125	OK	

10) You may repeat steps 1-9- to install up to 31 BASE PDUs to the cascade.

11) When all install codes are well set, click on “Reboot now” to apply the configuration of the cascade.

The finished setup should look like this:



Note that wireless sensors could be added to this cascade.

► *„Removing a BASE unit from the link chain*

Important: Do not unplug the BASE unit before it has been removed from the table by the NODE unit.

Access the web interface of the PDU:

1) Log in to the web interface.
2) Go to PDU.
3) In the Link PDUs column, select the BASE unit that you wish to remove from the chain.
4) Select "Release Link PDU" in the Link PDUs column.
5) Confirm the release of the BASE unit in the pop-up window.

On success the BASE unit will be removed from the table in the Link PDUs column.

- It is now safe to unplug the removed BASE unit.

Replacing a NODE

In case of a malfunction, a NODE controller module can be switched with a new one. Push the orange button positioned between the LCD display and the outlets and remove the NODE controller module from the PDU. Afterwards a new module can be plugged into the PDU.

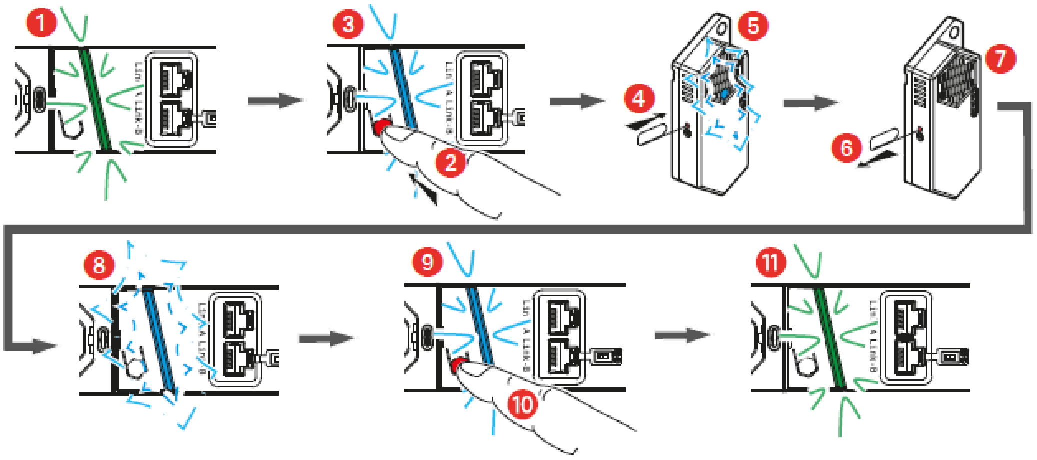
Connecting External Equipment (Optional)

More features are available if you connect external equipment to your NX1 PDU. This chapter will explain how to connect wireless sensors.

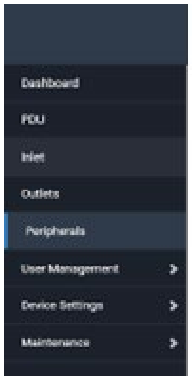
Pairing a wireless sensor

Follow the steps described below to pair a wireless sensor with your PDU:

1) The LED status indicator is green (initial state).
2) Press and release the pairing button on your NX1 PDU.
3) A blue LED will light up, indicating that the pairing button of the PDU is active.
4) Use a paperclip to press the pairing button of the wireless sensor.
5) The blue sensor LED with flash shortly.
6) Release the paper clip.
7) The sensor LED will go off.
8) The blue LED of the PDU will flash, indicating that the commission is in process.
9) You can now add more wireless sensors (steps 4 -7).
10) Press and release the pairing button on the PDU to close the pairing process.
11) The green LED on the PDU indicates that pairing is completed and PDU is ready for operation.

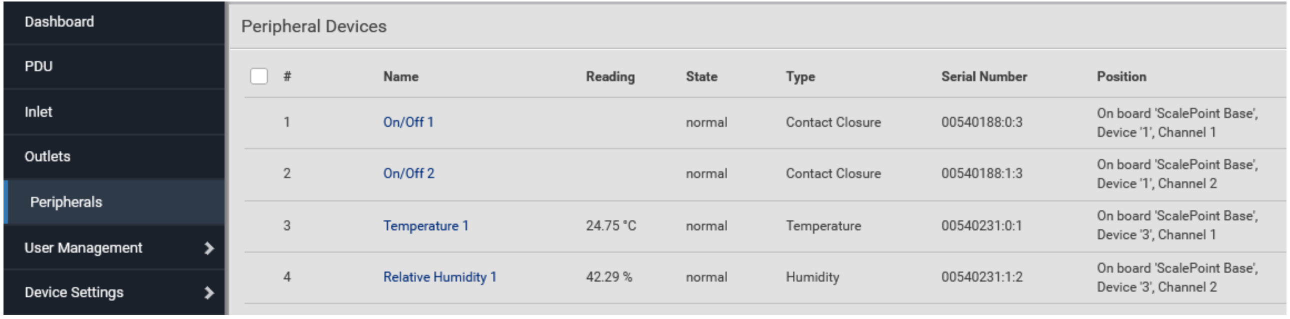


In the web interface of the PDU, go to Peripherals. Check if the sensor is listed in the Peripheral Devices list.



Note that there may be a 2-minute delay before the sensor will be available in the UI. Alternatively, you can press the pairing button on the long side of the sensor's casing. See Pairing Wireless Sensors. This will send out a data frame immediately, which will make the sensor visible in the Peripheral Devices list of the PDU.

In this example, 2 sensors were added (a contact sensor and a Temperature/Humidity sensor).



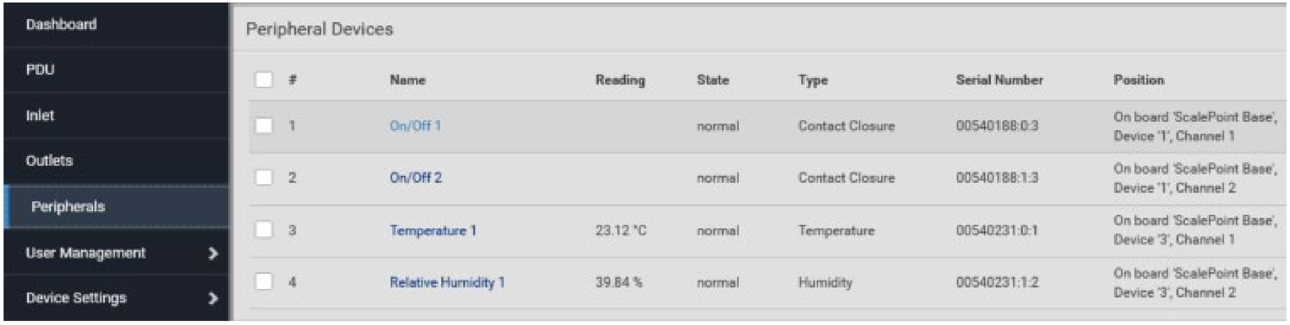
Peripheral Devices

#	Name	Reading	State	Type	Serial Number	Position
1	On/Off 1		normal	Contact Closure	00540188:0:3	On board 'ScalePoint Base', Device '1', Channel 1
2	On/Off 2		normal	Contact Closure	00540188:1:3	On board 'ScalePoint Base', Device '1', Channel 2
3	Temperature 1	24.75 °C	normal	Temperature	00540231:0:1	On board 'ScalePoint Base', Device '3', Channel 1
4	Relative Humidity 1	42.29 %	normal	Humidity	00540231:1:2	On board 'ScalePoint Base', Device '3', Channel 2

Note that each Sensor has 2 devices (2 devices On/Off for contact sensor, and device Temperature + Relative Humidity for Temperature/Humidity sensor).
The sensors send their data every 130 seconds.
In addition, the contact closure sensor sends information immediately in the event of a change of state.
A sensor will enter the status Unavailable if no data frame was received by the PDU for 60 minutes. This may be due to an empty battery or the sensor being out of range.

Manage parameters of contact sensors

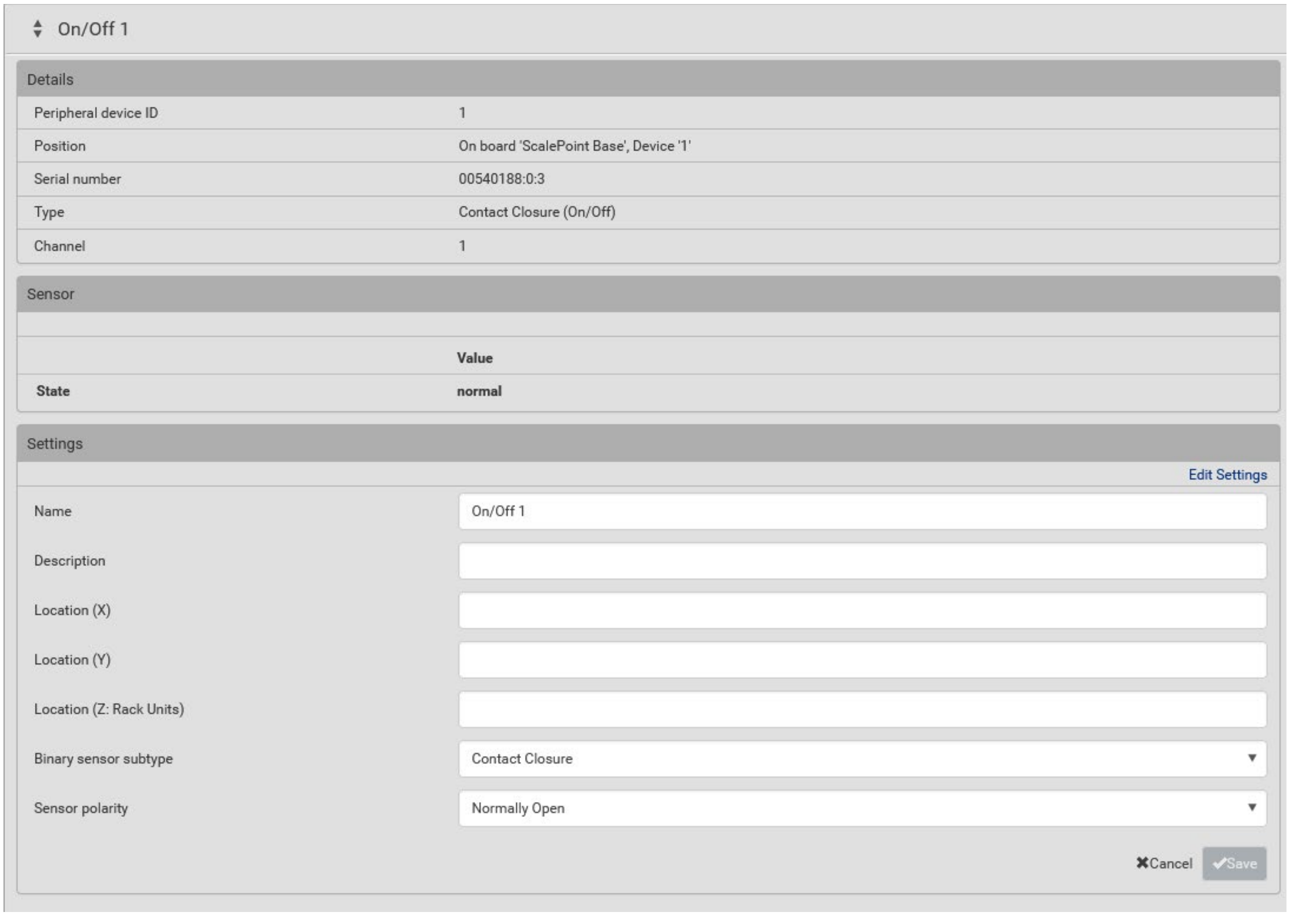
For configuration click on the peripheral device.
On/Off Device



Peripheral Devices

#	Name	Reading	State	Type	Serial Number	Position
1	On/Off 1		normal	Contact Closure	00540188:0:3	On board 'ScalePoint Base', Device '1', Channel 1
2	On/Off 2		normal	Contact Closure	00540188:1:3	On board 'ScalePoint Base', Device '1', Channel 2
3	Temperature 1	23.12 °C	normal	Temperature	00540231:0:1	On board 'ScalePoint Base', Device '3', Channel 1
4	Relative Humidity 1	39.84 %	normal	Humidity	00540231:1:2	On board 'ScalePoint Base', Device '3', Channel 2

For example, by clicking on the device **On/Off 1** opens the following configuration page:



On/Off 1

Details

Peripheral device ID	1
Position	On board 'ScalePoint Base', Device '1'
Serial number	00540188:0:3
Type	Contact Closure (On/Off)
Channel	1

Sensor

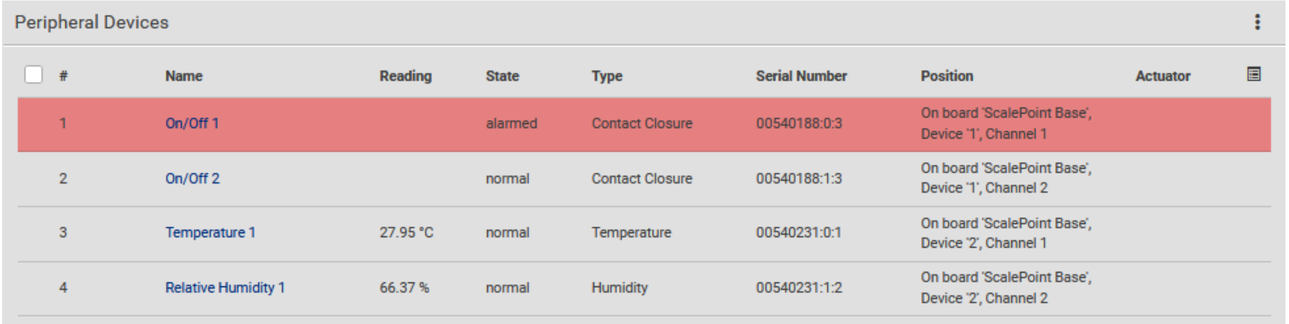
	Value
State	**normal**

Settings

Name	On/Off 1
Description	
Location (X)	
Location (Y)	
Location (Z: Rack Units)	
Binary sensor subtype	Contact Closure
Sensor polarity	Normally Open

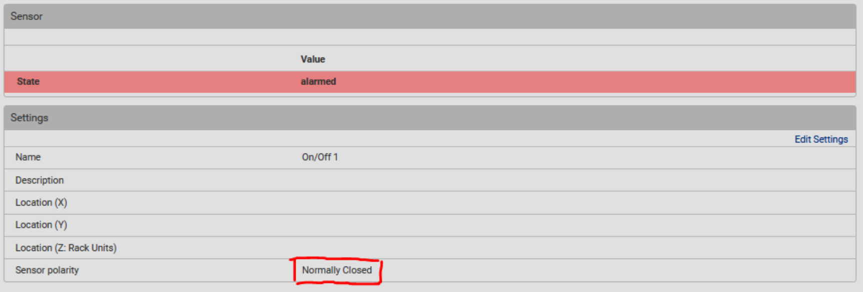
You can define its name, the description of this device, its location and the polarity of the device (Normally opened or Normally Closed).

If the contact is in an abnormal state, an alarm is triggered and is displayed in red on the webpage and the LED Base (see below).



Peripheral Devices

□ #	Name	Reading	State	Type	Serial Number	Position	Actuator
1	On/Off 1		alarmed	Contact Closure	00540188:0:3	On board 'ScalePoint Base', Device '1', Channel 1	
2	On/Off 2		normal	Contact Closure	00540188:1:3	On board 'ScalePoint Base', Device '1', Channel 2	
3	Temperature 1	27.95 °C	normal	Temperature	00540231:0:1	On board 'ScalePoint Base', Device '2', Channel 1	
4	Relative Humidity 1	66.37 %	normal	Humidity	00540231:1:2	On board 'ScalePoint Base', Device '2', Channel 2	

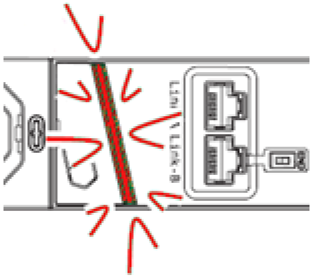


Sensor

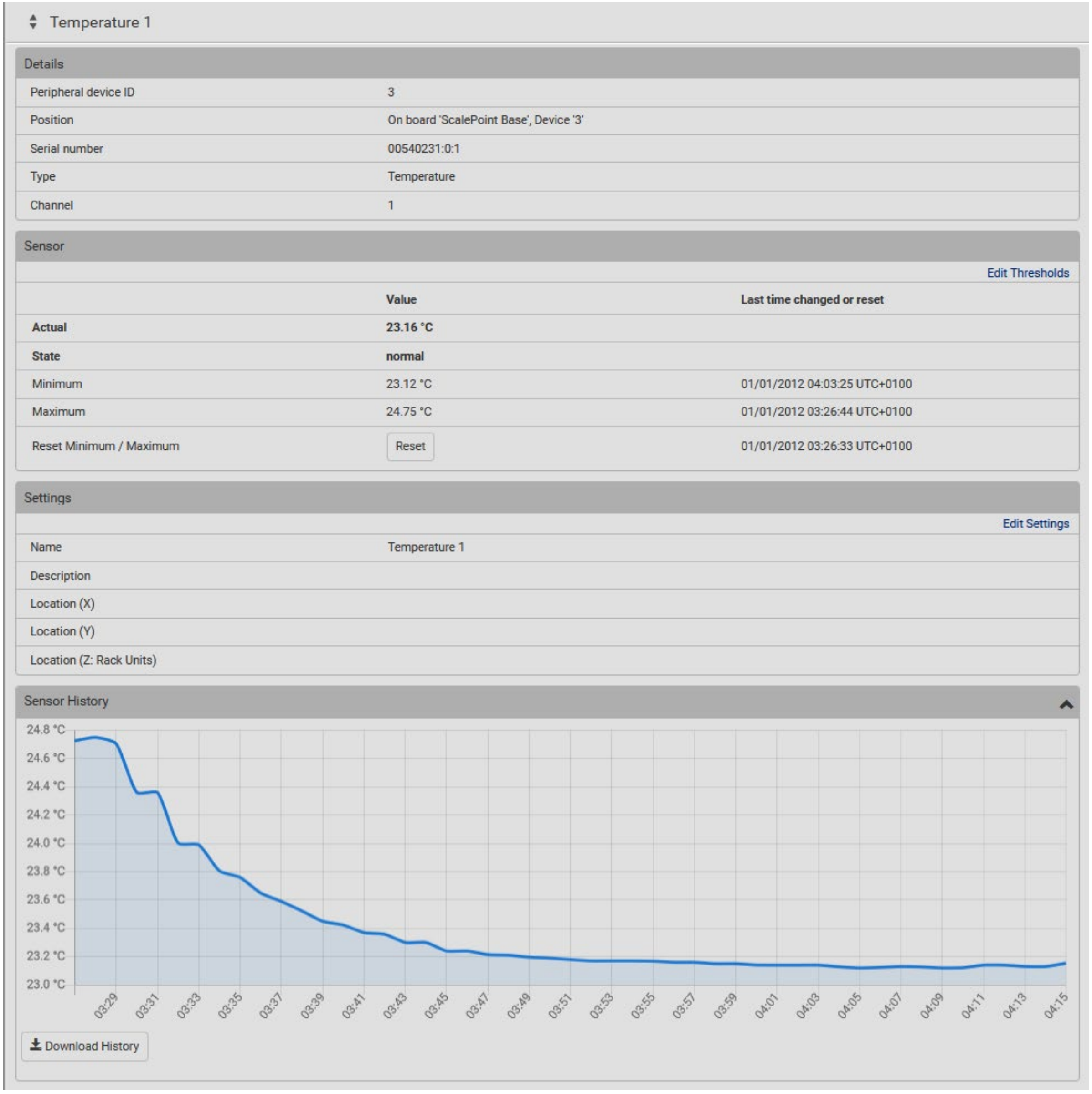
	Value
State	alarmed

Settings

Name	On/Off 1
Description	
Location (X)	
Location (Y)	
Location (Z: Rack Units)	
Sensor polarity	Normally Closed



Temperature Device



Temperature 1

Details

Peripheral device ID	3
Position	On board 'ScalePoint Base', Device '3'
Serial number	00540231:0:1
Type	Temperature
Channel	1

Sensor

Edit Thresholds

	Value	Last time changed or reset
Actual	**23.16 °C**	
State	**normal**	
Minimum	23.12 °C	01/01/2012 04:03:25 UTC+0100
Maximum	24.75 °C	01/01/2012 03:26:44 UTC+0100
Reset Minimum / Maximum	Reset	01/01/2012 03:26:33 UTC+0100

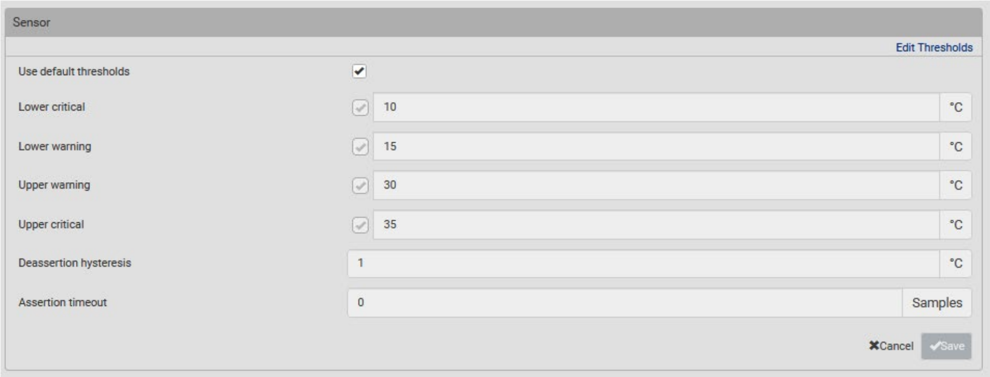
Settings

Edit Settings

Name	Temperature 1
Description	
Location (X)	
Location (Y)	
Location (Z: Rack Units)	

Sensor History

The sensor threshold can be managed in this part.

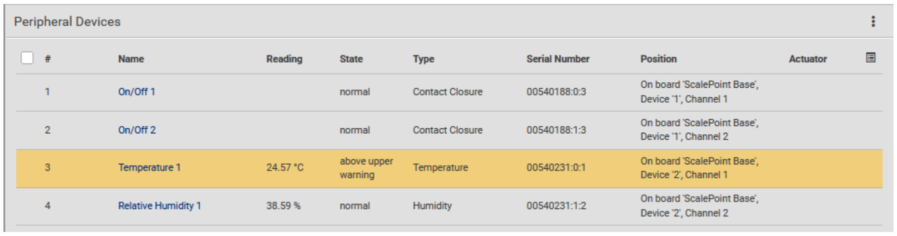


Sensor

Edit Thresholds

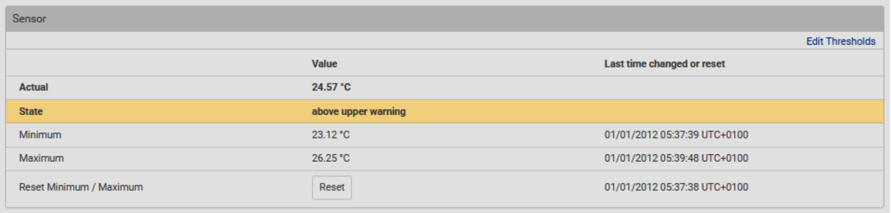
Use default thresholds	☑	
Lower critical	☑ 10	°C
Lower warning	☑ 15	°C
Upper warning	☑ 30	°C
Upper critical	☑ 35	°C
Deassertion hysteresis	1	°C
Assertion timeout	0	Samples

If lower/upper warning threshold is reached the orange alarm is show in webpage and LED of the Base.



Peripheral Devices

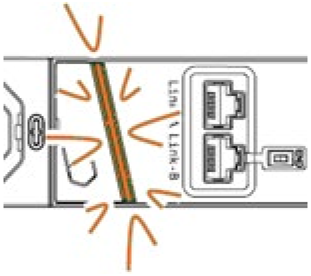
□	#	Name	Reading	State	Type	Serial Number	Position	Actuator
	1	On/Off 1		normal	Contact Closure	00540188:0:3	On board 'ScalePoint Base', Device '1', Channel 1	
	2	On/Off 2		normal	Contact Closure	00540188:1:3	On board 'ScalePoint Base', Device '1', Channel 2	
	3	Temperature 1	24.57 °C	above upper warning	Temperature	00540231:0:1	On board 'ScalePoint Base', Device '2', Channel 1	
	4	Relative Humidity 1	38.59 %	normal	Humidity	00540231:1:2	On board 'ScalePoint Base', Device '2', Channel 2	



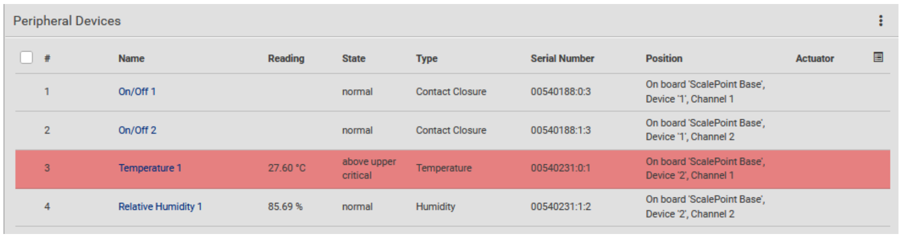
Sensor

Edit Thresholds

	Value	Last time changed or reset
Actual	24.57 °C	
State	above upper warning	
Minimum	23.12 °C	01/01/2012 05:37:39 UTC+0100
Maximum	26.25 °C	01/01/2012 05:39:48 UTC+0100
Reset Minimum / Maximum	Reset	01/01/2012 05:37:38 UTC+0100

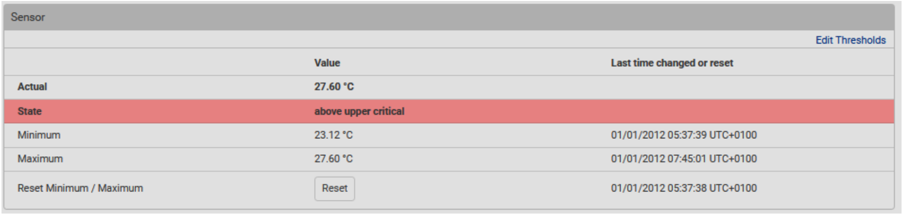


If lower/upper critical threshold is reached the red alarm is shown in webpage and LED of the Base.



Peripheral Devices

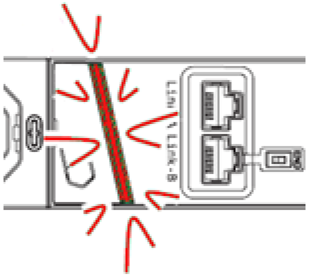
□	#	Name	Reading	State	Type	Serial Number	Position	Actuator
	1	On/Off 1		normal	Contact Closure	00540188:0:3	On board 'ScalePoint Base', Device '1', Channel 1	
	2	On/Off 2		normal	Contact Closure	00540188:1:3	On board 'ScalePoint Base', Device '1', Channel 2	
	3	Temperature 1	27.60 °C	above upper critical	Temperature	00540231:0:1	On board 'ScalePoint Base', Device '2', Channel 1	
	4	Relative Humidity 1	85.69 %	normal	Humidity	00540231:1:2	On board 'ScalePoint Base', Device '2', Channel 2	



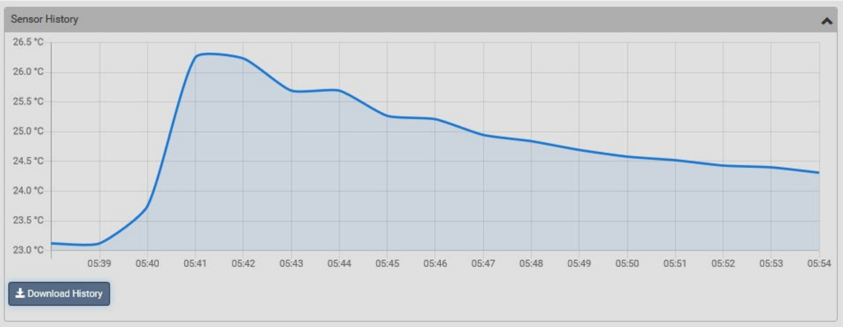
Sensor

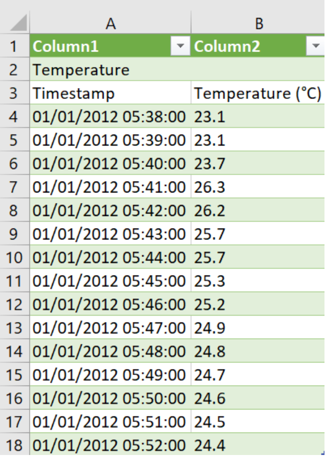
Edit Thresholds

	Value	Last time changed or reset
Actual	27.60 °C	
State	above upper critical	
Minimum	23.12 °C	01/01/2012 05:37:39 UTC+0100
Maximum	27.60 °C	01/01/2012 07:45:01 UTC+0100
Reset Minimum / Maximum	Reset	01/01/2012 05:37:38 UTC+0100



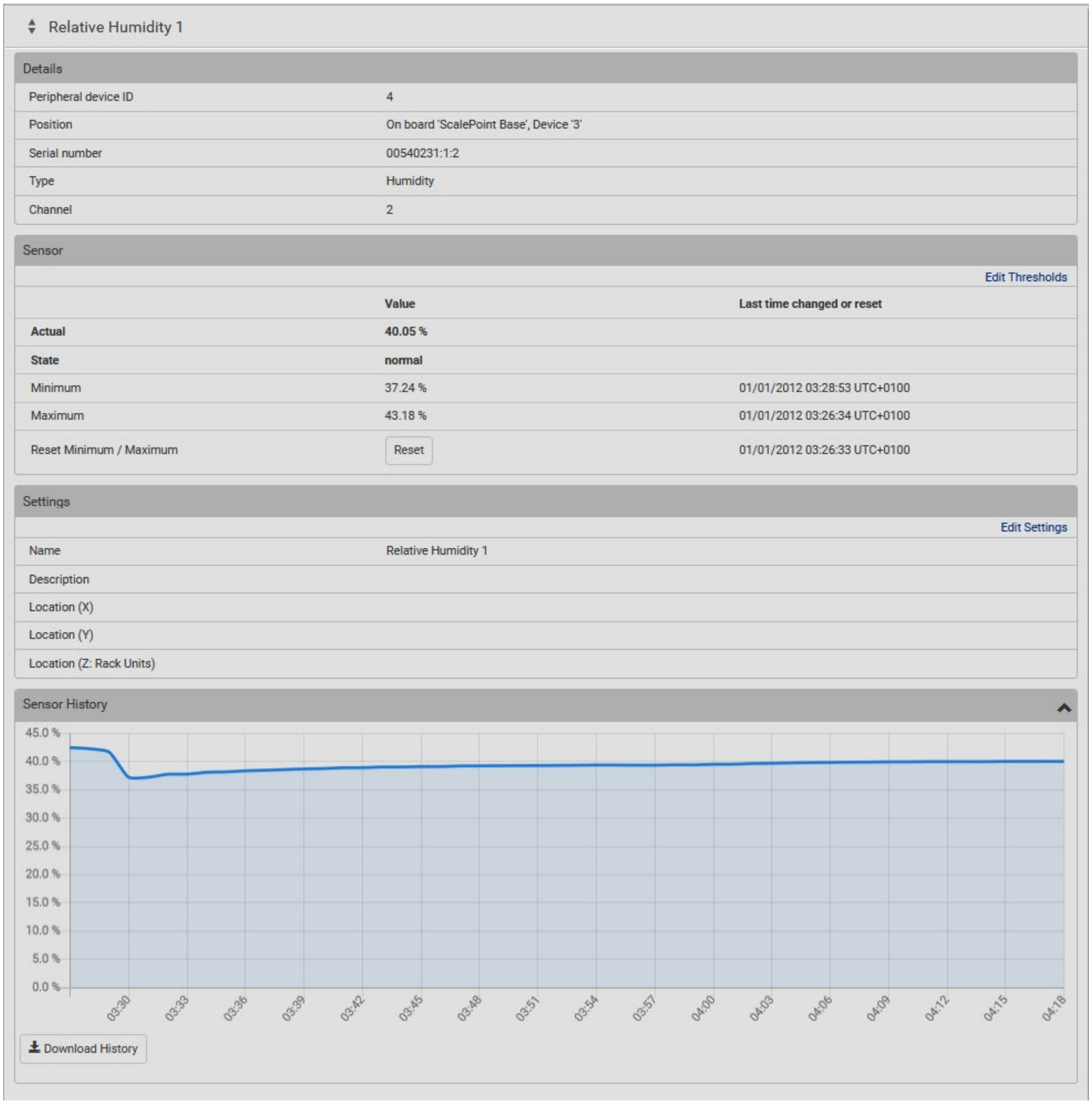
Temperature history is available as graphic or in a .csv file by clicking **Download History** button.





	A	B
1	Column1	Column2
2	Temperature	
3	Timestamp	Temperature (°C)
4	01/01/2012 05:38:00	23.1
5	01/01/2012 05:39:00	23.1
6	01/01/2012 05:40:00	23.7
7	01/01/2012 05:41:00	26.3
8	01/01/2012 05:42:00	26.2
9	01/01/2012 05:43:00	25.7
10	01/01/2012 05:44:00	25.7
11	01/01/2012 05:45:00	25.3
12	01/01/2012 05:46:00	25.2
13	01/01/2012 05:47:00	24.9
14	01/01/2012 05:48:00	24.8
15	01/01/2012 05:49:00	24.7
16	01/01/2012 05:50:00	24.6
17	01/01/2012 05:51:00	24.5
18	01/01/2012 05:52:00	24.4

Relative Humidity Device



Relative Humidity 1

Details

Peripheral device ID	4
Position	On board 'ScalePoint Base', Device '3'
Serial number	00540231:1:2
Type	Humidity
Channel	2

Sensor

Edit Thresholds

	Value	Last time changed or reset
Actual	**40.05 %**	
State	**normal**	
Minimum	37.24 %	01/01/2012 03:28:53 UTC+0100
Maximum	43.18 %	01/01/2012 03:26:34 UTC+0100
Reset Minimum / Maximum	Reset	01/01/2012 03:26:33 UTC+0100

Settings

Edit Settings

Name	Relative Humidity 1
Description	
Location (X)	
Location (Y)	
Location (Z: Rack Units)	

Sensor History

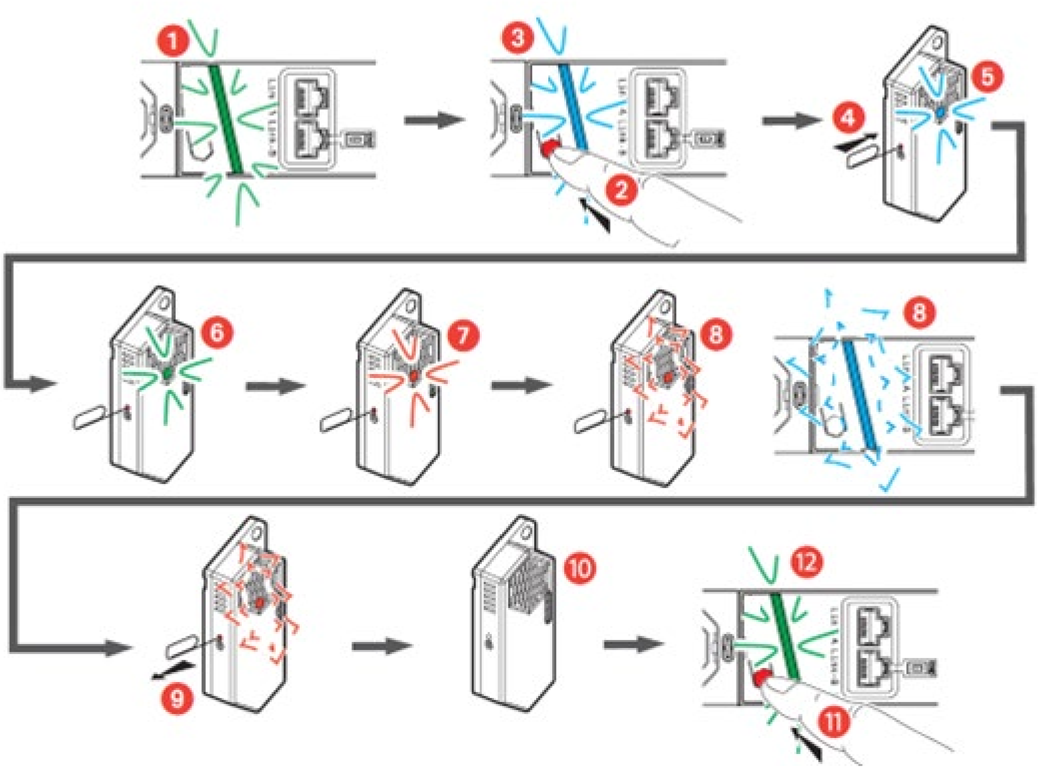
In the same way as with the Temperature Device, an orange alarm is shown in the Web GUI and the device LED if lower/upper warning thresholds are reached.

Reaching lower/upper critical warning thresholds will cause a red alarm shown in the Web GUI and the device LED.

Humidity historical information is available as graphic or in a .csv file by clicking **Download History** button.

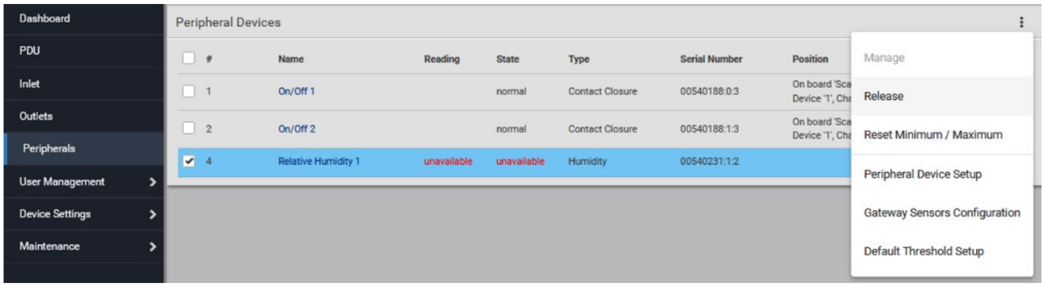
Unpairing sensors

The unpairing of a wireless sensor can be initiated by pressing the pairing button of both the sensor and PDU.



1) The Led status indicator on the PDU is green (initial state).
2) Press the pairing button on your NX1 PDU.
3) The LED turns blue.
4) Press and hold the pairing button of the wireless sensor with a paper clip.
5) Wait for the LED to light up blue,
6) then green
7) and red. Hold the button until the red LED blinked several times, then release.
8) The PDU LED acknowledges by flashing blue.
9) Release the push button of the sensor.
10) The contact sensor LED is Off.
11) Press once again the pairing button on the PDU.
12) LED on PDU goes green (end of pairing process). The removal process of the wireless sensor is now complete.

Check the Peripheral Devices list on the Web Interface of your PDU to see if it was successfully removed from the list. Click on ⋮ to access to parameters information and select **Release** to remove the device from the list.



Peripheral Devices

□	#	Name	Reading	State	Type	Serial Number	Position
□	1	On/Off 1		normal	Contact Closure	00540188:0:3	On board 'Sca Device '1', Cha
□	2	On/Off 2		normal	Contact Closure	00540188:1:3	On board 'Sca Device '1', Cha
☑	4	Relative Humidity 1	unavailable	unavailable	Humidity	00540231:1:2	

Introduction to PDU Components

This chapter explains how to use the NX1 PDU, including:

- Introduction to the LEDs and ports on the PDU
- Operation of the front panel display
- The overcurrent protector's behavior
- Resetting the PDU

Panel Components

NX1 PDU comes in Zero U and 1U sizes. All types of models come with the following components on the outer panels.

- Inlet
- Outlets
- Connection ports
- Dot-matrix LCD display

► *Inlet*

Connect each NX1 PDU to an appropriately rated branch circuit. Refer to the label or nameplate affixed to your NX1 PDU for appropriate input ratings or range of ratings.

There is no power switch on the NX1 PDU. To power cycle the PDU, unplug it from the branch circuit, wait 10 seconds and then plug it back in.

► *Outlets*

The total number of outlets varies from model to model.

NX1 Switched PDU

These models are outlet-switching capable. A small LED is adjacent to each outlet to indicate the state of the relay board.

LED state	Outlet status	What it means
Not lit	Powered OFF	The outlet is turned off and no power is available. OR the control circuitry's power supply is broken. OR the outlet's associated circuit breaker has tripped.
GREEN	ON and LIVE	LIVE power. The outlet is on and power is available.

NX1 Metered PDU

These models are NOT outlet-switching capable, so all outlets are always in the ON state. Outlet LEDs are not available.

Connection Port Functions

► *PDU Node*

A NX1 NODE PDU has 4 ports.

► *4 front panel ports:*

- LINK port x 1
- USB-A port x 1
- USB-B port x 1
- Ethernet port x 1 (10/100)

► *PDU Base*

A NX1 BASE PDU has 2 ports.

- LINK-A port x 1
- LINK-B port x 1

► *Port functions:*

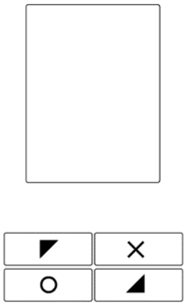
The table below explains the function of each port.

Port	Used for
USB-B	Cascading NX1 Node PDUs for sharing a network connection. Establishing a USB connection between a computer and the NX1 PDU for: Using the command line interface "CLI".
USB-A	This is a "host" port, which is powered. Connecting a USB flash device. Cascading NX1 PDUs for sharing a network connection.
LINK (RJ-45)	Cascading NX1 PDUs over RS-485 Link Chain

ETH 10/100	NX1 PDU has one Ethernet port, supporting up to 100 Mbps. Connecting the NX1 PDU to your company's network via a standard network patch cable This connection is necessary to administer or access the NX1 PDU remotely. There are two small LEDs adjacent to the port: Green indicates a physical link and activity. Yellow indicates communications at 10/100 BaseT speeds. Note: Network connection to this port is not required if the NX1 PDU is a link unit in the cascading configuration.

Front Panel Display

The following diagram shows the dot-matrix LCD display panel on a NODE unit module.



You can use the LCD display to view the PDU information. It consists of:

- A dot-matrix LCD display
- Four control buttons

If the orientation of your Zero U model's LCD content does not meet your need, you can manually change it and stick to the orientation. See Manually Changing NX1 PDU's Zero U LCD Orientation.

Note: All dot-matrix LCD display diagrams illustrated in the Online Help are for Zero U models. Your dot-matrix LCD may look slightly different if it is on a 1U model.

Automatic and Manual Modes

After powering on or resetting the NX1 PDU, the front panel LCD display first shows some dots, then Raritan logo and finally enters the automatic mode.

▶ *Automatic mode without alerts available:*

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

If overcurrent protectors are available on your NX1 PDU, the display cycles between both the inlet and overcurrent protector information.

Note: You can make a NX1 PDU with overcurrent protectors show the inlet information only in the automatic mode.

▶ *Manual mode:*

To view more information or control outlets if your NX1 PDU is outlet-switching capable, enter the manual mode.

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

To return to the automatic mode, press ✕ once or multiple times.

▶ *When an alert exists:*

- In the automatic mode, when an alert occurs, the LCD display stops cycling through information, and warns you by showing the alerts notice listed in a bold font.

To enter the manual mode, press ✕ .

- In the manual mode, alerts will be listed.

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

Operating the Dot-Matrix LCD Display

Enter manual mode when you want to operate the dot-matrix LCD display. You can use the dot-matrix LCD display to:

- Show information of the NX1 PDU, built-in components, or connected peripheral devices

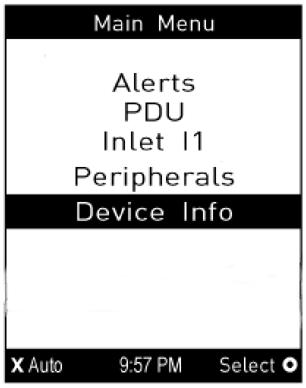
Main Menu

The Main Menu contains 5 to 8 menu commands, depending on the model.

Control buttons that can be used and the system time are shown at the bottom of the LCD display.

► *NX1 PDU LCD Main Menu (Zero U):*

If any alerts exist, it will be listed on the display in a bold font.



Menu command	Function
Alerts	Indicates all alerted sensors, if any.
PDU	Shows the PDU information (Rated voltage, current, power...). If Base PDUs are cascaded using RS485, shows basic information about each cascaded PDU.
Inlet I1	Shows the inlet I1's information.
OCPs	Shows a list of overcurrent protector information.
Outlets	This menu command is available on Switched PDUs only. Shows each outlet's information. If your PDU supports outlet-switching, you can turn on, off or power cycle an outlet.

Peripherals	Shows the information of connected environmental sensors, such as the temperature sensor.
Device Info	Shows the device information, such as IP and MAC address. See Device Info.

Alerts

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

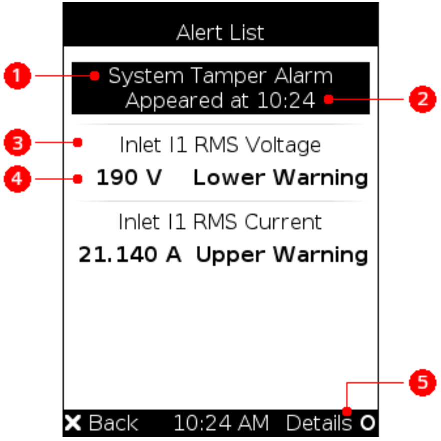
- Any numeric sensor that enters the warning or critical range if the thresholds have been enabled
- State sensors that enter the alarmed state

Tip: The same information is available in the web interface's Dashboard.

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

► *To view alerted sensors:*

- Press ◤ or ◢ to select "Alerts" in the Main Menu, and press ○.
- Alerted sensors, if any, will be listed.



Alert List

System Tamper Alarm
Appeared at 10:24

Inlet I1 RMS Voltage
190 V Lower Warning

Inlet I1 RMS Current
21.140 A Upper Warning

✕ Back 10:24 AM Details ○

Number	Description
1	Alarm names.
2	The time the alarm occurred. If the alarm occurred at least two times, then more information is shown. Number of alarms The first occurrence time The last occurrence time
3	Alerted sensor names.

4	Sensor readings and/or states. A numeric sensor shows both the reading and state. A state sensor shows the state only. Available states are listed below. For further information Alarmed Lower Critical = below lower critical Lower Warning = below lower warning Upper Warning = above upper warning Upper Critical = above upper critical Open (only available for NX1 PDUs with overcurrent protectors)
5	The 'Details' command appears for alarms only. If your Alert List comprises alerted sensors only, then 'Details' is not shown.

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

- (Optional) If there are alarms in the Alert List, you can perform the following operations.
- Press ○ to view detailed information of the alarm.
- (Optional) If the alarm occurred more than one time, the numbers of current page and total pages are shown in the top-right corner, similar to the above diagram. Press ◤ or ◢ to view the information of other occurrences.
- To acknowledge all alarms now, press ○ .

PDU

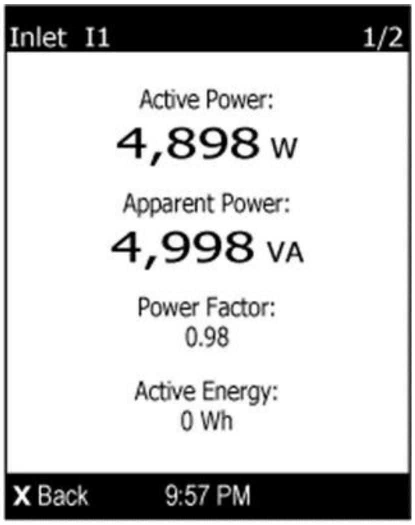
- Press ◤ or ◢ to select "PDU" in the Main Menu, and press ○ .
- It will display the active energy on the entire PDU and for the circuits.
- To return to the Main Menu, press ✕ .

Inlet

An inlet's information is divided into two pages. Page numbers are indicated in the top-right corner of the LCD display.

► *To show the inlet information:*

- Press ◤ or ◢ to select "Inlet I1" in the Main Menu, and press ○ .
- The first page shows the inlet's active power (W), apparent power (VA), power factor (PF), and active energy (Wh).



Inlet I1 1/2

Active Power:
4,898 W

Apparent Power:
4,998 VA

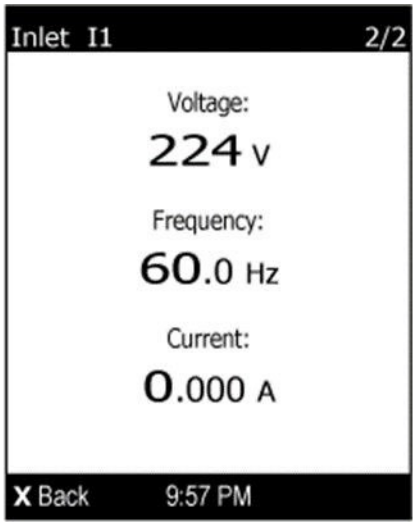
Power Factor:
0.98

Active Energy:
0 Wh

X Back 9:57 PM

To go to other page(s), press ◤ or ◢ .

- For a single-phase model, the second page shows the inlet's voltage (V), frequency (Hz) and current (A).



Inlet I1 2/2

Voltage:
224 V

Frequency:
60.0 Hz

Current:
0.000 A

X Back 9:57 PM

For a three-phase model, the next several pages respectively show unbalanced current's percentage, line frequency, and the current and voltage values of each line.

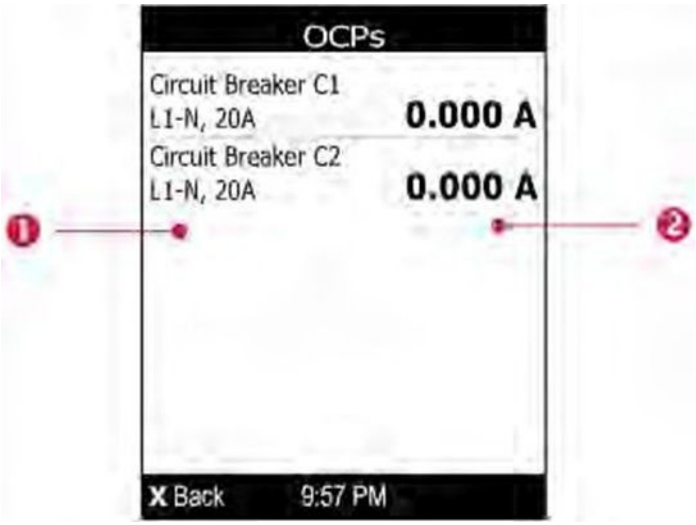
- To return to the Main Menu, press ✕ .

OCPs

If your model has more overcurrent protectors (OCPs) than the LCD display can show at a time, a page number appears in the top-right corner of the display. Otherwise, no page numbers are available.

► *To show the overcurrent protector information:*

- Press ◤ or ◢ to select "OCPs" in the Main Menu, and press ○ .
- The LCD display shows a list of overcurrent protectors like the following diagram.



OCPs

Circuit Breaker C1
L1-N, 20A 0.000 A

Circuit Breaker C2
L1-N, 20A 0.000 A

Number	Description
1	Overcurrent protector names. Associated lines and rated current are displayed below each overcurrent protector's name.
2	Current reading of the corresponding overcurrent protector.

- If the desired overcurrent protector is not visible, press ◤ or ◢ to scroll up or down.

Outlets

This outlet-related section applies to Switched PDUs only.

With the front panel display, you can do the following for outlets:

- Show each outlet's information.

Multiple outlet information can be displayed on the LCD display.

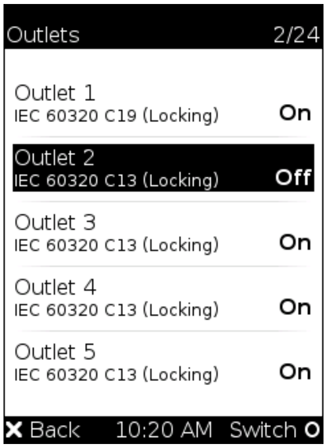
Control buttons that can be used and the system time are shown at the bottom of the LCD display.

► *To show outlets information:*

- Press ◤ or ◢ to select "Outlets" in the Main Menu, and press ○ .
- The LCD display shows a list of outlets with their receptacle types, and power states which are indicated by the status to the right of the outlet.

The currently-selected outlet number and total of outlets are indicated in the top-right corner of the display.

- ON indicates that this outlet is powered on.
- OFF indicates that this outlet is powered off.



Outlets 2/24

Outlet 1
IEC 60320 C19 (Locking) On

Outlet 2
IEC 60320 C13 (Locking) Off

Outlet 3
IEC 60320 C13 (Locking) On

Outlet 4
IEC 60320 C13 (Locking) On

Outlet 5
IEC 60320 C13 (Locking) On

✕ Back 10:20 AM Switch ○

- Press ◤ or ◢ to select an outlet, and press ○ .
- If the desired outlet is not visible, press ◤ or ◢ to scroll up or down.
- To return to the Main Menu, press ✕ several times until the Main Menu is shown.

Outlet Groups

This outlet related section applies to Switched PDUs only.

You can do the following on the front panel display:

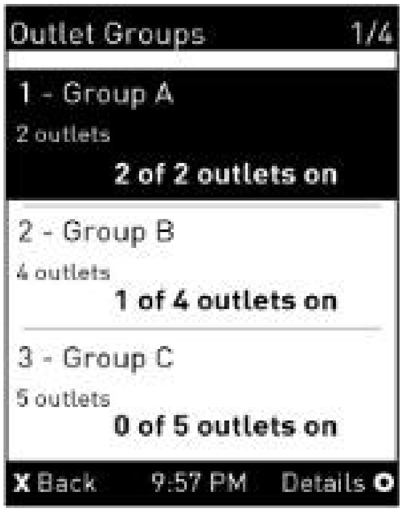
- Show each outlet group's information, including each member outlet of a group.

If any outlet group has been created, the front panel then shows a list of these groups and their status.

Control buttons that can be used and the system time are shown at the bottom of the LCD display.

► *To show an outlet group's information:*

- Press ◤ or ◢ to select "Outlet Groups" in the Main Menu, and press ○
- The LCD display shows a list of outlet groups with the information below:
- The total number of outlets in the group
- The total number of outlets that are turned ON in the group



Outlet Groups 1/4

1 - Group A
2 outlets
2 of 2 outlets on

2 - Group B
4 outlets
1 of 4 outlets on

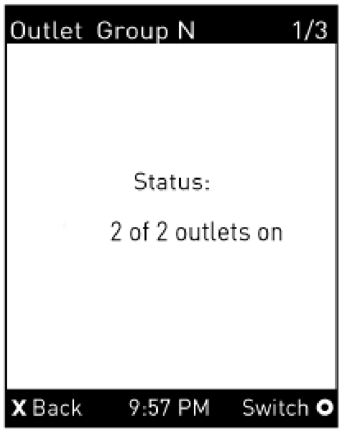
3 - Group C
5 outlets
0 of 5 outlets on

X Back 9:57 PM Details ○

The currently-selected outlet group's number and total of outlet groups are indicated in the top-right corner of the display, such as "1/4" in the above diagram.

- Press ◤ or ◢ to select an outlet group, and press ○ .
- If the desired outlet group is not visible, press ◤ or ◢ to scroll up or down.
- The LCD display shows the selected outlet group's power state.

Note: In the following diagrams, N represents the selected outlet group's index number. The rightmost number in the title bar represents this group's total pages.



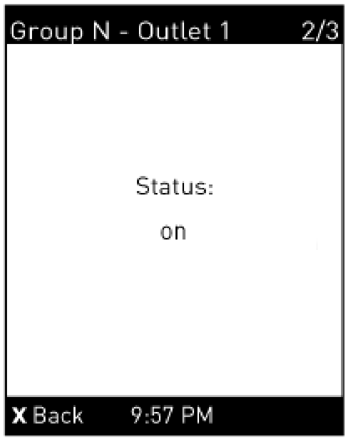
Outlet Group N 1/3

Status:

2 of 2 outlets on

X Back 9:57 PM Switch ○

- To check the status of each member outlet of the group, press ◤ or ◢.



Group N - Outlet 1 2/3

Status:

on

X Back 9:57 PM

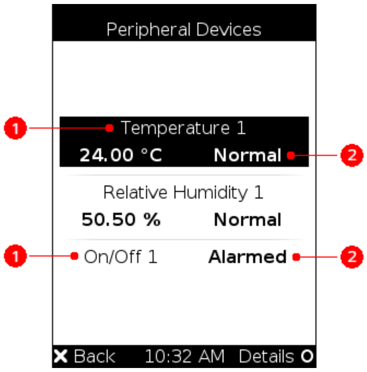
- To return to the Main Menu, press ✕ several times until the Main Menu is shown.

Peripherals

If there are no environmental sensors connected to your NX1 PDU, the LCD display shows the message "No managed devices" for the "Peripherals" menu command.

► *To show environmental sensor information:*

- Press ◤ or ◢ to select "Peripherals" in the Main Menu, and press ○.
- The display shows a list of environmental sensors.
- If the desired sensor is not visible, press ◤ or ◢ to scroll up or down.
- When the list exceeds one page, the currently-selected sensor's ID number and total of managed sensors are indicated in the top-right corner of the display.
- If any sensor enters the warning, critical, or alarmed state, like 'Tamper Detector 1' shown below, it will be listed in the GUI.



Peripheral Devices

Temperature 1
24.00 °C Normal

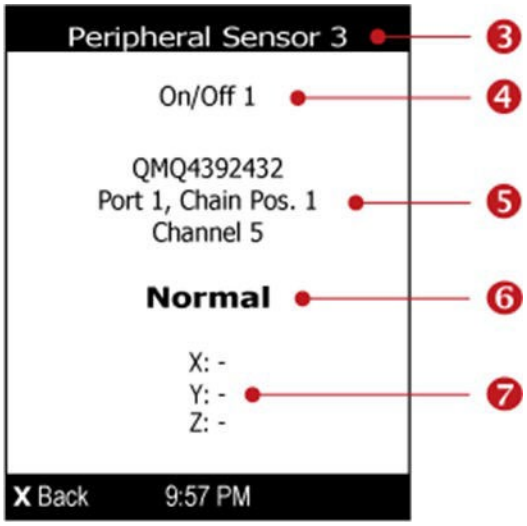
Relative Humidity 1
50.50 % Normal

On/Off 1 Alarmed

✕ Back 10:32 AM Details O

Number	Description
1	Sensor names.
2	Sensor states as listed below. n/a = unavailable Normal Alarmed Lower Critical = below lower critical Lower Warning = below lower warning Upper Warning = above upper warning Upper Critical = above upper critical On Off Open Closed A numeric sensor shows both the reading and state. A state sensor shows the state only.

- To view an environmental sensor's detailed information, press ◤ or ◢ to select that sensor, and press ○ . A screen like the following is shown.



Peripheral Sensor 3

On/Off 1

QMQ4392432
Port 1, Chain Pos. 1
Channel 5

Normal

X: -
Y: -
Z: -

X Back 9:57 PM

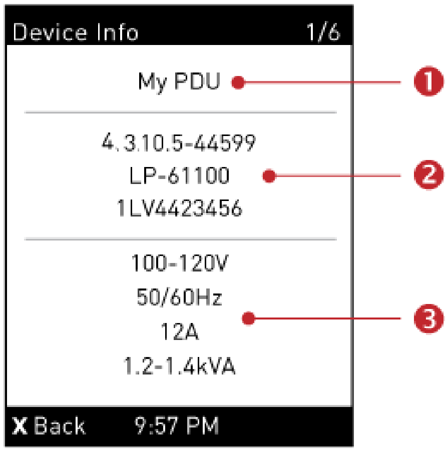
Number	Description
3	The ID number assigned to this sensor. A sensor shows "Peripheral Sensor x" (x is the ID number)
4	Sensor name.
5	The following information is listed. Serial number
6	Depending on the sensor type, any of the following information is displayed: State of a state sensor: Normal, Alarmed, Open or Closed. Reading of a numeric sensor.
7	X, Y, and Z coordinates which you specify for this sensor.

Device Info

The display shows the device's information, network and IPv4/IPv6 settings through various pages. Page numbers are indicated in the top-right corner of the LCD display.

► *To show the device information:*

- Press ◤ or ◢ to select "Device Info" in the Main Menu, and press ○ .
- Device information similar to the following diagram displays.



Device Info 1/6

My PDU

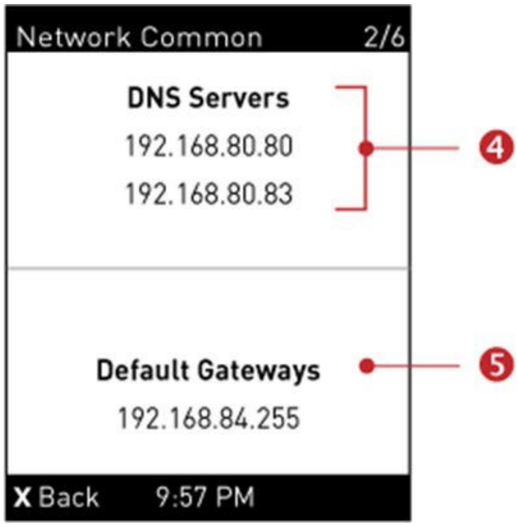
4.3.10.5-44599
LP-61100
1LV4423456

100-120V
50/60Hz
12A
1.2-1.4kVA

X Back 9:57 PM

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

- Press ◢ to show the Network Common page.



Network Common 2/6

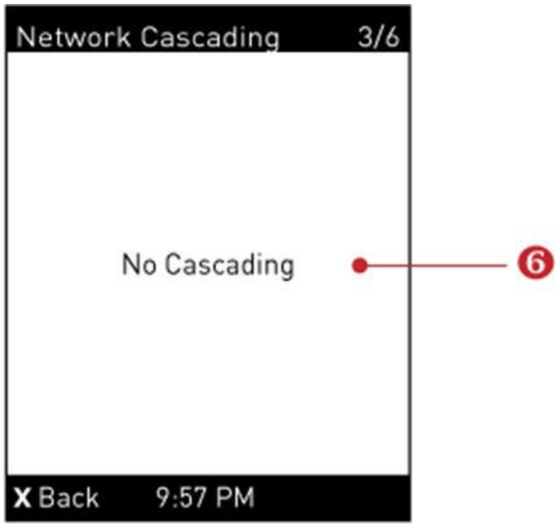
DNS Servers
192.168.80.80
192.168.80.83

Default Gateways
192.168.84.255

X Back 9:57 PM

Number	Description
4	DNS servers.
5	Default gateways.

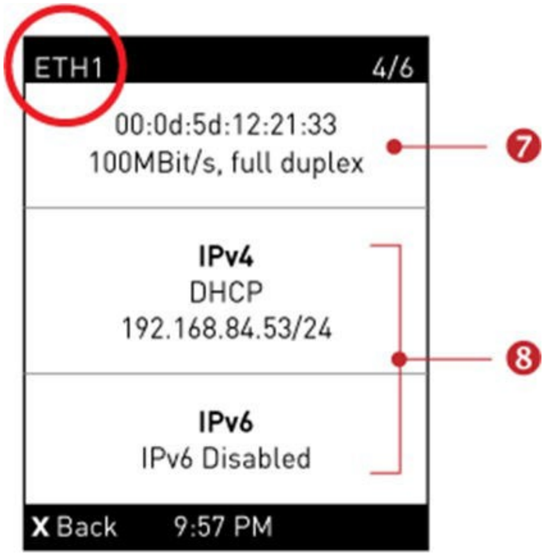
- Press ◢ to show the Network Cascading page.



Number	Description
6	Cascading status, which can be one of the following: No Cascading: This device's cascading mode is set to none. Port Forwarding Primary: This device's cascading mode is set to Port Forwarding, and it is a primary unit. Link Unit Connected: Indicates whether the presence of a link unit is detected - yes or no. Port Forwarding Link: This device's cascading mode is set to Port Forwarding, and it is a link unit. Link Unit Connected: Indicates whether the presence of a link unit is detected - yes or no. Cascade Position: Indicates the position of a link unit in the Port Forwarding mode. 1 represents Link Unit 1, 2 represents Link Unit 2, and so on. A port forwarding link unit will also display primary unit 's IP address on this page.

Press ◢ to show the Ethernet page.

A NX1 PDU has one Ethernet page – ETH1.



00:0d:5d:12:21:33
100MBit/s, full duplex

IPv4
DHCP
192.168.84.53/24

IPv6
IPv6 Disabled

9:57 PM

Number	Description
7	Ethernet interface information, including: MAC address. Speed. Full or half duplex.
8	IPv4/IPv6 network information, including: Network configuration: DHCP (or Automatic), or Static. Static represents Static IP. IP address. Prefix length, such as "/24". Note: If you disable any Ethernet interface, a message 'Interface Disabled' is shown.

If you do not enable IPv4/IPv6 settings, an 'IPv4 (or IPv6) Disabled' message is displayed.

Manually Changing NX1 PDU's Zero U LCD Orientation

If the LCD's orientation does not meet your need, you can manually configure it. The factory default is 0 degree orientation, common on 0U PDUs.

► *To set up the LCD orientation:*

- Press ◤ or ◢ simultaneously until you see the LCD shows "Fixed Orientation".
- If the current LCD orientation does not meet your need, repeat the above step until the orientation you preferred is displayed.

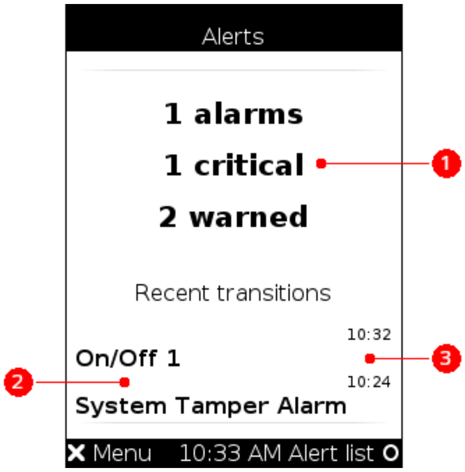
Alerts Notice

In the automatic mode, if an alert occurs, the LCD display automatically shows a notice in bold font indicating the alert levels, the total number of alerted sensors and information of the latest transitions.

- When all alerted sensors enter the warning levels, they will be listed in a bold font on the screen.
- When at least one of the alerted sensors enters the critical level or there is any "alarm", a bold 'critical' notice will appear on the screen.

The following illustrates the alerts notices.

► *When there are only alerted sensors -- NO ALARMS are present:*



Alerts

1 alarms

1 critical

2 warned

Recent transitions

10:32

On/Off 1

10:24

System Tamper Alarm

✕ Menu 10:33 AM Alert list ○

Number	Description
1	The total of alerted sensors in critical and warning levels.
2	A list of final alerted sensors that changed their readings or states.
3	The final time that each alerted sensor updated its readings or states.

► *When there is any alarm present:*

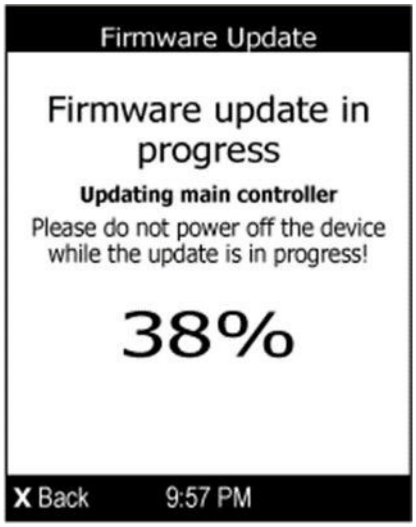
The LCD display looks like the above diagram except that it shows the alarm(s) and the available command in the bottom-right corner is 'Actions' instead of 'Alert list'.

► *Available operations:*

- For the notice listing alerted sensors only, press ○ to view a list of all alerted sensors. See Alerts.
- For the notice where at least an alarm is present, press ○ . Then do the following:
- Two options display. Press ◤ or ◢ to select either option, and press ○ .
- Show alert list: This option lists all alerted sensors and alarms. You still can choose to acknowledge alarms after viewing the list. See Alerts.
- Acknowledge all alarms: This option immediately acknowledges all existing alarms, without showing the list of alarms.
- (Optional) If 'Acknowledge all alarms' is selected in the above step, a confirmation prompt similar to the diagram below appears. Press ◤ or ◢ to confirm or abort the operation, and press ○ .

Showing the Firmware Upgrade Progress

When upgrading the NX1 PDU, the firmware upgrade progress will be displayed as a percentage on the LCD display, like the following diagram.



Firmware Update

Firmware update in progress

Updating main controller

Please do not power off the device while the update is in progress!

38%

In the end, a message appears, indicating whether the firmware upgrade succeeded or failed.

Restarting the PDU

To restart the PDU, you can unplug the device from the chassis. Wait a few seconds then plug it in again and wait until the PDU has restarted. Please note that this procedure does not reset any settings within the PDU.

Note: Do NOT unplug NODE while firmware update!

Alternatively, you can reset the PDU using the CLI command line.

Circuit Breakers

NX1 PDU models rated over 16A or 32A contain overcurrent protectors for outlets, which are usually branch circuit breakers. These circuit breakers automatically trip (disconnect power) when the current flowing through the circuit breaker exceeds its rating.

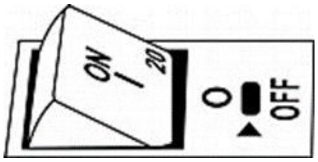
When a circuit breaker trips, power flow ceases to all outlets connected to it. You must manually reset the circuit breaker so that affected outlets can resume normal operation.

Resetting the Button-Type Circuit Breaker

Your button-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

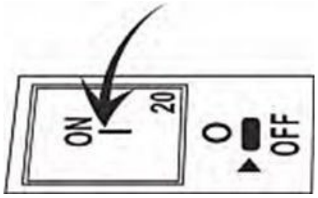
► *To reset the button-type breakers:*

- Locate the breaker which ON button is up, indicating that the breaker has tripped.



Examine your NX1 PDU and the connected equipment to remove or resolve the cause that results in the overload or short circuit. This step is required, or you cannot proceed with the next step.

- Press the ON button until it is completely down.



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

- Firefox® 52 and later
- Safari® (Mac)
- Google® Chrome® 52 and later
- Android 4.2 and later
- iOS 7.0 and later
- Edge (Windows 10, 11 (chrome-based versions))

Login, Logout and Password Change

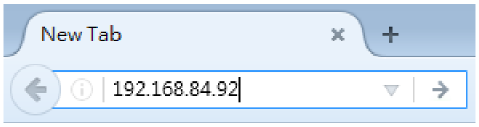
The first time you log in, use the factory default "admin" user credentials. For details, refer to the Quick Setup Guide accompanying the product. Password change is forced upon first login.

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 NX1 PDU
   - 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) Enter your user name and password, accept any security agreement displayed, and click Login.
4) 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.

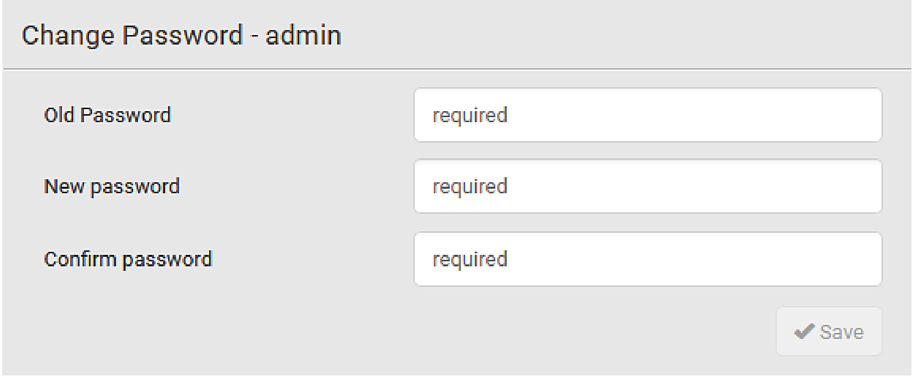
- ▶ *Password change required on first login:*

- 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.

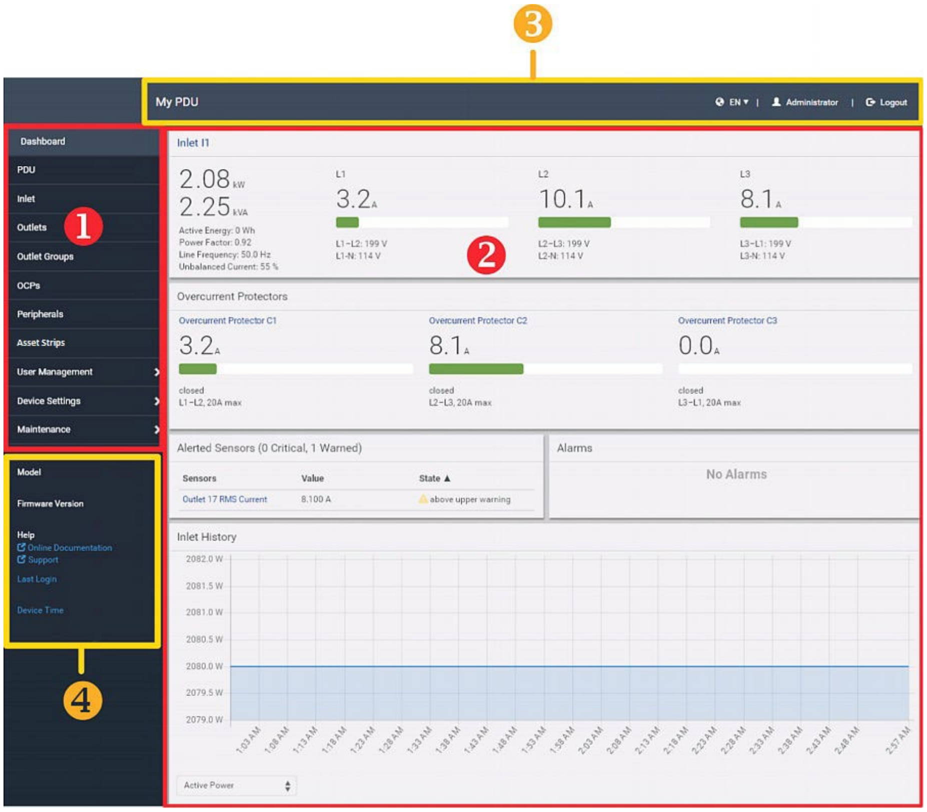
- Choose User Management > Change Password. Change the password and click Save.


Change Password - admin

Old Password	required
New password	required
Confirm password	required

Web Interface Overview

The web interface consists of four areas as shown below.



Inlet I1

2.08 kW
2.25 kVA
Active Energy: 0 Wh
Power Factor: 0.92
Line Frequency: 50.0 Hz
Unbalanced Current: 55 %

L1
3.2 A
L1–L2: 199 V
L1-N: 114 V

L2
10.1 A
L2–L3: 199 V
L2-N: 114 V

L3
8.1 A
L3–L1: 199 V
L3-N: 114 V

Overcurrent Protectors

Overcurrent Protector C1
3.2 A
closed
L1–L2, 20A max

Overcurrent Protector C2
8.1 A
closed
L2–L3, 20A max

Overcurrent Protector C3
0.0 A
closed
L3–L1, 20A max

Alerted Sensors (0 Critical, 1 Warned)

Sensors	Value	State ▲
Outlet 17 RMS Current	8.100 A	⚠ above upper warning

Alarms

No Alarms

Number	Web interface element
❶	*Menu* - Not all models support all menu options.
❷	Data/setup page of the selected menu item.
❸	• Left side: - NX1 PDU device name. • Right side: - Displayed language, which is English (EN) by default. You can change it. - Your login name, which you can click to view your user account settings. - Logout button.

❹	From top to bottom -- • Your NX1 PDU model. • Current firmware version. • Online Documentation: link to the online help. • Support: link to Technical Support. • Date and time of your user account's last login.
	- Click Last Login to view your login history. • NX1 PDU system time, which is converted to the time zone of your computer or mobile device. - Click Device Time to open the Date/Time setup page.

Menu

Depending on your model and hardware configuration, your NX1 PDU may show all or some menu items shown below.

Menu	**Information shown**
Dashboard	Summary of the NX1 PDU status, including a list of alerted sensors and alarms, if any.
PDU	Device data and settings, such as the device name and MAC address.
Inlet	Inlet status and settings, such as inlet thresholds.
Outlets	Outlet status, settings and outlet control if your model is outlet-switching capable.
Outlet Groups	Only PDUs with outlet-switching feature show this menu item. You can create groups of outlets. Functions that you can perform on an outlet group vary depending on the model you purchased.
OCPs	The OCPs menu item displays only if your model is equipped with overcurrent protectors. OCP status and settings, such as OCP thresholds.
Peripherals	Status and settings of environmental sensor packages, if connected.
User Management	Data and settings of user accounts and groups, such as password change.
Device Settings	Device-related settings, including network, security, system time, event rules and more.
Maintenance	Device information and maintenance commands, such as firmware upgrade, device backup and reset.

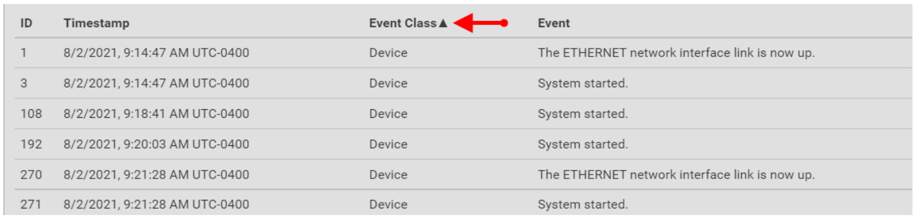
Quick Access to a Specific Page

If you often visit a specific page in the NX1 PDU 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
1	8/2/2021, 9:14:47 AM UTC-0400	Device	The ETHERNET network interface link is now up.
3	8/2/2021, 9:14:47 AM UTC-0400	Device	System started.
108	8/2/2021, 9:18:41 AM UTC-0400	Device	System started.
192	8/2/2021, 9:20:03 AM UTC-0400	Device	System started.
270	8/2/2021, 9:21:28 AM UTC-0400	Device	The ETHERNET network interface link is now up.
271	8/2/2021, 9:21:28 AM UTC-0400	Device	System started.

Dashboard - PDUs

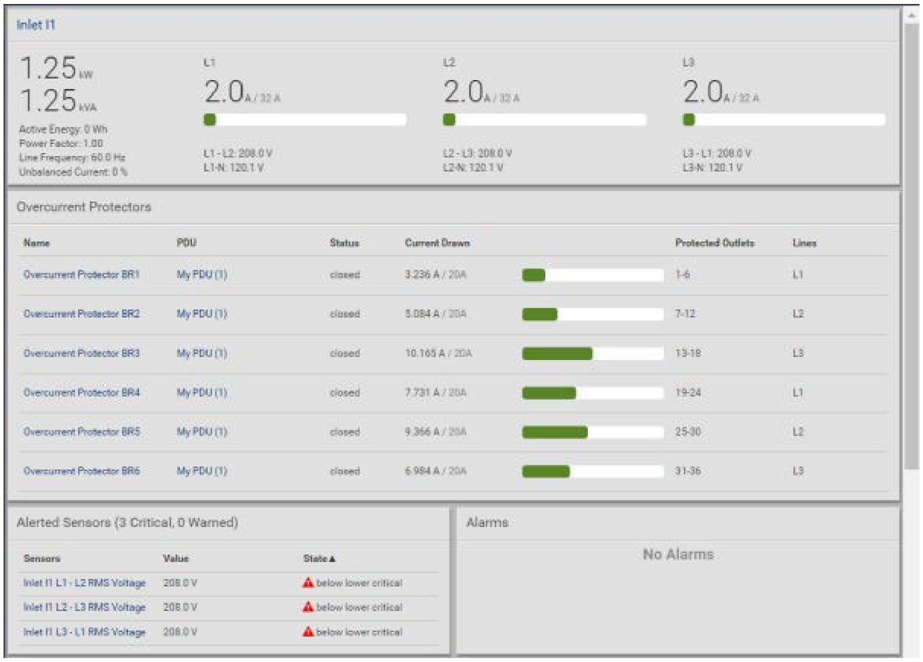
- The Dashboard page gives you an overview of your NX1 PDU in various sections, depending on your model.
- Click any blue hyperlink to go to the main page for that information.
- Not all models have overcurrent protectors.

► *What to look for:*

- All green status bars indicate performance in normal ranges.
- Red or yellow status bars indicate alerts or alarms.
- Check the Alerted Sensors and Alarms sections for any issues that need attention.
- Alarms are listed if there are events that must be acknowledged according to your configurations.
- Alerts are listed when sensor thresholds are entered according to your configurations.

► *What can be customized on the Dashboard?*

- The Inlet History chart at the bottom of the Dashboard shows active power by default.
- Select a different data type to change the chart view temporarily.



Inlet I1

1.25 kW
1.25 kVA
Active Energy: 0 Wh
Power Factor: 1.00
Line Frequency: 60.0 Hz
Unbalanced Current: 0 %

L1
2.0 A / 32 A
L1 - L2: 208.0 V
L1-N: 120.1 V

L2
2.0 A / 32 A
L2 - L3: 208.0 V
L2-N: 120.1 V

L3
2.0 A / 32 A
L3 - L1: 208.0 V
L3-N: 120.1 V

Overcurrent Protectors

Name	PDU	Status	Current Drawn	Protected Outlets	Lines
Overcurrent Protector BR1	My PDU (1)	closed	3.236 A / 20A	1-6	L1
Overcurrent Protector BR2	My PDU (1)	closed	5.084 A / 20A	7-12	L2
Overcurrent Protector BR3	My PDU (1)	closed	10.165 A / 20A	13-18	L3
Overcurrent Protector BR4	My PDU (1)	closed	7.731 A / 20A	19-24	L1
Overcurrent Protector BR5	My PDU (1)	closed	9.366 A / 20A	25-30	L2
Overcurrent Protector BR6	My PDU (1)	closed	6.984 A / 20A	31-36	L3

Alerted Sensors (3 Critical, 0 Warned)

Sensors	Value	State ▲
Inlet I1 L1 - L2 RMS Voltage	208.0 V	⚠ below lower critical
Inlet I1 L2 - L3 RMS Voltage	208.0 V	⚠ below lower critical
Inlet I1 L3 - L1 RMS Voltage	208.0 V	⚠ below lower critical

Alarms

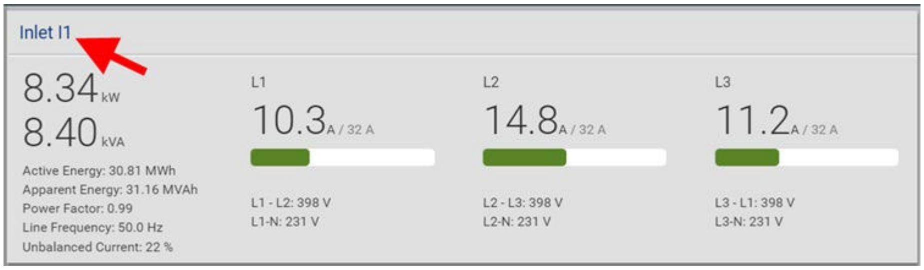
No Alarms

Dashboard - Inlet I1

The number of phases shown in the Inlet section is model dependent.

► *Link to the Inlet page:*

To view more information or configure the inlet(s), click this section's title 'Inlet I1' to go to the Inlet page.



Inlet I1

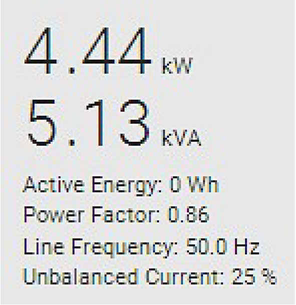
8.34 kW
8.40 kVA
Active Energy: 30.81 MWh
Apparent Energy: 31.16 MVAh
Power Factor: 0.99
Line Frequency: 50.0 Hz
Unbalanced Current: 22 %

L1
10.3 A / 32 A
L1 - L2: 398 V
L1-N: 231 V

L2
14.8 A / 32 A
L2 - L3: 398 V
L2-N: 231 V

L3
11.2 A / 32 A
L3 - L1: 398 V
L3-N: 231 V

► *Left side - generic inlet power data:*

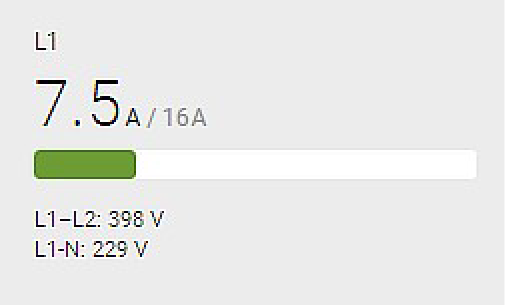


4.44 kW
5.13 kVA
Active Energy: 0 Wh
Power Factor: 0.86
Line Frequency: 50.0 Hz
Unbalanced Current: 25 %

The left side lists all or some of the following data. Available data is model dependent.

- Active power (kW or W)
- Apparent power (kVA or VA)
- Active energy (kWh or Wh)
- Power factor
- Line frequency (Hz)
- Unbalanced current (%) - *model dependent*

► *Right side - inlet's current and voltage:*



L1

7.5 A / 16A

L1–L2: 398 V
L1-N: 229 V

The right side shows the current and voltage data per phase. For a single-phase device, it shows only one line, but for a three-phase device, it shows three lines (L1, L2 and L3).

Inlet data from top to bottom includes:

- RMS current (A) and rated current
  - The smaller, gray text adjacent to RMS current is the rated current.
- A bar showing the RMS current level
- RMS voltage (V)

The RMS current bars automatically change colors to indicate the current status according to your configured thresholds. To configure thresholds, see Inlet.

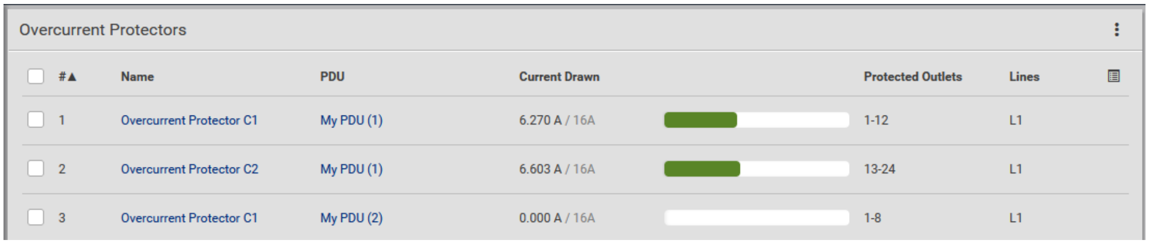
Status	**Bar colors**
normal	🟩
above upper warning	🟨
above upper critical	🟥

Dashboard - OCP

Availability and total number of OCPs depend on the models.

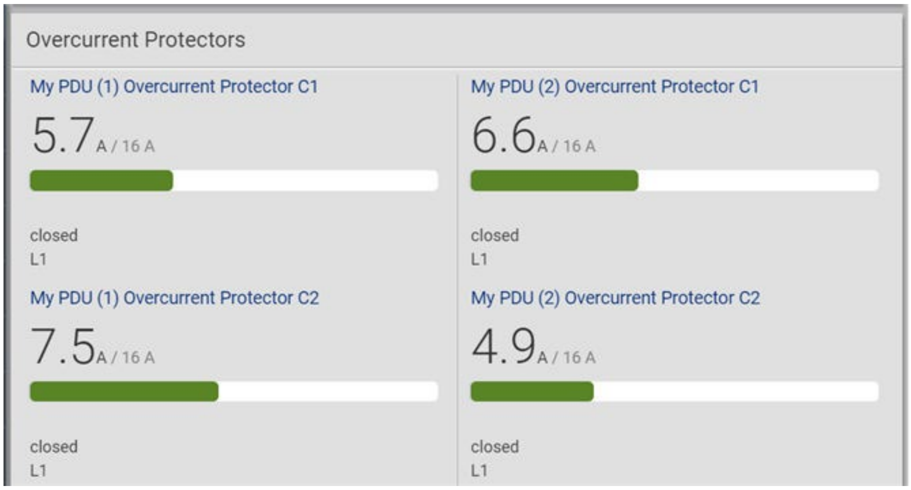
► *Each OCP's link:*

To view more information or configure individual OCPs, click the desired OCP's index number, which is either BR1, BR2, and so on; or C1, C2 and so on, to go to its setup page.



Overcurrent Protectors

□	#▲	Name	PDU	Current Drawn	Protected Outlets	Lines
□	1	Overcurrent Protector C1	My PDU (1)	6.270 A / 16A	1-12	L1
□	2	Overcurrent Protector C2	My PDU (1)	6.603 A / 16A	13-24	L1
□	3	Overcurrent Protector C1	My PDU (2)	0.000 A / 16A	1-8	L1



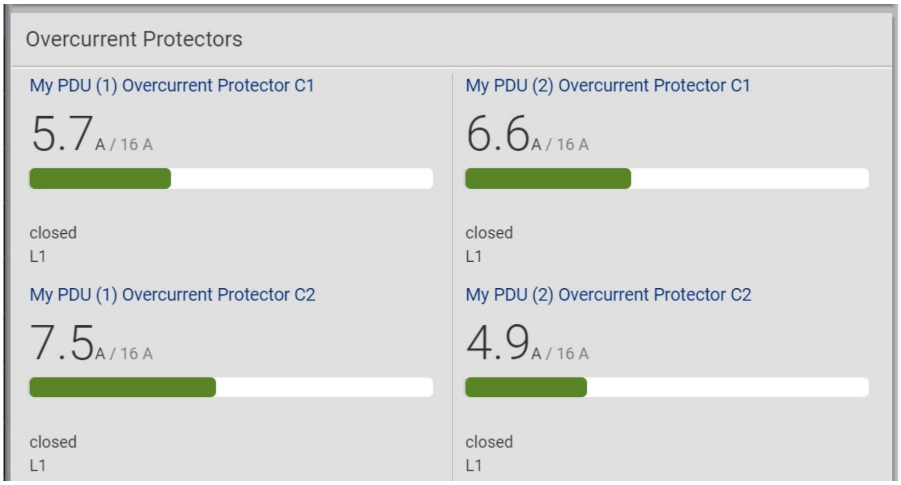
Overcurrent Protectors

My PDU (1) Overcurrent Protector C1
5.7 A / 16 A
closed
L1

My PDU (2) Overcurrent Protector C1
6.6 A / 16 A
closed
L1

My PDU (1) Overcurrent Protector C2
7.5 A / 16 A
closed
L1

My PDU (2) Overcurrent Protector C2
4.9 A / 16 A
closed
L1



Overcurrent Protectors

My PDU (1) Overcurrent Protector C1
5.7 A / 16 A
closed
L1

My PDU (2) Overcurrent Protector C1
6.6 A / 16 A
closed
L1

My PDU (1) Overcurrent Protector C2
7.5 A / 16 A
closed
L1

My PDU (2) Overcurrent Protector C2
4.9 A / 16 A
closed
L1

► *Each OCP's power data:*

OCP data from top to bottom includes:

- RMS current (A), and rated current
  - Smaller gray text adjacent to RMS current is each OCP's rated current, such as "16A" shown in the above diagram.
- A bar showing OCP current levels
- OCP status -- open or closed
- Associated line pair

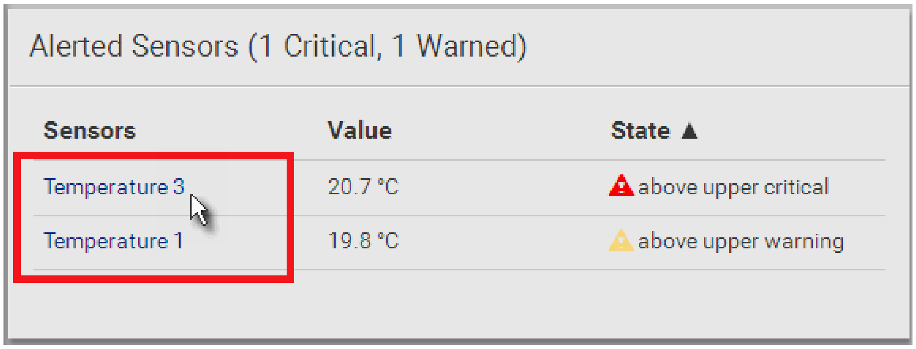
The RMS current bars automatically change colors to indicate the current status according to your configured thresholds. To configure thresholds, see OCPs.

Status	Bar colors
normal	🟩
above upper warning	🟨
above upper critical	🟥

Dashboard - Alerted Sensors

When any internal sensors or environmental sensor packages connected to the NX1 PDU 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 Pages.



Alerted Sensors (1 Critical, 1 Warned)

Sensors	Value	State ▲
Temperature 3	20.7 °C	⚠ above upper critical
Temperature 1	19.8 °C	⚠ above upper warning

▶ *Summary in the section title:*

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

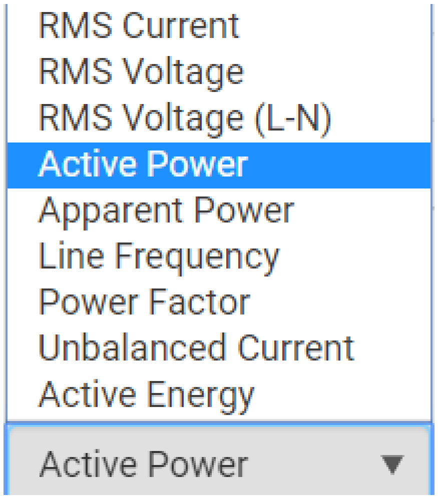
For example:

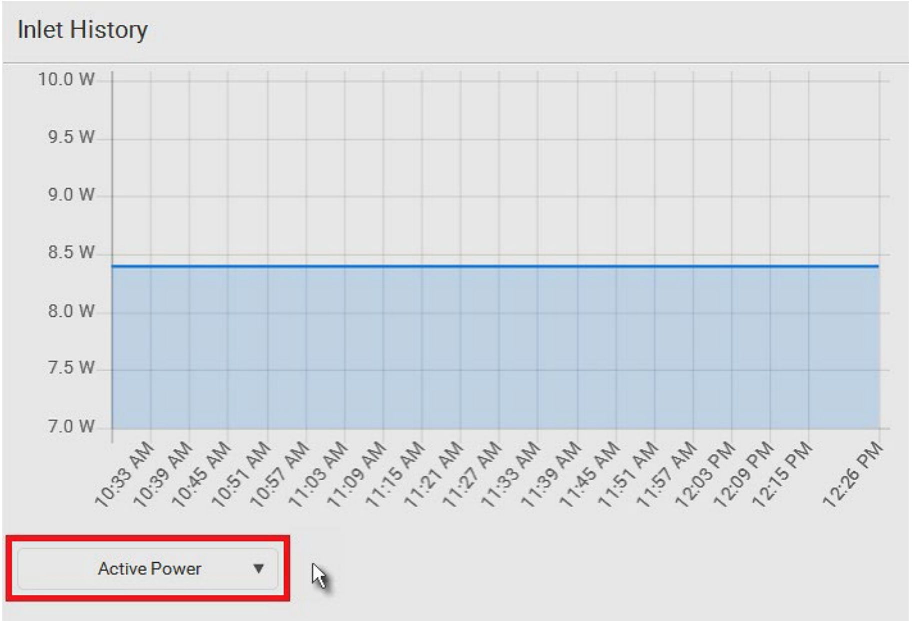
- 1 Critical: 1 sensor enters the critical or alarmed state. 1 Warned: 1 'numeric' sensor enters the warning state.
    - Numeric sensors enter warning or critical states, as their values enter the threshold ranges.
    - State sensors enter an alarmed state.

See Sensor States for more details.

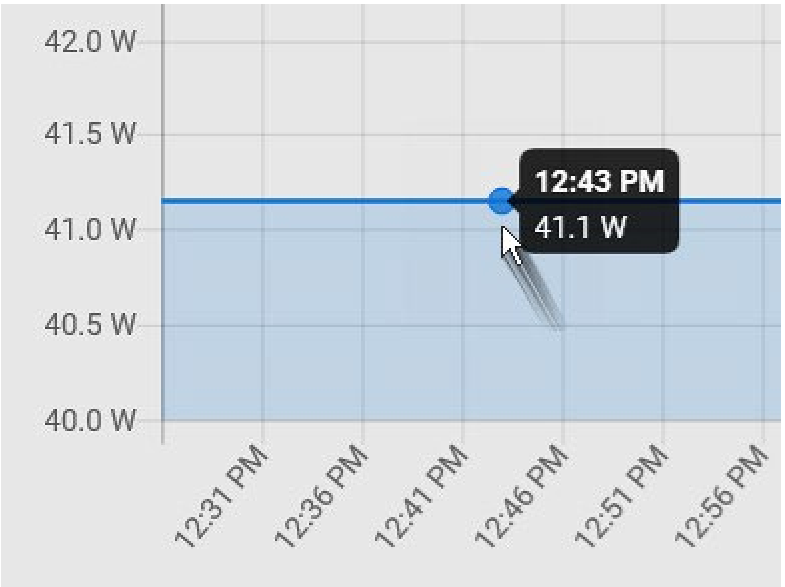
⚠	Numeric sensors: • Warning
⚠	Numeric sensors: • Critical
	State sensors: • Alarmed state

Dashboard - Inlet History

- The Inlet History graph displays the history of the sensor values. Select a different data type by clicking the selector ▼ below the diagram.
- 



- 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.

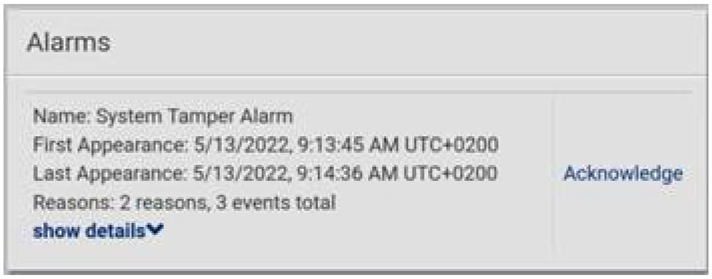


Dashboard - Alarms

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.

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

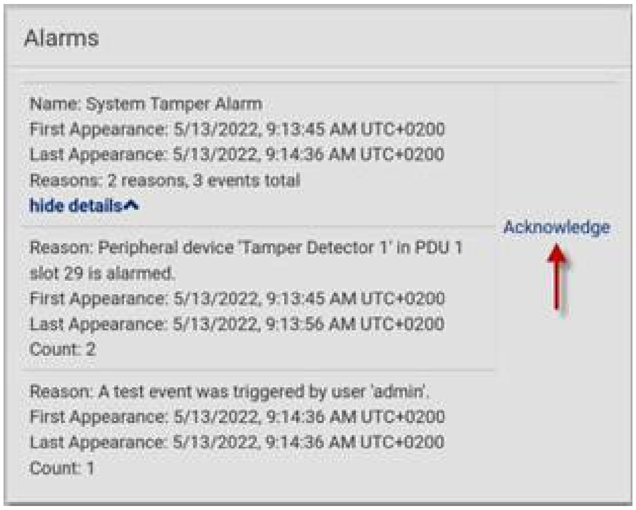


Alarms

Name: System Tamper Alarm
First Appearance: 5/13/2022, 9:13:45 AM UTC+0200
Last Appearance: 5/13/2022, 9:14:36 AM UTC+0200
Reasons: 2 reasons, 3 events total

► *To acknowledge an alarm:*

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



Alarms

Name: System Tamper Alarm
First Appearance: 5/13/2022, 9:13:45 AM UTC+0200
Last Appearance: 5/13/2022, 9:14:36 AM UTC+0200
Reasons: 2 reasons, 3 events total

Reason: Peripheral device 'Tamper Detector 1' in PDU 1 slot 29 is alarmed.
First Appearance: 5/13/2022, 9:13:45 AM UTC+0200
Last Appearance: 5/13/2022, 9:13:56 AM UTC+0200
Count: 2

Reason: A test event was triggered by user 'admin'.
First Appearance: 5/13/2022, 9:14:36 AM UTC+0200
Last Appearance: 5/13/2022, 9:14:36 AM UTC+0200
Count: 1

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.
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	This field appears only when there are multiple types of events triggering the same alert. 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.

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.

PDU

Generic information and PDU settings are available on the PDU page.

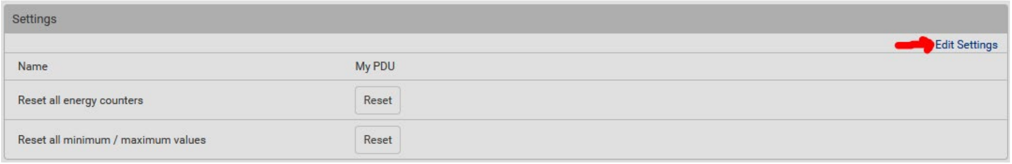
To open the PDU page, click 'PDU' in the Menu.

► *Device information shown:*

- Firmware version
- Serial number
- MAC address
- Rating

► *To configure global settings:*

1) Click Edit Settings.



Name	My PDU
Reset all energy counters	Reset
Reset all minimum / maximum values	Reset

2) Now you can configure the fields.

Field	Function	Note
Name	Customizes the device name.	

3) Click Save.

► *To reset ALL energy counters:*

An energy reading is a value of total accumulated energy, which is never reset, even if the power fails or the NX1 PDU is rebooted. However, you can manually reset this reading to restart the energy accumulation process. Only users with the "Admin" role assigned can reset energy readings.

Note: This reset button does not reset the energy values of outlet groups. Go to the Outlet Groups page to reset that value.

1) On the PDU page, in the Settings section, make sure Edit Settings is not clicked, or cancel out of editing settings.
2) On the Reset all energy counters option, click Reset, then click on the confirmation message.
   - All energy readings are reset to zero.

Tip: You can also reset the energy reading of an individual inlet or outlet on those pages.

► *To reset all minimum/maximum values:*

For readings that record a maximum and minimum numeric value, you can reset these values as needed to clear the previous highs and lows.

1) On the PDU page, in the Settings section, make sure Edit Settings is not clicked, or cancel out of editing settings.
2) On the Reset all minimum/maximum values option, click Reset, then click on the confirmation message.
   - All previously recorded maximum and minimum values are reset.

Inlet

You can view all inlet information, configure inlet-related settings, or reset the inlet active energy and min/max sensor values on the Inlet page. To open this page, click 'Inlet' in the *Menu.*

Inlet thresholds help you identify when your inlet enters warning or critical level. In addition, you can have NX1 PDU automatically generate alert notifications for any warning or critical status. See Event Rules and Actions.

Overview:

- Inlet power overview, which is the same as Dashboard - Inlet I1.

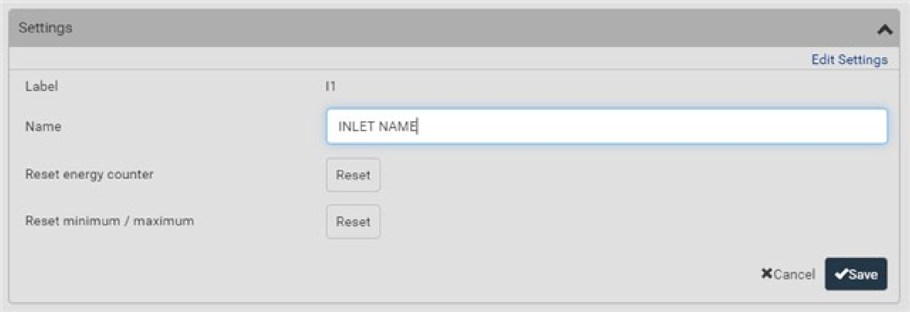
► *Sensors:*

- A list of inlet sensors with more details. Available inlet sensors depends on the model.
  - Sensors show both readings and states.
  - Sensors in warning or critical states are highlighted in yellow or red.
- Inlet's power chart, which is the same as Dashboard - Inlet History.

► *Settings--Name the inlet:*

Scroll down past the Sensor list to the Settings.

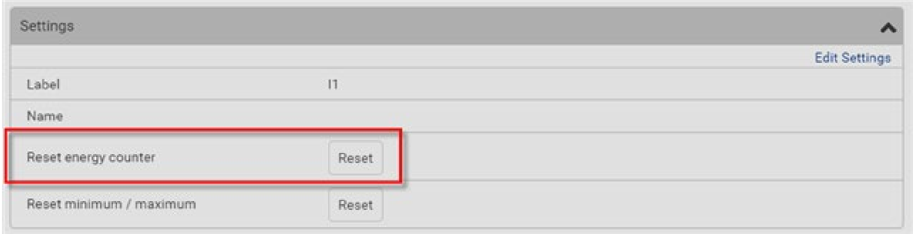
- Click Edit Settings, enter a name for the inlet, then click Save. For example, name the inlet after the power source.
- The inlet's custom name is displayed on the Inlet or Dashboard page, followed by its label in parentheses.



Label	I1
Name	INLET NAME
Reset energy counter	Reset
Reset minimum / maximum	Reset

► *Settings--Reset energy counter:*

The energy counter reset feature per inlet is especially useful when your NX1 PDU has more than one inlet. Only users with the "Admin" role assigned can reset this value.



Label I1

Name

Reset energy counter Reset

Reset minimum / maximum Reset

- Click Reset and then confirm in the message.

  This inlet's active energy reading is then reset to zero.

Tip: To reset ALL active energy counters on the NX1 PDU, go to the PDU page.

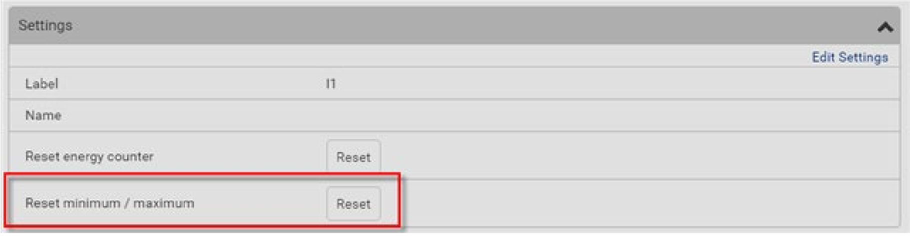
► *Settings: Reset minimum/maximum:*

All inlet sensors with numeric readings store their minimum and maximum recorded reading. You can reset these as desired. Only users with the "Admin" role assigned can reset this value.

Tip: To enable the display of minimum/maximum for any sensor, click the ☰ Options icon at the top right of the Sensors lists.

- Click Reset and then confirm in the message.

  The min/max values and the "unchanged since" timestamps are reset to this moment's sensor readings.



Label I1

Name

Reset energy counter Reset

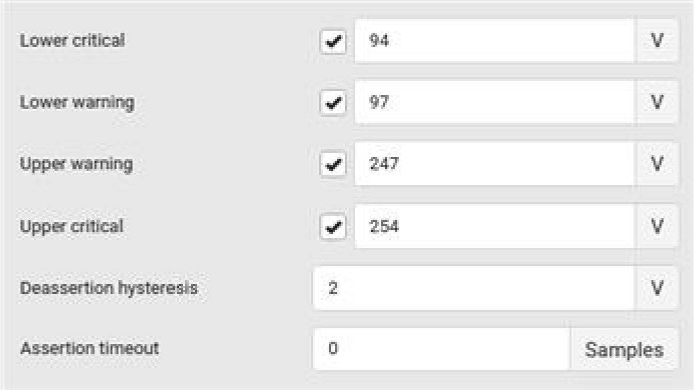
Reset minimum / maximum Reset

► *To configure inlet thresholds:*

By default, there are pre-defined RMS voltage and current threshold values in related fields. You can modify them to meet your needs.

1) Click the Thresholds title bar at the bottom of the page to display inlet thresholds.

2) Click the desired sensor to open the settings.
3) To enable a threshold, select the corresponding checkbox.
4) Type a new value in the accompanying text box.



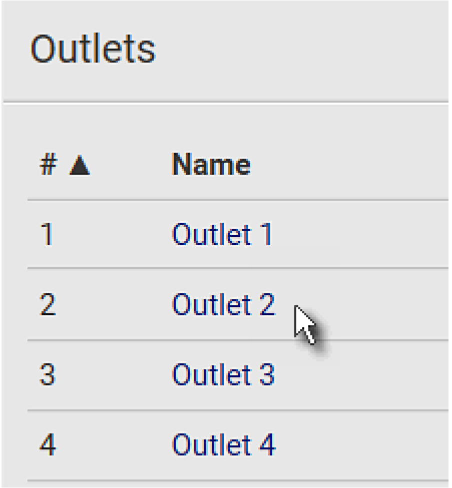
Lower critical	☑	94	V
Lower warning	☑	97	V
Upper warning	☑	247	V
Upper critical	☑	254	V
Deassertion hysteresis		2	V
Assertion timeout		0	Samples

Outlets

The Outlets page shows a list of all outlets and the overview of outlet status and data. To open this page, click 'Outlets' in the *Menu.*

Individual Outlet Pages

An outlet's data/setup page is opened after clicking the outlet's name on the Outlets overview page.



Outlets

# ▲	Name
1	Outlet 1
2	Outlet 2
3	Outlet 3
4	Outlet 4

The individual outlet's page shows this outlet's detailed information.

► *To configure this outlet:*

1) Click Edit Settings.

2) Configure available fields. Note that the fields marked with * are only available on outlet-switching capable models.

Field	Description
Name	Type an outlet name up to 64 characters long.
*State on device startup	Click this field to select this outlet's initial power state. • Options: *on*, *off*, *last known* and *PDU defined*. • Note that any option other than "PDU defined" will override the global outlet state setting on this particular outlet.
*Power off period during power cycle	Select an option to determine how long this outlet is turned off before turning back on. • Options: *PDU defined* or customized time. See Power-Of f Period Options for Individual Outlets. • Note that any time setting other than "PDU defined" will override the global power-off period setting on this particular outlet.

*Non-critical	Select this checkbox only when you want this outlet to turn off in the load shedding mode. See Load Shedding Mode: Activate or Deactivate.

1) Click Save.
2) The outlet's custom name, if available, is displayed in the outlets list, following by its label in parentheses.

Note for 'State on device startup': This setting works only when 'Relay behavior on power loss' is set to *Non-latching*. This is because all relays keep their states unchanged in the latching mode regardless of the power supply status.

Detailed Information on Outlet Pages

Each outlet's data page has the Details section for showing general outlet information and Sensors section for showing the outlet sensor status.

► *Details section:*

Field	**Description**
Label	The physical outlet number
Outlet status	This information is only available on outlet-switching capable models. On or Off
Receptacle type	This outlet's receptacle type
Lines	Lines associated with this outlet
Inlet	Inlet associated with this outlet
Overcurrent protector	This information is available only when your NX1 PDU has overcurrent protectors. Overcurrent protector associated with this outlet

Power-Off Period Options for Individual Outlets

There are two options for setting the power-off period during the power cycle on each individual outlet's page.

Option	Function
PDU defined (configured value)	Follows the global power-off period setting, which is set on the *PDU page.* The value in parentheses is the current global value.
Customized time	• Select an existing time option, or type a new value *with an appropriate time unit added, such as s for seconds.*

Outlet Groups

Only PDUs with outlet-switching feature show this menu item.

Choose Outlet Groups in the *Menu*.

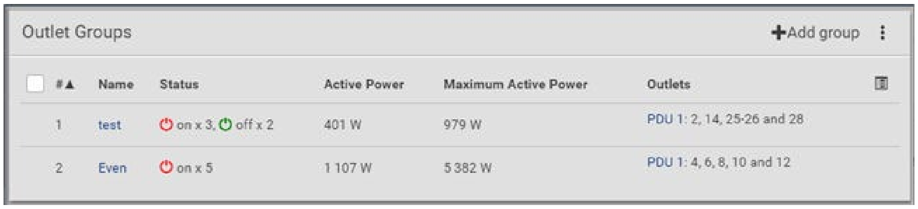
► *Required permissions:*

You must have one of the permissions below to be able to operate all or some of the outlet group features.

- Administrator Privileges -- *all operations*
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration -- *creating, editing and deleting outlet groups*
- Switch Outlet Group -- *powering on, off or cycle outlet groups*

► *Outlet group data:*

The Outlet Groups page will list all outlet groups you create.



□	#▲	Name	Status	Active Power	Maximum Active Power	Outlets
	1	test	on x 3, off x 2	401 W	979 W	PDU 1: 2, 14, 25-26 and 28
	2	Even	on x 5	1 107 W	5 382 W	PDU 1: 4, 6, 8, 10 and 12

- For each group, you can view the following data on the Outlet Groups page:
  - Group number
  - Name: the outlet group name displays as a link. Click to go to the details page for the group.
  - Status: number of outlets with status ON, number of outlets with status OFF.
  - Active Power: The active power for the group. A sum of all member outlets' active power values.
  - Maximum Active Power: Hidden by default. Click the columns icon to add this data. The highest recorded active power for the group.
  - Outlets: A list of the outlet numbers who are members of the group. The PDU(s) of the outlets displays as links.

Creating an Outlet Group

You can create an outlet group if you often have to perform the same action on the same outlets at a regular interval.

For example, create an outlet group when you need to:

- Power cycle specific outlets every week.
- Sum up and track specific outlets' active power values every month.
- Sum up the increased values of specific outlet's active energy values every month.

Note that an outlet can be a member of one or multiple groups.

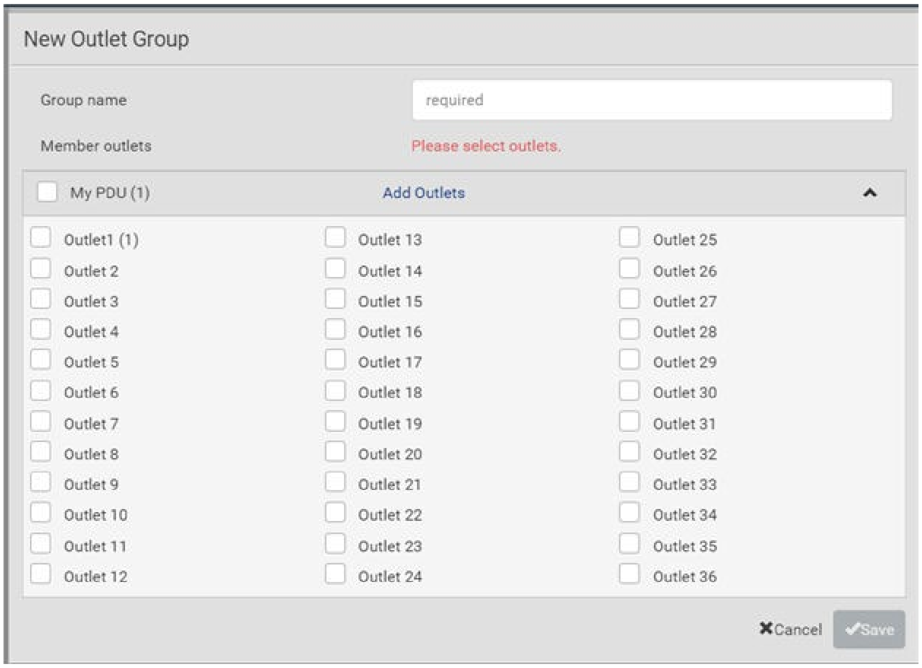
To create an outlet group, you must have either permission below.

- Administrator Privileges
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration

► *To create an outlet group:*

1) In the Outlet Groups page, click Add Group.
2) Enter a Group name.

Tip: Outlet group names do not have to be unique. Different groups with the same group name can be identified through their unique index numbers.



New Outlet Group

Group name: required

Member outlets: Please select outlets.

3) Click Save.

Outlet Group Power Control

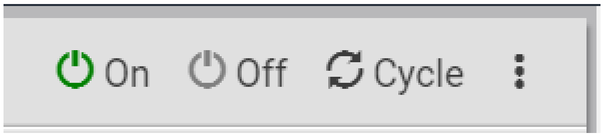
You must have either permission below to power control any outlet groups.

- Administrator Privileges
- Switch Outlet Group

The power control commands are available on the Outlet Groups main page, where you can select one or more groups to control AND on the individual outlet groups page, where you can control that group only while viewing details.

► *To switch one or multiple groups on the Outlet Groups page:*

1) On the Outlet Groups page, select the group or groups you want to control.
2) The power control commands appear in the top right corner.
3) Click a power control command.

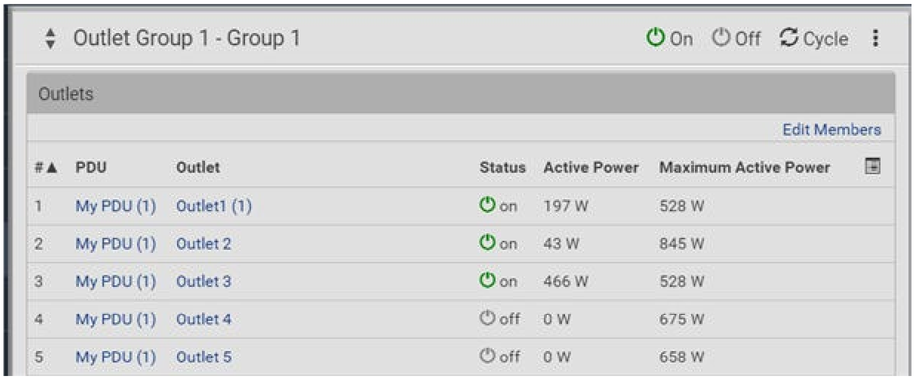


- On: Power ON
- Off: Power OFF
- Cycle: Power cycle turns outlet OFF then back ON

4) Confirm the operation when prompted.

► *To switch one group on a specific outlet group's page:*

1) In the Outlet Groups page, click a group name to go to its details page.
2) Click a power control command on the top-right corner.



# ▲	PDU	Outlet	Status	Active Power	Maximum Active Power
1	My PDU (1)	Outlet1 (1)	on	197 W	528 W
2	My PDU (1)	Outlet 2	on	43 W	845 W
3	My PDU (1)	Outlet 3	on	466 W	528 W
4	My PDU (1)	Outlet 4	off	0 W	675 W
5	My PDU (1)	Outlet 5	off	0 W	658 W

3) Confirm the operation when prompted.

If Switchable Outlet Groups are Limited

For the Switch Outlet Group permission, if you assign a role to any user, which permits the user to switch only "specific" outlet groups instead of all outlet groups, the following switching issue may appear.

► *Issue:*

- When an outlet group that the user originally can switch is deleted, and then re-created with the same group name, the user will not be able to switch the "new" outlet group with the same group name.

► *Solution:*

1) Edit the role assigned to the user. See Editing or Deleting Users.
2) Find the Switch Outlet Group permission, and re-select that newly-created outlet group in its outlet group list.

Note: The above issue does not occur for any role which has "All Outlet Groups" selected for its Switch Outlet Group permission.

Modifying an Outlet Group

To modify an outlet group, you must have either permission below.

- Administrator Privileges
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration

► *To modify the member outlets:*

1) On the Outlet Groups page, click a group name to go to its details page.
2) Click Edit Members.
3) Add or remove outlets of this group by selecting or clearing checkboxes.
4) Click Save.

► *To change the group name:*

1) Scroll down to the Settings section, then click Edit Settings.
2) Type a new name.
3) Click Save.

Deleting an Outlet Group

To delete an outlet group, you must have either permission below.

- Administrator Privileges
- Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration

You can delete one or multiple outlet groups at a time.

To delete a single outlet group only, there are two methods -- either Outlet Groups page or individual group page.

► *To delete one or multiple groups on the Outlet Groups page:*

1) On the Outlet Groups page, select one or more outlet groups.
2) Click ⋮ > Delete, then confirm the operation when prompted.

► *To delete a group on a specific outlet group's page:*

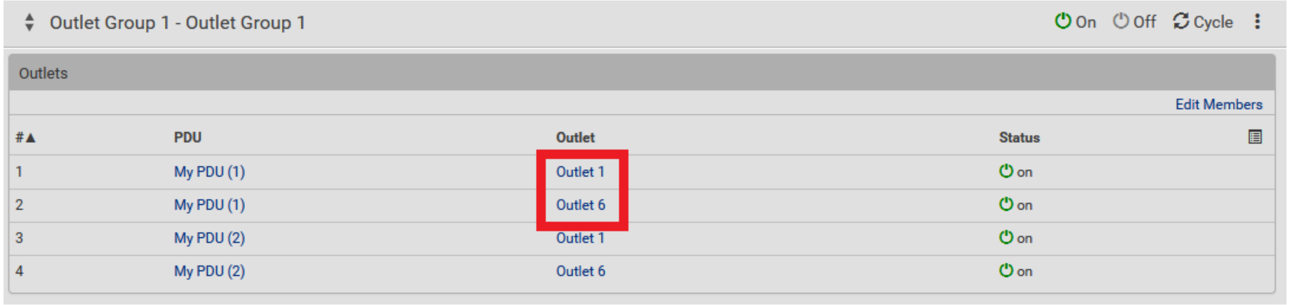
1) Open a specific outlet group's page by clicking on its name.
2) Click ⋮ > Delete, then confirm the operation when prompted.

Viewing More Information

On the individual outlet group page, you can view more information by doing the following.

► *To visit a member outlet's page from the current page:*

- On an outlet group's individual page, you can go to a member outlet's page easily. Just click the outlet links in the Outlets section.



#▲	PDU	Outlet	Status
1	My PDU (1)	Outlet 1	on
2	My PDU (1)	Outlet 6	on
3	My PDU (2)	Outlet 1	on
4	My PDU (2)	Outlet 6	on

► *To visit a different outlet group's page from the current page:*

- On an outlet group's individual page, you can go to another outlet group's page easily. Just click the outlet selector ▲▼ on the top-left corner.

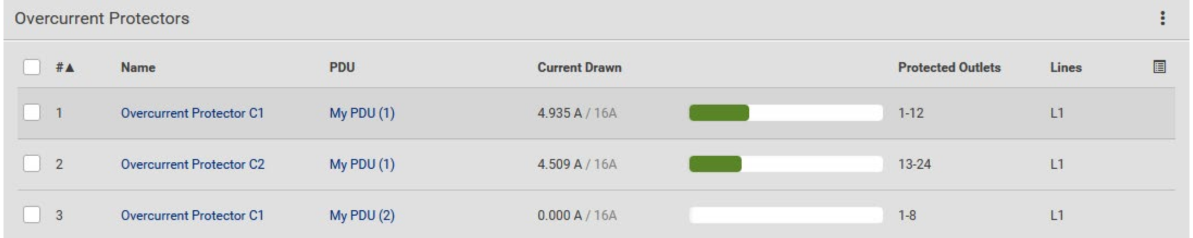
OCPs

The OCPs page is available only when your model has overcurrent protectors, such as circuit breakers.

The OCPs page lists all overcurrent protectors as well as their status. If its current level enters the alarmed state, it is highlighted in red or yellow.

To open the OCPs page, click 'OCPs' in the *Menu.*

You can go to each OCP's data/setup page by clicking its name on this page. OCPs may be numbered C1, C2, and so on, or BR1, BR2 and so on.



Overcurrent Protectors ⋮

☐	#▲	Name	PDU	Current Drawn		Protected Outlets	Lines
☐	1	Overcurrent Protector C1	My PDU (1)	4.935 A / 16A		1-12	L1
☐	2	Overcurrent Protector C2	My PDU (1)	4.509 A / 16A		13-24	L1
☐	3	Overcurrent Protector C1	My PDU (2)	0.000 A / 16A		1-8	L1

► Overcurrent protector overview:

- Current drawn, rated current and current bar
  - The smaller, gray text adjacent to "current drawn" is the rated current of each OCP.
  - The RMS current bars change colors to indicate the status if the OCP thresholds have been configured and enabled.

Status	**Bar colors**
normal	🟩
above upper warning	🟨
above upper critical	🟥

Note: The "below lower warning" and "below lower critical" states also show yellow and red colors respectively. However, it is not meaningful to enable the two thresholds for current levels.

- Protected outlets, which are indicated with outlet numbers
- Associated lines

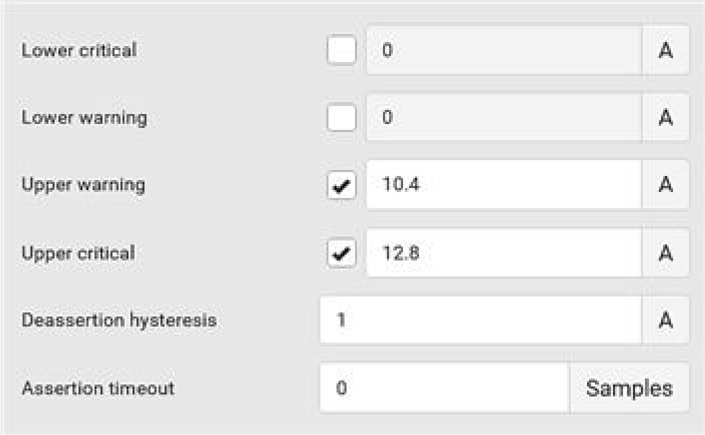
► *To configure current thresholds for multiple overcurrent protectors:*

OCP thresholds, when enabled, help you identify the OCP whose RMS current enters the warning or critical level with the yellow or red color. In addition, you can automatically generate alert notifications for any warning or critical status.

Note: By default, upper thresholds of an OCP's RMS current have been configured. You can modify them as needed.

Click ⋮ > Threshold Bulk Setup.

1) Select one or multiple OCPs.
2) Click Edit Thresholds.
3) Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.



Lower critical	□	0	A
Lower warning	□	0	A
Upper warning	☑	10.4	A
Upper critical	☑	12.8	A
Deassertion hysteresis		1	A
Assertion timeout		0	Samples

4) Click Save.

Individual OCP Pages

An OCP's data/setup page is opened after clicking any OCP's name on the OCPs or Dashboard page.

► *General OCP information:*

Field	**Description**
Label	This OCP's physical number. • C1, C2, C3... • BR1, BR2, BR3...

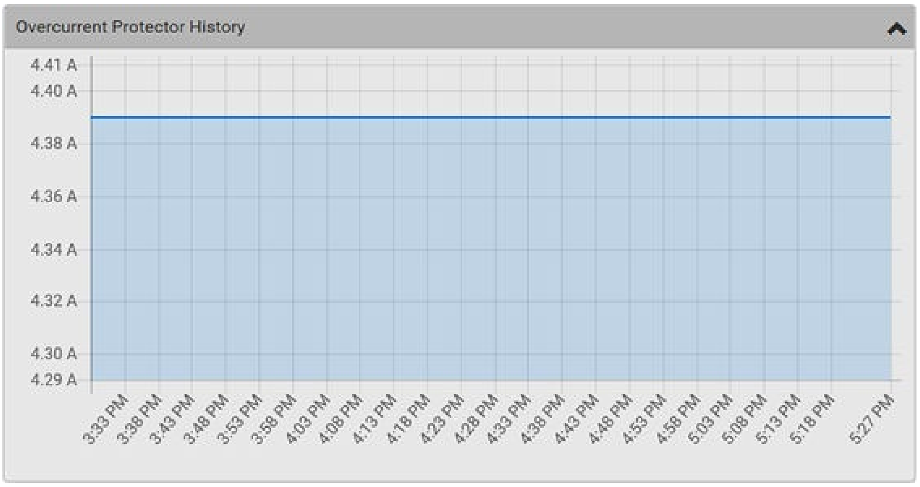
Field	Description
Type	This OCP's type.
Rating	This OCP's rated current.
Lines	Lines associated with this OCP.
Protected outlets	Outlets associated with this OCP.
Inlet	Inlet associated with this OCP.
RMS current	This OCP's current state and readings, including current drawn and current remaining.

► *To customize this OCP's name:*

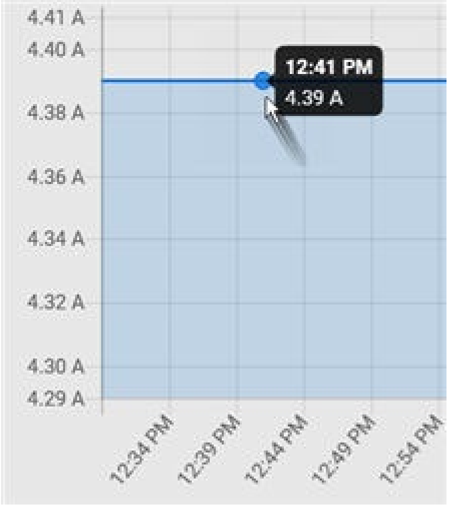
1) Click Edit Settings.
2) Type a name.
3) Click Save.

► *To view this OCP's RMS current chart:*

This OCP's data chart is shown in the Overcurrent Protector History section.



- 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.

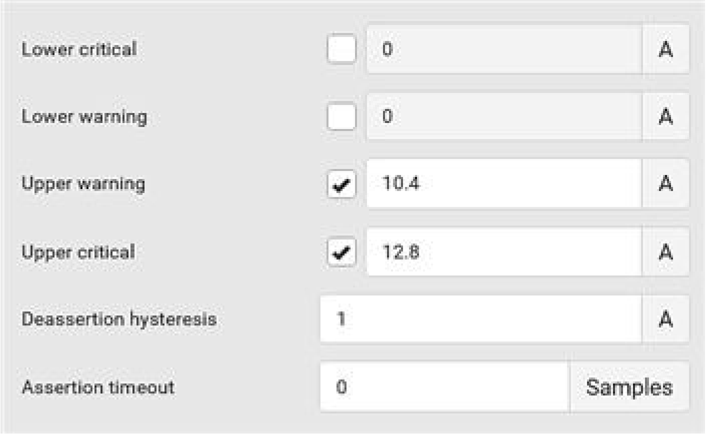


► *To configure this OCP's threshold settings:*

By default, upper thresholds of an OCP's RMS current have been configured. You can modify them as needed.

1) Click the Thresholds title bar at the bottom of the page to display the threshold data.

2) Click the RMS current sensor, then make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.

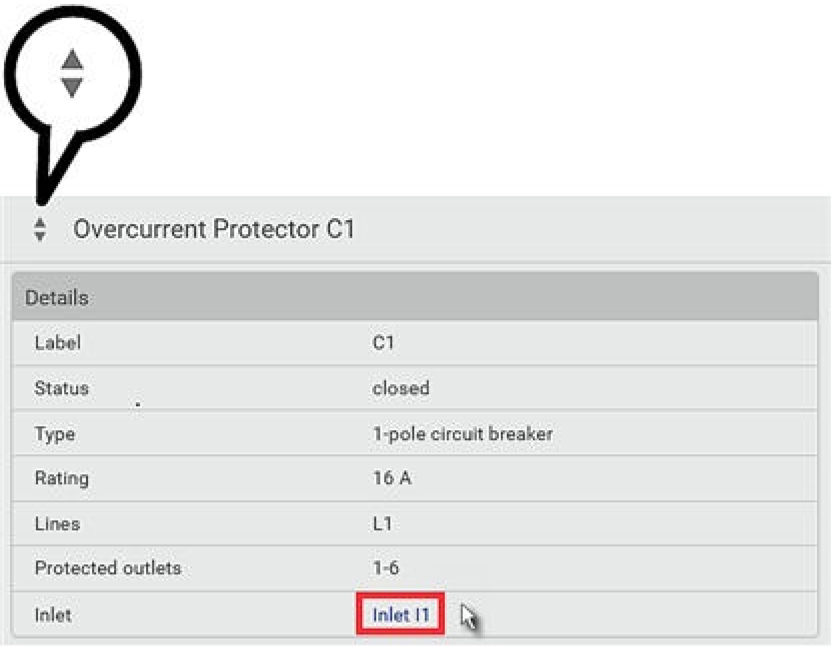


Lower critical	☐	0	A
Lower warning	☐	0	A
Upper warning	☑	10.4	A
Upper critical	☑	12.8	A
Deassertion hysteresis		1	A
Assertion timeout		0	Samples

3) Click Save.

► *Other operations:*

- Go to another OCP's data/setup page by clicking the OCP selector ▲▼ on the top-left corner.
- Go to the associated Inlet's data page by clicking the Inlet link in the Details section.



Overcurrent Protector C1

Details	
Label	C1
Status	closed
Type	1-pole circuit breaker
Rating	16 A
Lines	L1
Protected outlets	1-6
Inlet	Inlet I1

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.

NX1 PDU communicates with *managed* sensors only and retrieves their data. One NX1 PDU can manage a maximum of 8 sensors (2 channels each).

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

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

► *Sensor overview on this page:*

If any sensor enters an alarmed state, it is highlighted in yellow or red.

Column	Description
Name	By default, the name assigned contains: • Sensor type, such as "Temperature" or "Dry Contact." • Sequential number of the same sensor type, like 1, 2, 3 and so on. You can customize the name. Customize names on the individual sensor page.
Reading	Numeric sensors, such as temperature and humidity, show the reading.
State	Available for all sensors.
Type	Sensor type.
Serial Number	This is the serial number printed on the sensor package's label.
Position	Position indicates where this sensor is located in the sensor chain. Identifying the Sensor Position and Channel

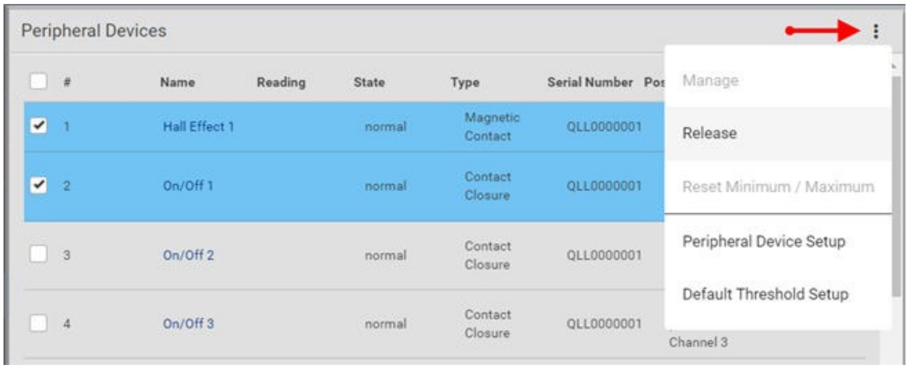
► *To release or manage sensors:*

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. When you manage multiple sensors at once, ID numbers are automatically assigned, and nothing else is changed or released.

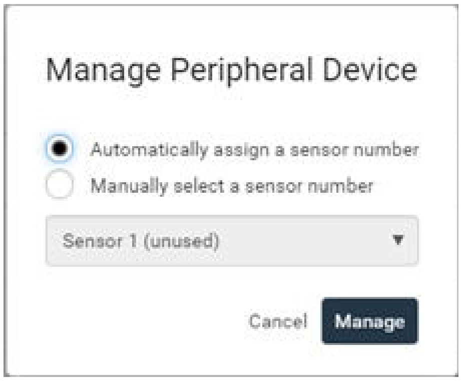
1) Select the sensors that you want to manage/release from management.

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.


Peripheral Devices

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



Manage Peripheral Device

● Automatically assign a sensor number

○ Manually select a sensor number

Sensor 1 (unused) ▾

► *To configure sensor-related settings:*

1) Click ⋮ > Peripheral Device Setup.

Field	Function	Note
Peripheral device Z coordinate format	Options to describe the vertical locations (Z coordinates) of environmental sensor packages. • *Rack units or Free-form* See Z Coordinate Format	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.
Peripheral device auto management	Enables or disables the automatic management feature for Raritan environmental sensor packages. • *Default is Enabled.*	Automatic Management of Sensors
Altitude	Specify the altitude of NX1 PDU above sea level when a differential air pressure sensor is attached. • *Range: -425 to 3000 meters (-1394 to 9842 feet)* • *Negative numbers indicate locations below sea level.*	• The device's altitude is associated with the altitude correction factor. • The default altitude measurement unit is meter. • Your user preference for measurements will take effect here.

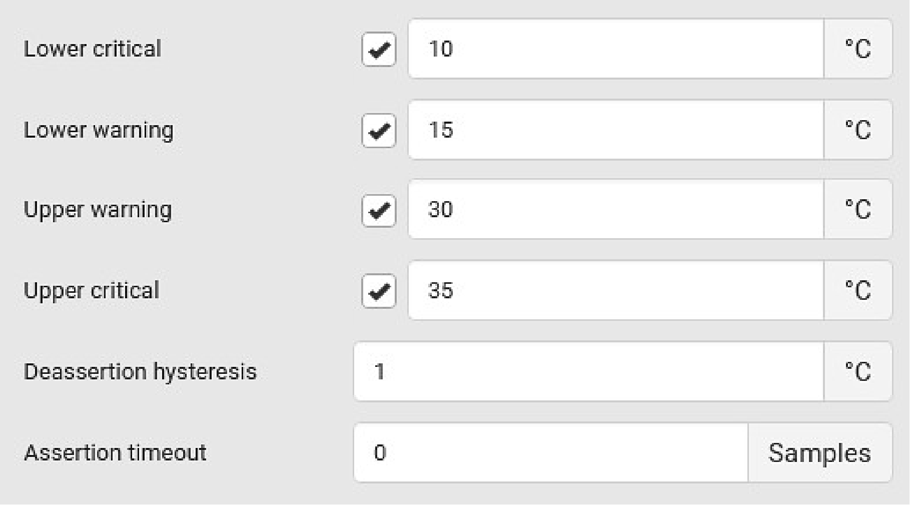
2) Click Save.

► *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 Pages.

3) Click ⋮ > Default Threshold Setup.
4) Click a sensor to open the threshold settings.
5) Make changes as needed.

- To enable any threshold, select the corresponding checkbox.
- Type a new value in the accompanying text box.



Lower critical	☑	10	°C
Lower warning	☑	15	°C
Upper warning	☑	30	°C
Upper critical	☑	35	°C
Deassertion hysteresis		1	°C
Assertion timeout		0	Samples

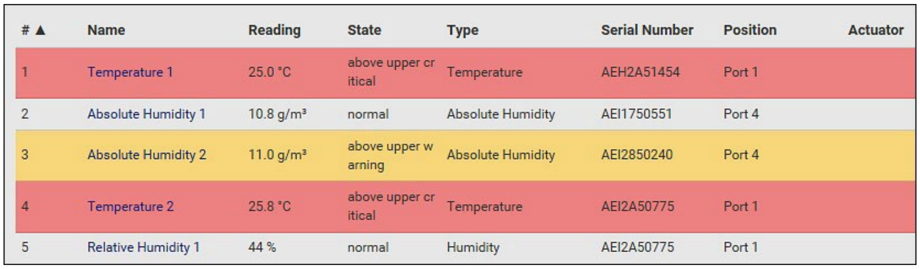
6) Deassertion hysteresis: An alarm is cleared when the sensor reading normalizes the specified amount away from the threshold. In the screenshot example above, if temperature normalizes by more than 1 degree of the threshold, the alarm is cleared. When the reading is within 1°C from the threshold, the 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.

7) 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.

8) Click Save.

Yellow- or Red-Highlighted Sensors

The NX1 PDU 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.



# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	Temperature 1	25.0 °C	above upper critical	Temperature	AEH2A51454	Port 1	
2	Absolute Humidity 1	10.8 g/m^3	normal	Absolute Humidity	AEI1750551	Port 4	
3	Absolute Humidity 2	11.0 g/m^3	above upper warning	Absolute Humidity	AEI2850240	Port 4	
4	Temperature 2	25.8 °C	above upper critical	Temperature	AEI2A50775	Port 1	
5	Relative Humidity 1	44 %	normal	Humidity	AEI2A50775	Port 1	

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

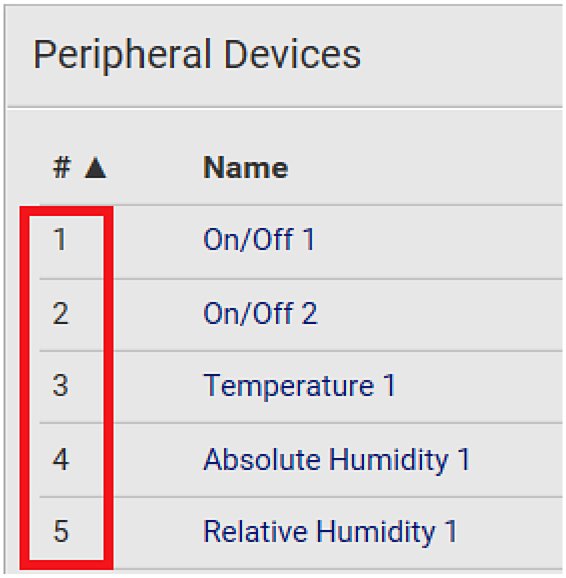
Sensor status	Color	States shown in the interface	Description
Unknown	⬜	unavailable	Sensor state or readings cannot be detected.
		unmanaged	Sensors are not being managed.

Normal	⬜	normal	- Numeric or state sensors are within the normal range. -- OR -- - No thresholds have been enabled for numeric sensors.
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.

Managed vs Unmanaged Sensors

► *Managed sensors:*

- NX1 PDU communicates with managed sensors and retrieves their data.
- Managed sensors are always listed on the Peripheral Devices page whether they are physically connected or not.
- They have an ID number as illustrated below.



Peripheral Devices

# ▲	Name
1	On/Off 1
2	On/Off 2
3	Temperature 1
4	Absolute Humidity 1
5	Relative Humidity 1

- 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:*

- NX1 PDU does NOT communicate with unmanaged sensors.
- Unmanaged sensors are listed only when they are physically connected to NX1 PDU. 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 States

An environmental sensor 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.

► *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	• For numeric sensors, it means the readings are within the normal range. • For state sensors, it means they enter the normal state.
below lower critical	"R" < Lower Critical threshold
below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
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	• Communication with the managed sensor is lost.

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

► *Unmanaged sensor states:*

State	***Description***

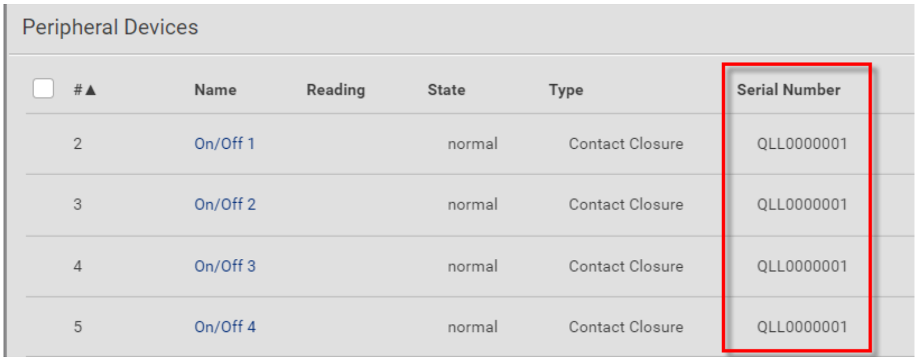
unmanaged	***Sensors are physically connected to the NX1 PDU but not managed yet.***

Note: Unmanaged sensors 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 appears listed in the web interface when it is detected. Match the serial number from the tag to those listed in the sensor table.



Peripheral Devices

□	# ▲	Name	Reading	State	Type	Serial Number
	2	On/Off 1		normal	Contact Closure	QLL0000001
	3	On/Off 2		normal	Contact Closure	QLL0000001
	4	On/Off 3		normal	Contact Closure	QLL0000001
	5	On/Off 4		normal	Contact Closure	QLL0000001

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 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.

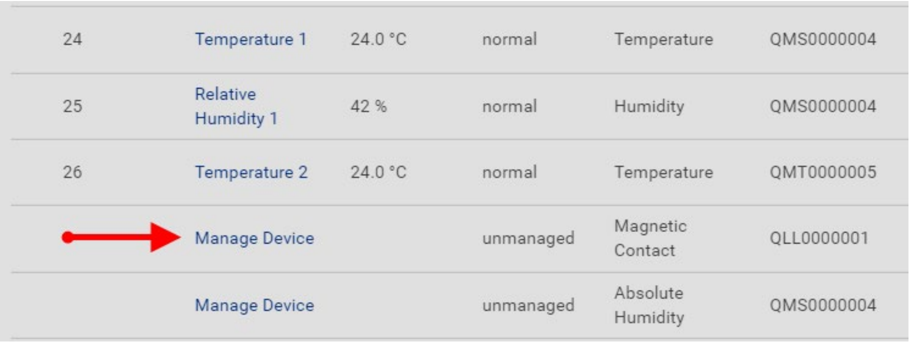
Managing One Sensor

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

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

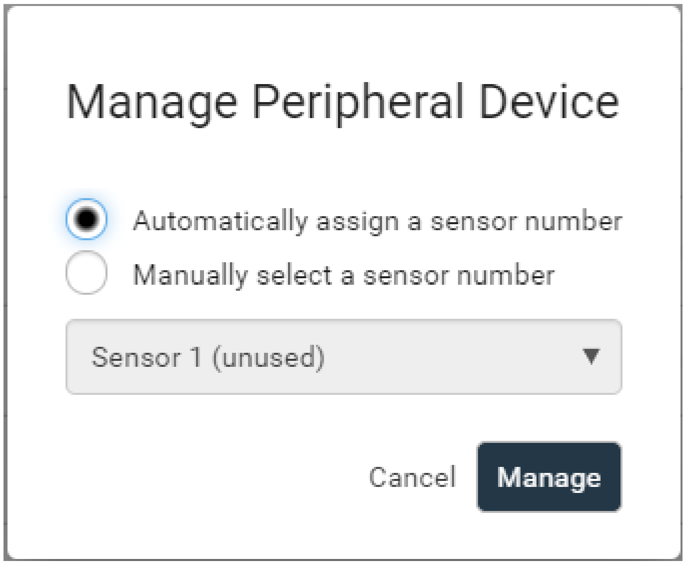
▶ *To manage only one sensor:*

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



24	Temperature 1	24.0 °C	normal	Temperature	QMS0000004
25	Relative Humidity 1	42 %	normal	Humidity	QMS0000004
26	Temperature 2	24.0 °C	normal	Temperature	QMT0000005
	Manage Device		unmanaged	Magnetic Contact	QLL0000001
	Manage Device		unmanaged	Absolute Humidity	QMS0000004

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

- Select "Automatically assign a sensor number" to assign an unused ID number. This method does not release any managed sensor.
- 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.

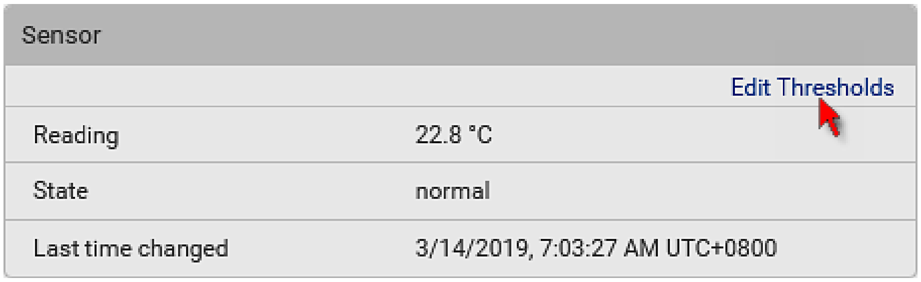
Individual Sensor Pages

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

Note that only a numeric sensor has threshold settings, while a state sensor 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 NX1 PDU automatically generate alert notifications for any warning or critical status.

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

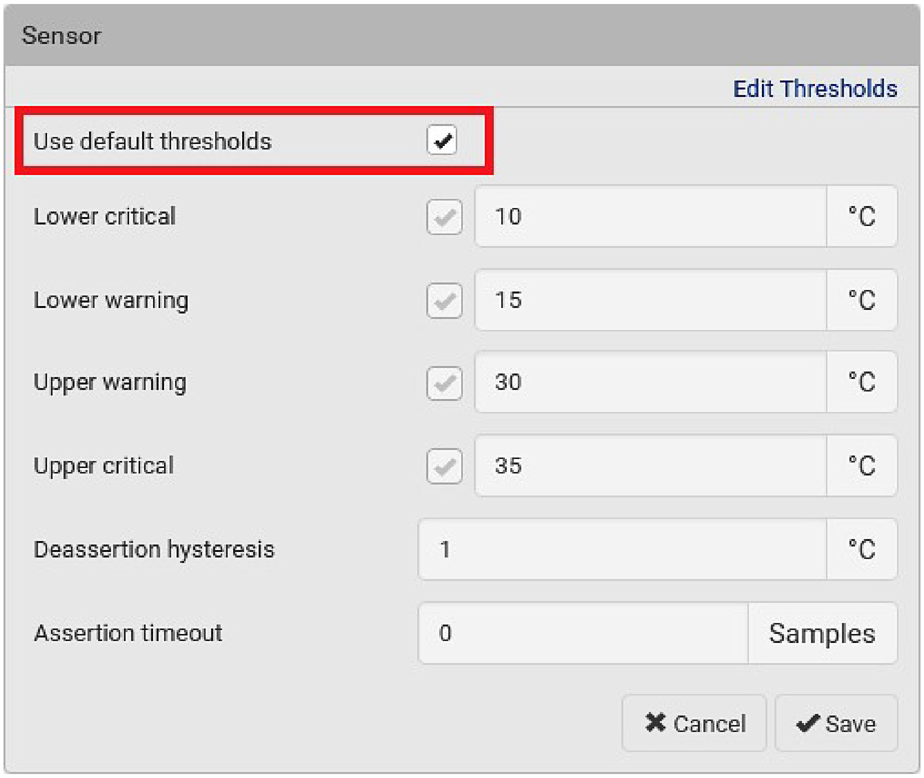
1) Click Edit Thresholds.



Reading	22.8 °C
State	normal
Last time changed	3/14/2019, 7:03:27 AM UTC+0800

Tip: The date and time shown on the NX1 PDU 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 ☑

Lower critical	☑	10	°C
Lower warning	☑	15	°C
Upper warning	☑	30	°C
Upper critical	☑	35	°C
Deassertion hysteresis		1	°C
Assertion timeout		0	Samples

- 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.

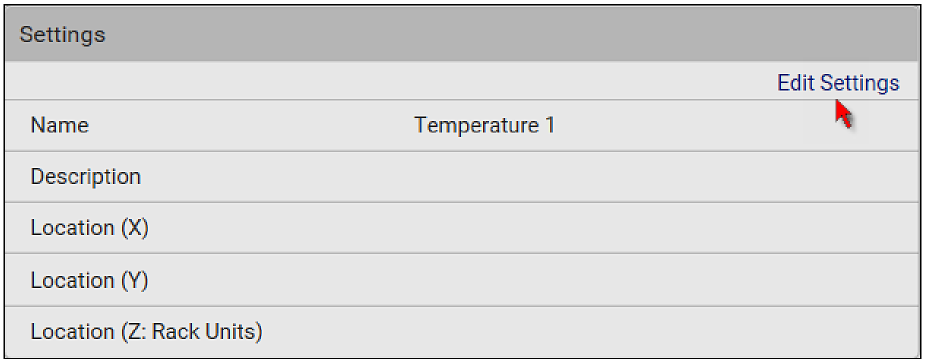
Note: For concepts of thresholds, deassertion hysteresis and assertion timeout, see Sensor Threshold Settings.

---

3) Click Save.

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

1) Click Edit Settings.



Settings

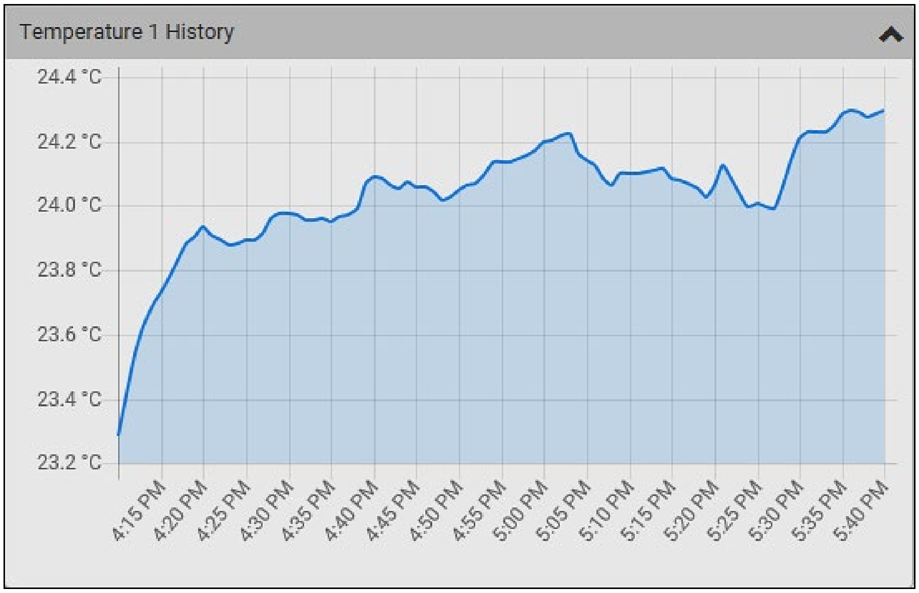
Name	Temperature 1
Description	
Location (X)	
Location (Y)	
Location (Z: Rack Units)	

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

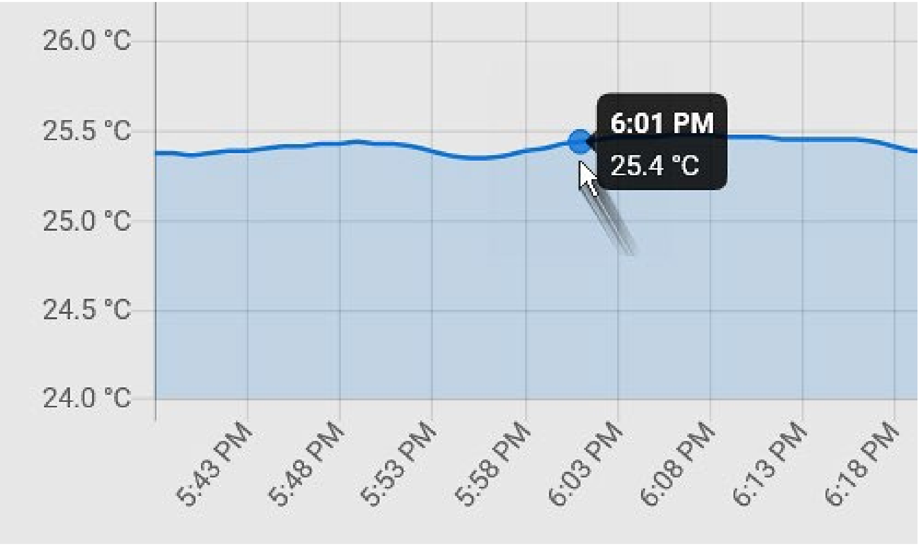
Fields	Description
Name	A name for the sensor.
Description	Any descriptive text you want.
Location (X, Y and Z)	Describe the sensor's location in the data center by typing alphanumeric values for the X, Y and Z coordinates. See Sensor Location Example: X, Y, Z Coordinates. If the term "Rack Units" appears in parentheses in the Z location, you must type an integer number. The Z coordinate's format is determined on the page of *Peripherals.*
Binary Sensor Subtype	This field is available for any Raritan contact closure sensor except for DX2-DH2C2's contact closure sensors. Determine the sensor type of your contact closure detector. • *Contact Closure* detects the door lock or door open/closed status. • *Smoke Detection* detects the appearance of smoke. • *Water Detection* detects the appearance of water on the floor. • *Vibration* detects the vibration of the floor.

▶ *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 do not have such data.

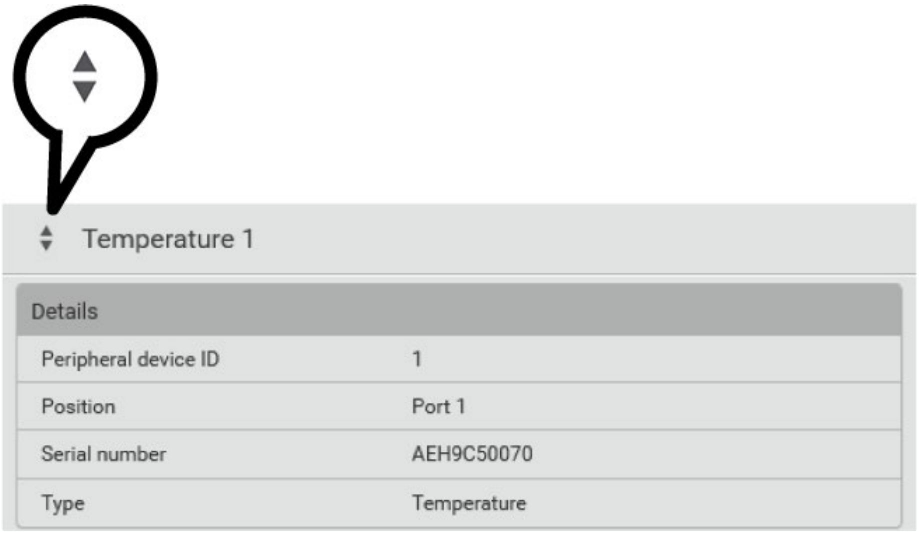


- To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data are displayed as illustrated below.



▶ *Other operations:*

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



Temperature 1

Details	
Peripheral device ID	1
Position	Port 1
Serial number	AEH9C50070
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 Location Example: X, Y, Z Coordinates

Use the X, Y and Z coordinates to describe each sensor'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.

Sensor battery level

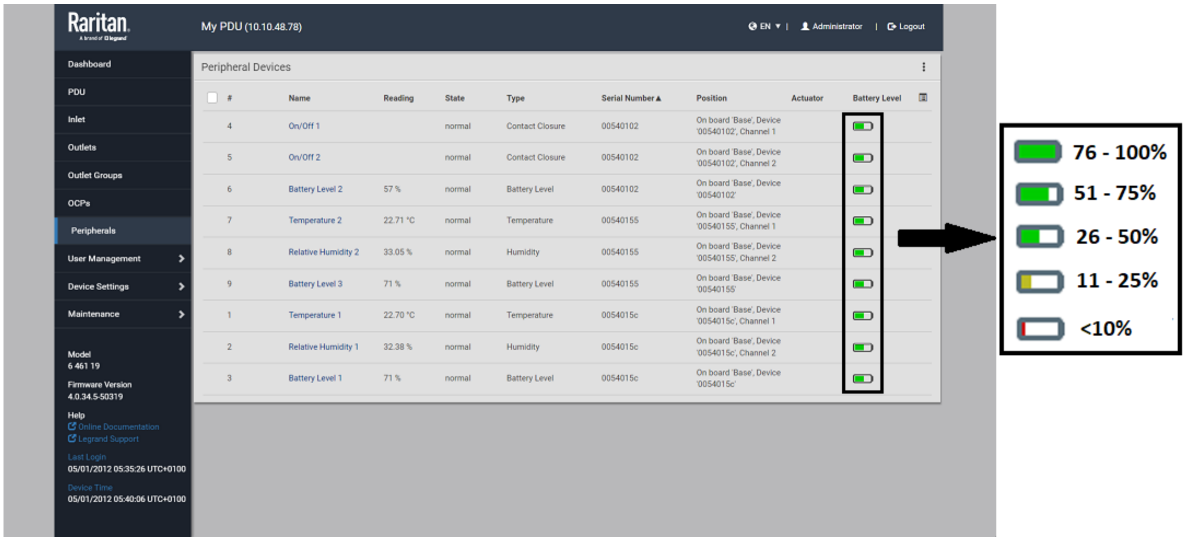
Wireless sensors are powered by Zigbee Green Power Technology.Thanks to this energy-friendly radio communication mode, the life of the battery is preserved and a standard battery won't need to be replaced for at least 5 years.

Battery level display

It is possible to view the battery level of each sensor via the web user interface in the tab "peripherals".

Sensors are sorted by serial number by default, so that lines relating to the same sensors and displaying their measurements, status and battery level are grouped together.

To see the battery level at a glance, an icon is displayed by default in the last column. It indicates the range of the battery level.



Peripheral Devices

□	#	Name	Reading	State	Type	Serial Number ▲	Position	Actuator	Battery Level
	4	On/Off 1		normal	Contact Closure	00540102	On board 'Base', Device '00540102', Channel 1		🟩
	5	On/Off 2		normal	Contact Closure	00540102	On board 'Base', Device '00540102', Channel 2		🟩
	6	Battery Level 2	57 %	normal	Battery Level	00540102	On board 'Base', Device '00540102'		🟩
	7	Temperature 2	22.71 °C	normal	Temperature	00540155	On board 'Base', Device '00540155', Channel 1		🟩
	8	Relative Humidity 2	33.05 %	normal	Humidity	00540155	On board 'Base', Device '00540155', Channel 2		🟩
	9	Battery Level 3	71 %	normal	Battery Level	00540155	On board 'Base', Device '00540155'		🟩
	1	Temperature 1	22.70 °C	normal	Temperature	0054015c	On board 'Base', Device '0054015c', Channel 1		🟩
	2	Relative Humidity 1	32.38 %	normal	Humidity	0054015c	On board 'Base', Device '0054015c', Channel 2		🟩
	3	Battery Level 1	71 %	normal	Battery Level	0054015c	On board 'Base', Device '0054015c'		🟩

Model
6 461 19

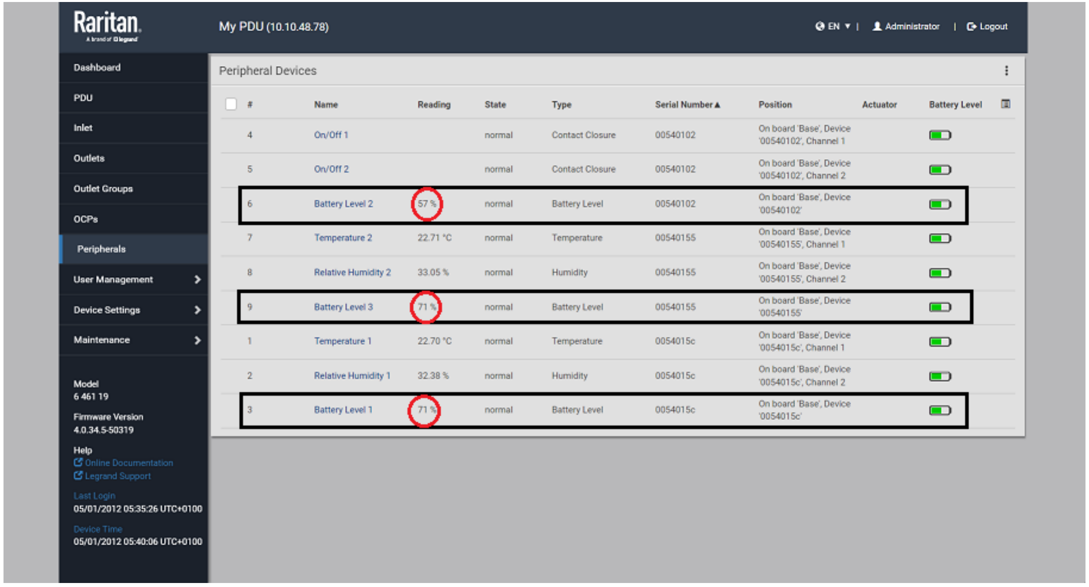
Firmware Version
4.0.34.5-50319

Help

Last Login
05/01/2012 05:35:26 UTC+0100

Device Time
05/01/2012 05:40:06 UTC+0100

In addition, each sensor has its own line displaying the battery level measurement.



Model
6 461 19

Firmware Version
4.0.34.5-50319

Last Login
05/01/2012 05:35:26 UTC+0100

Device Time
05/01/2012 05:40:06 UTC+0100

Peripheral Devices

#	Name	Reading	State	Type	Serial Number ▲	Position	Actuator	Battery Level
4	On/Off 1		normal	Contact Closure	00540102	On board 'Base', Device '00540102', Channel 1		🔋
5	On/Off 2		normal	Contact Closure	00540102	On board 'Base', Device '00540102', Channel 2		🔋
6	Battery Level 2	57 %	normal	Battery Level	00540102	On board 'Base', Device '00540102'		🔋
7	Temperature 2	22.71 °C	normal	Temperature	00540155	On board 'Base', Device '00540155', Channel 1		🔋
8	Relative Humidity 2	33.05 %	normal	Humidity	00540155	On board 'Base', Device '00540155', Channel 2		🔋
9	Battery Level 3	71 %	normal	Battery Level	00540155	On board 'Base', Device '00540155'		🔋
1	Temperature 1	22.70 °C	normal	Temperature	0054015c	On board 'Base', Device '0054015c', Channel 1		🔋
2	Relative Humidity 1	32.38 %	normal	Humidity	0054015c	On board 'Base', Device '0054015c', Channel 2		🔋
3	Battery Level 1	71 %	normal	Battery Level	0054015c	On board 'Base', Device '0054015c'		🔋

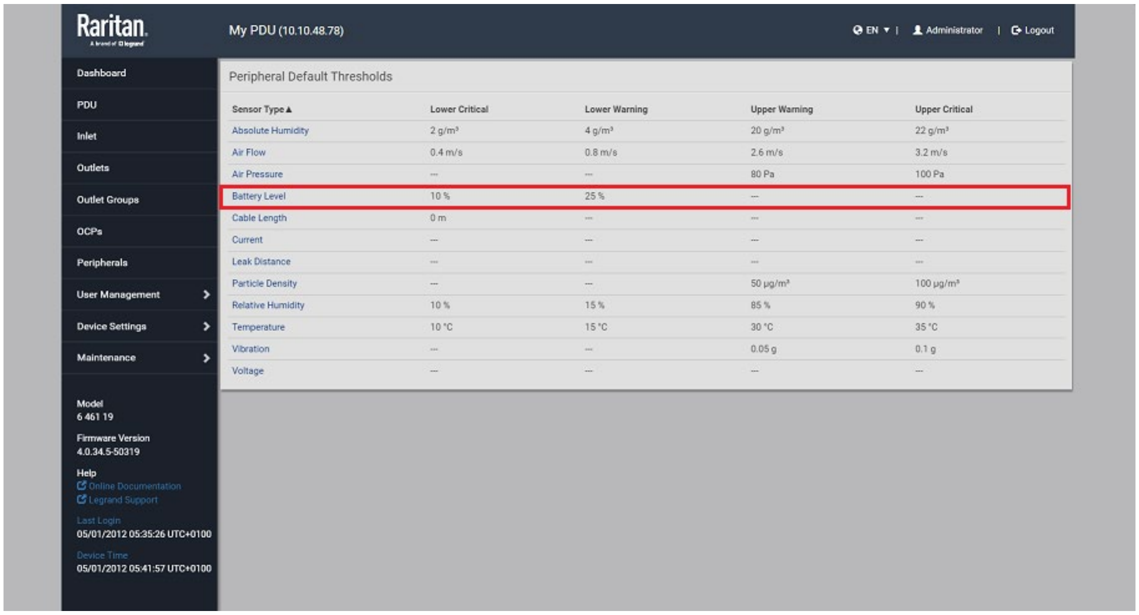
Setting alerts on battery level

Battery level alerts are set to warn you when the battery needs replacing.

The thresholds for alerts are set by default as follow:

- lower critical = 10%
- lower warning = 25%
- upper warning/critical = none

Default thresholds can be modified via the "Peripheral Default Thresholds" menu



Model
6 461 19

Firmware Version
4.0.34.5-50319

Last Login
05/01/2012 05:35:26 UTC+0100

Device Time
05/01/2012 05:41:57 UTC+0100

Peripheral Default Thresholds

Sensor Type ▲	Lower Critical	Lower Warning	Upper Warning	Upper Critical
Absolute Humidity	2 g/m³	4 g/m³	20 g/m³	22 g/m³
Air Flow	0.4 m/s	0.8 m/s	2.6 m/s	3.2 m/s
Air Pressure	---	---	80 Pa	100 Pa
Battery Level	10 %	25 %	---	---
Cable Length	0 m	---	---	---
Current	---	---	---	---
Leak Distance	---	---	---	---
Particle Density	---	---	50 µg/m³	100 µg/m³
Relative Humidity	10 %	15 %	85 %	90 %
Temperature	10 °C	15 °C	30 °C	35 °C
Vibration	---	---	0.05 g	0.1 g
Voltage	---	---	---	---

User Management

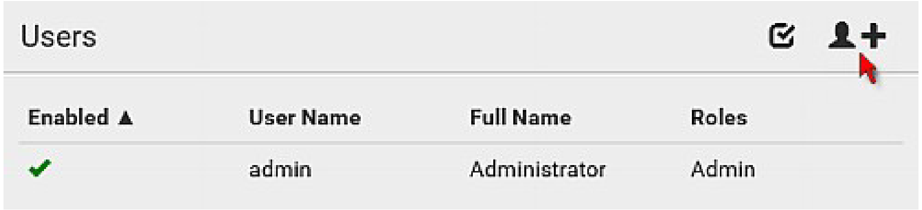
User Management deals with user accounts, permissions, and preferred measurement units on a per-user basis.

NX1 PDU is shipped with one built-in administrator account. You cannot delete this administrator account or change its roles, but you can disable it or rename it. If you disable the administrator account, you must designate another user as administrator by assigning the "Admin" role. 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.

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 .



Users

Enabled ▲	User Name	Full Name	Roles
✓	admin	Administrator	Admin

► *User information:*

Field/setting	Description
User name	The name the user enters to log in. • 1 to 32 characters • Case sensitive • Colon character :, forward slash /, and spaces are NOT permitted.
Full name	The user's first and last names.
Password, Confirm password	• 4 to 64 characters • Case sensitive • Spaces are permitted.
Telephone number	The user's telephone number
Email address	The user's email address • Up to 128 characters • Case sensitive
Enable	When selected, the user can log in.
Force password change on next login	When selected, a password change request automatically appears the next time the user logs in.

► *Roles:*

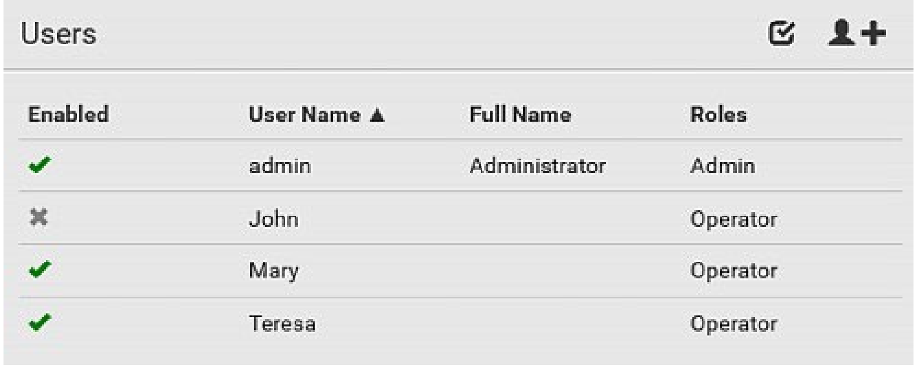
Select one or multiple roles to determine the user's permissions. A user can have a maximum of 32 roles. Note: With multiple roles selected, a user has the union of all roles' permissions.

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
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration (if your model is a PDU) • Switch Outlet (if your model supports it) • Switch Outlet Group (if your model supports it) • View Event Settings • View Local Event Log

Editing or Deleting Users

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



Users

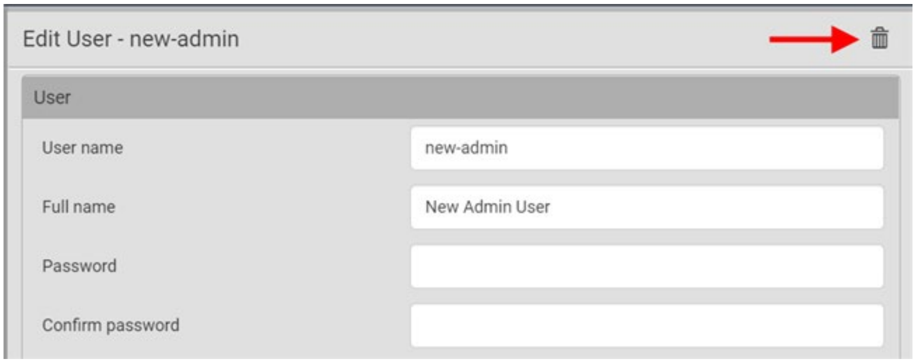
Enabled	User Name ▲	Full Name	Roles
✓	admin	Administrator	Admin
✖	John		Operator
✓	Mary		Operator
✓	Teresa		Operator

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 🗑, and confirm the operation.



Edit User - new-admin

User

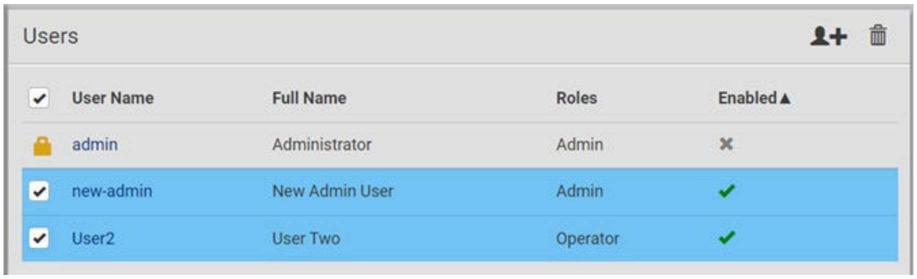
User name	new-admin
Full name	New Admin User
Password	
Confirm password	

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 🗑 then click to confirm.

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



Users

☑	User Name	Full Name	Roles	Enabled ▲
🔒	admin	Administrator	Admin	✖
☑	new-admin	New Admin User	Admin	✓
☑	User2	User Two	Operator	✓

Creating Roles

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

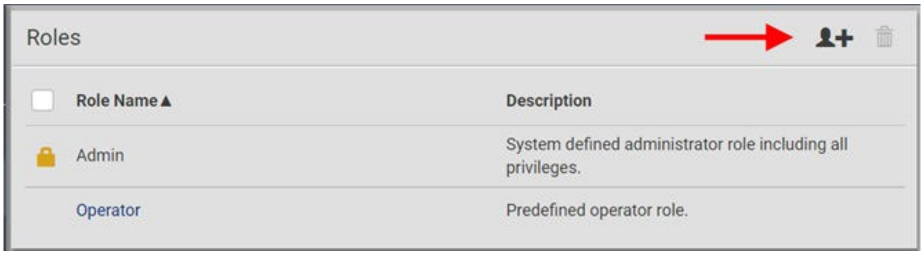
The NX1 PDU provides two built-in roles.

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration • Switch Outlet (for supported models) • Switch Outlet Group (for supported models) • View Event Settings • View Local Event Log

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

► *To create a role:*

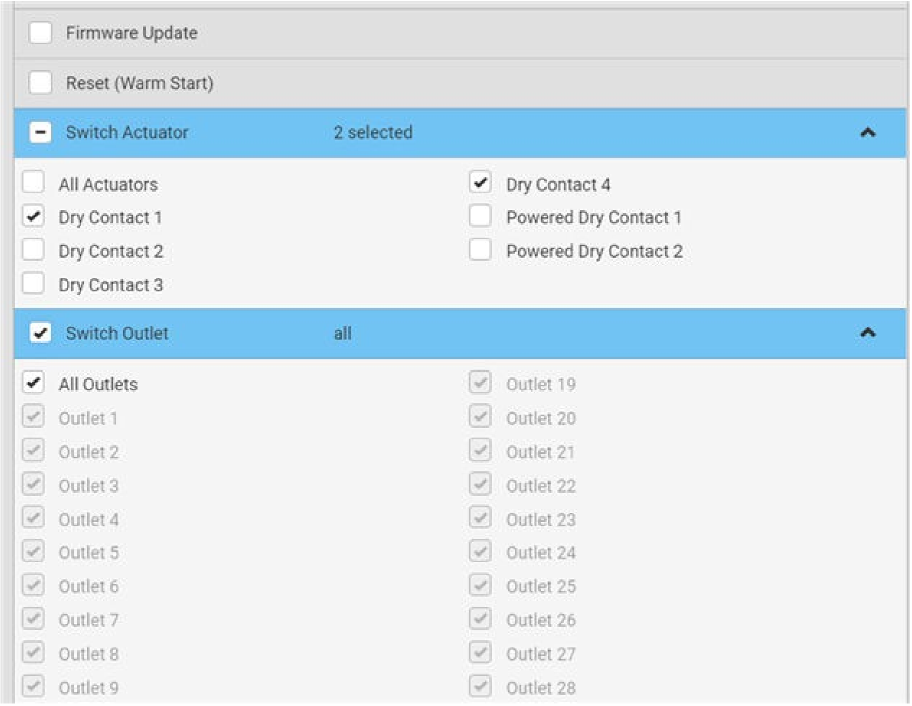
1) Choose User Management > Roles > New icon 👤+ .



Roles

☐ Role Name ▲	Description
Admin	System defined administrator role including all privileges.
Operator	Predefined operator 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 Outlet privileges, you can specify the outlets that users can switch on/off.



□ Firmware Update

□ Reset (Warm Start)

⊟ Switch Actuator 2 selected

□ All Actuators	☑ Dry Contact 4
☑ Dry Contact 1	□ Powered Dry Contact 1
□ Dry Contact 2	□ Powered Dry Contact 2
□ Dry Contact 3	

☑ Switch Outlet all

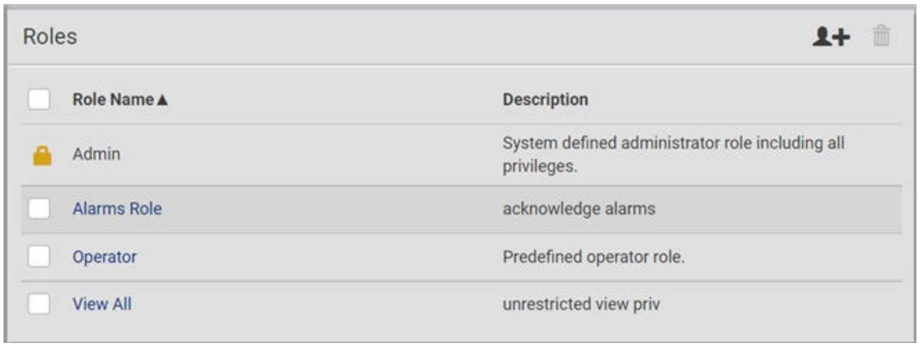
☑ All Outlets	☑ Outlet 19
☑ Outlet 1	☑ Outlet 20
☑ Outlet 2	☑ Outlet 21
☑ Outlet 3	☑ Outlet 22
☑ Outlet 4	☑ Outlet 23
☑ Outlet 5	☑ Outlet 24
☑ Outlet 6	☑ Outlet 25
☑ Outlet 7	☑ Outlet 26
☑ Outlet 8	☑ Outlet 27
☑ Outlet 9	☑ Outlet 28

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.



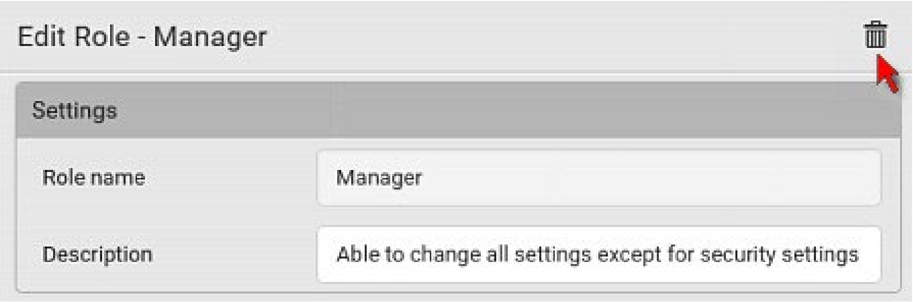
Roles

	Role Name ▲	Description
🔒	Admin	System defined administrator role including all privileges.
□	Alarms Role	acknowledge alarms
□	Operator	Predefined operator role.
□	View All	unrestricted view priv

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 🗑 , and confirm the operation.



Edit Role - Manager

Settings

Role name	Manager
Description	Able to change all settings except for security settings

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 🗑 then click Delete in the confirmation message.

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 .

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.

Field	Description
Pressure unit	Preferred units for pressure -- Pascal or Psi. • Pascal = one newton per square meter • Psi = pounds per square inch

1) 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. • Pascal = one newton per square meter • Psi = pounds per square inch

1) Click Save.

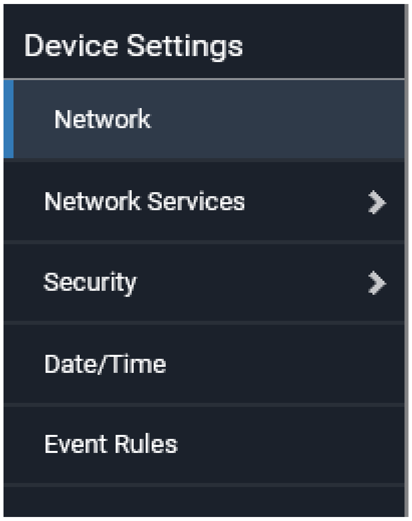
User Interfaces Showing Default Units

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 and Internet protocol-related settings on the Network page after connecting the NX1 PDU to your network.

You can enable the wired networking so that there are multiple IP addresses. 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 NX1 PDU has more than one IPv4 or IPv6 address.

However, in the BRIDGING mode, there is only one IP address for wired networking.

Default gateways are configured per interface.

Important: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETHERNET interface do NOT function.

► *After enabling either or both Internet protocols:*

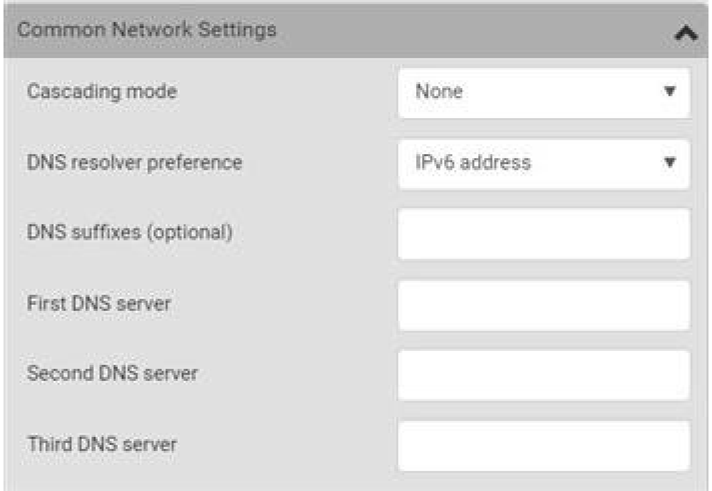
After enabling IPv4 and/or IPv6, all but not limited to the following protocols will be compliant with the selected Internet protocol(s):

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

Note: NX1 PDU 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.



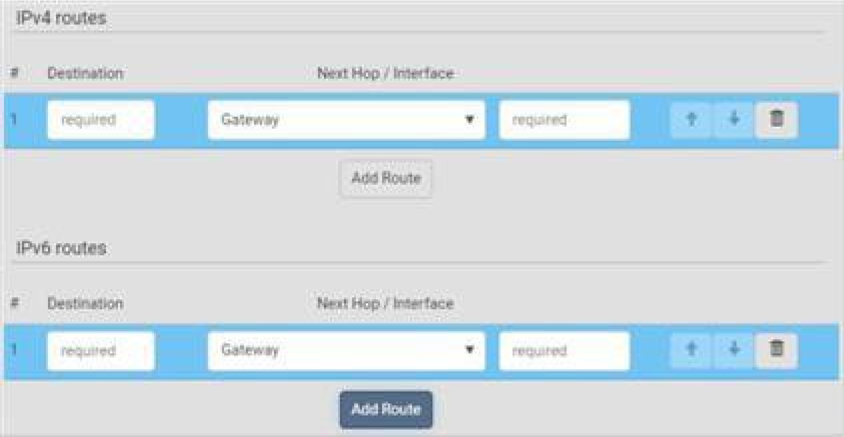
Common Network Settings

Cascading mode	None
DNS resolver preference	IPv6 address
DNS suffixes (optional)	
First DNS server	
Second DNS server	
Third DNS server	

Field	Description
Cascading mode	Leave it to the default "None" unless you are establishing a cascading chain. • Setting the Cascading Mode
DNS resolver preference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. • IPv4 address: Use the IPv4 addresses. • IPv6 address: Use the IPv6 addresses.
DNS suffixes (optional)	Specify a DNS suffix name if needed.

Field	Description
First/Second/ Third DNS server	Manually specify static DNS server(s). • If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. • If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, DHCP-assigned DNS servers are used.

You can manually configure or the route information using IPv4 and IPv6 static routes. See Static Route Examples and Static Route Interface Names.



802.1 x Security Overview

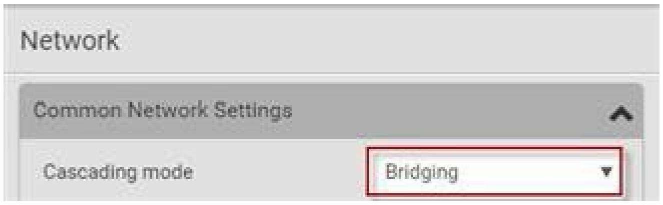
You can configure IEEE 802.1X authentication separately on each LAN port to give NX1 PDU a secure access on your LAN or WLAN. This authentication protocol will authenticate a user's identity based on their credentials or certificate, which will be verified by their RADIUS authentication server. 802.1X 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 NX1 PDU to exchange the secure information. See Setting Up a TLS Certificate to configure and upload the proper certificate.

Ethernet (Wired) Interface Settings

On the Network page, click the ETHERNET section to configure the port.

► *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.



Network

Common Network Settings

Cascading mode: Bridging

► *IPv4 settings:*

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP auto configuration	Select the method to configure IPv4 settings. • *DHCP*: Auto-configure IPv4 settings via DHCP servers. • *Static*: Manually configure the IPv4 settings.
Preferred hostname	Enter the hostname you prefer for IPv4 connectivity

- 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:*

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP auto configuration	Select the method to configure IPv6 settings. • *Automatic*: Auto-configure IPv6 settings via DHCPv6. • *Static*: Manually configure the IPv6 settings.
Preferred hostname	• Enter the hostname you prefer for IPv6 connectivity

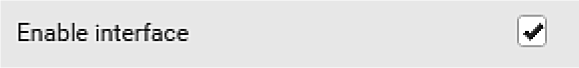
- Automatic settings: Optionally specify the preferred hostname, which must meet the above requirements.
- Static settings:
  - Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

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 ETHERNET section, but not available in the BRIDGE section.



Enable interface ☑

► *Other Ethernet settings:*

Field	**Description**
Speed	Select a LAN speed. • *Auto:* System determines the optimum LAN speed through auto-negotiation. • *10 MBit/s:* Speed is always 10 Mbps. • *100 MBit/s:* Speed is always 100 Mbps.
Duplex	Select a duplex mode. • *Auto:* Selects the optimum transmission mode through auto-negotiation. • *Full:* Data is transmitted in both directions simultaneously. • *Half:* Data is transmitted in one direction at a time.
Current state	Show the LAN's current status, including the current speed and duplex mode.
MTU	• Set the MTU from 1280 to 1500.
Enable LLDP	• Default is enabled. When LLDP is enabled, device discovery is possible with LLDP management software that is often present in network switches.
Authentication	Select an authentication method. • *No Authentication:* No authentication data is required. • *EAP: NX1 PDU 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.*

Field	Description
Outer authentication	This field appears when 'EAP' is selected. There are two authentication methods for EAP. - *PEAP:* A TLS tunnel is established, and an inner authentication method can be specified for this tunnel. - *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Inner authentication	This field appears when both 'EAP' and 'PEAP' are selected. - *MS-CHAPv2:* Authentication based on the given password using MS-CHAPv2 protocol. - *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Identity	This field appears when 'EAP' is selected. Type your user name.
Password	This field appears only when 'EAP', 'PEAP' and 'MS-CHAPv2' are all selected. Type your password.
Client certificate, Client private key, Client private key password	A client certificate is required for two scenarios: (1) EAP+TLS, (2) EAP+PEAP+TLS . PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional. - Private keys in PKCS#1 and PKCS#8 formats are supported. - Client Private Key Password should be entered only when your private key is encrypted with a password. - To view the uploaded certificate, click Show Client Certificate. - To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.

Field	Description
CA certificate	This field appears when 'EAP' is selected. CA certificate is required when "Enable verification of TLS certificate chain" is selected by default; and strongly recommended

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.
Browse button	Click this button to import the certificate of the issuing CA. Then you can: • Click Show to view the certificate's content. • Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period. • After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Allow connection if system clock is incorrect	If powered off for a long time, the system time may be incorrect. 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. 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.

Diagnostic Log for Network Connections

A diagnostic log for inspecting connection errors that occurred during the EAP authentication 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 > Show EAP Authentication 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

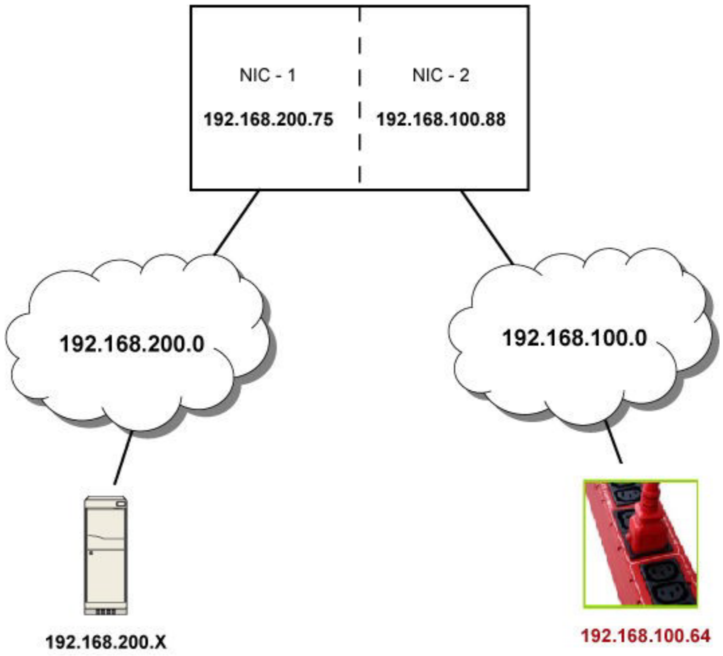
This section describes two static route examples: IPv4 and IPv6. Both examples assume that two network interface controllers (NIC) have been installed in one network server, leading to two available subnets, and IP forwarding has been enabled. All of the NICs and NX1 PDU devices in the examples use static 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.

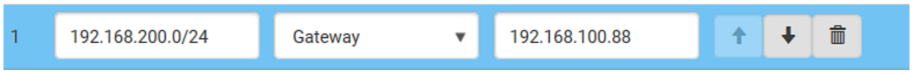
► *IPv4 example:*

- Your NX1 PDU: *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 NX1 PDU 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.

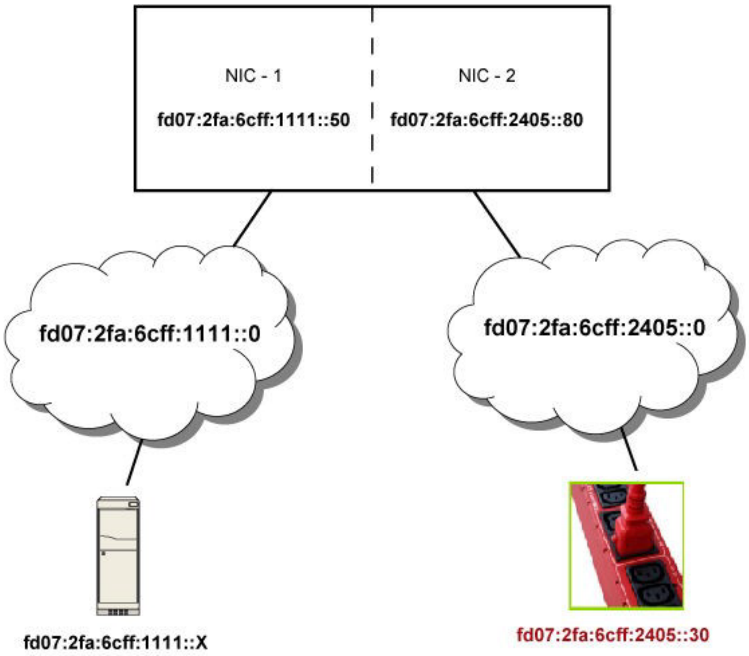


1	192.168.200.0/24	Gateway ▼	192.168.100.88	↑ ↓ 🗑

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.

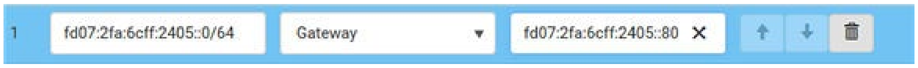
► *IPv6 example:*

- Your NX1 PDU: *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 NX1 PDU 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.

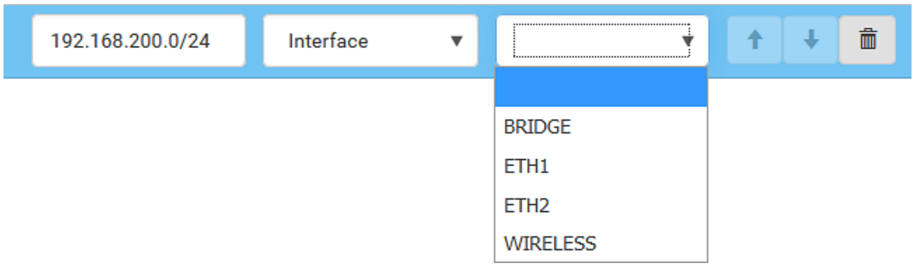


1 fd07:2fa:6cff:2405::0/64 | Gateway | fd07:2fa:6cff:2405::80

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 |

► *Interface list:*

Interface name	***Description***
BRIDGE	***When another wired network is connected to the Ethernet port of your NX1 PDU, and your NX1 PDU has been set to the bridging mode, select this interface name instead of the Ethernet interface.***
ETH1	***When another wired network is connected to the ETH1 port of your NX1 PDU, select this interface name.***

Setting the Cascading Mode

See Chapter Cascading Multiple NX1 PDUs via USB for Sharing Ethernet Connectivity

for 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.

Mode	**Description**
None	No cascading mode is enabled. This is the default.
Bridging	Each device in the cascading chain is accessed with a different IP address.
Port Forwarding	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.

3) 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
Port forwarding role (available on all cascaded devices)	*Primary or Expansion.* This is to determine which device is the primary and which ones are expansion devices.
Downstream interface (available on the primary device only)	*USB* This is to determine which port on the primary device is connected to Expansion 1.

4) (Optional) Configure the network settings by clicking the BRIDGE or ETHERNET 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 ETHERNET section.

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

5) 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.

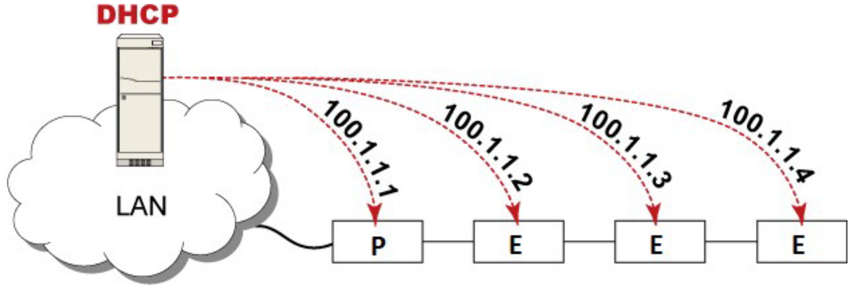
Cascading Modes Overview

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.

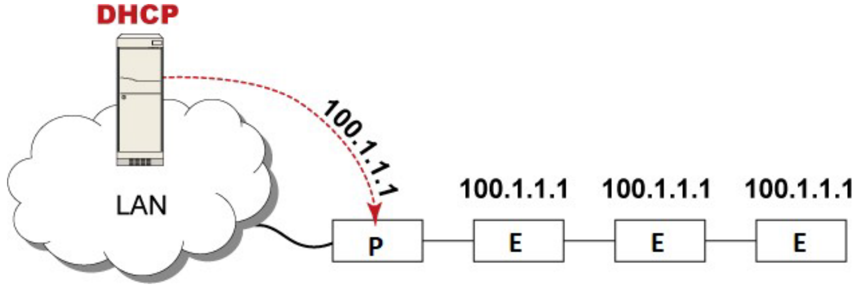
► *"Bridging" mode:*



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.

► *Comparison between cascading modes:*

- 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.

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
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.

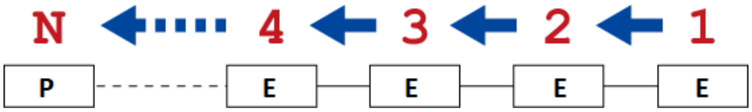
   - You must disconnect the LAN cable and ALL cascading cables connected to the two devices first before swapping them, and then reconnecting all cables.

► *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.

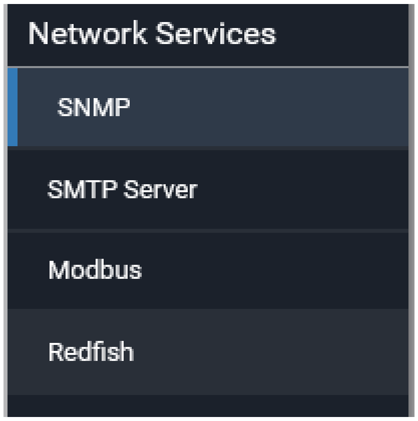
The following diagram indicates the correct sequence. 'N' is the final one.

- P = Primary device
- E = Expansion device



Configuring Network Services

NX1 PDU supports the following network communication services.



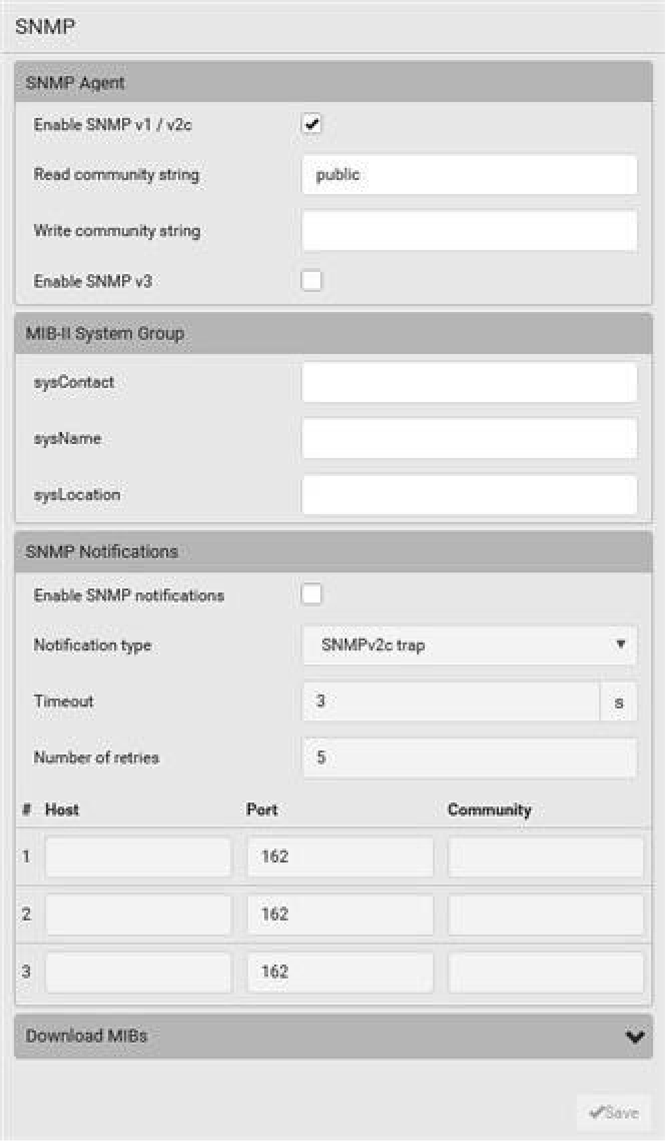
Configuring SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the NX1 PDU. 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.

► *To configure SNMP communication:*

1) Choose Device Settings > Network Services > SNMP.



SNMP

SNMP Agent

Enable SNMP v1 / v2c ☑

Read community string: public

Write community string:

Enable SNMP v3 □

MIB-II System Group

sysContact:

sysName:

sysLocation:

SNMP Notifications

Enable SNMP notifications □

Notification type: SNMPv2c trap

Timeout: 3 s

Number of retries: 5

#	Host	Port	Community
1		162	
2		162	
3		162	

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 NX1 PDU 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 NX1 PDU 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. - Default is 25
Sender email address	Type an email address for the sender.
Number of sending retries	Type the number of email retries. - Default is 2 retries
Time between sending retries	Type the interval between email retries in minutes. - Default is 2 minutes.
Field	**Description**
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. - The length of user name and password ranges between 4 and 64. Case sensitive. - Spaces are not allowed for the user name, but allowed for the password.
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: - Click Show to view the certificate's content. - Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	- Select this checkbox to make the authentication succeed regardless of the certificate's validity period. - After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.

1) 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.
2) Click Save.

► *Special note for AES ciphers:*

The NX1 PDU device's TLS-based protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between NX1 PDU and the client (such as a web browser), which is impacted by the cipher priority of NX1 PDU and the client's cipher availability/settings.

Tip: To force NX1 PDU to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Changing Modbus Settings

The NX1 PDU supports both the Modbus/TCP and Modbus Gateway features. Enable either or both Modbus features according to your needs.

► *Modbus/TCP Access:*

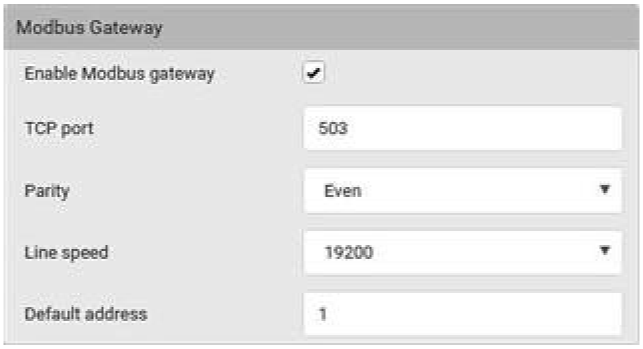
You can enable or disable the Modbus/TCP access to NX1 PDU, set it to the read-only mode, or change the TCP port.

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 checkbox of the "Enable read-only mode" field. To enable the read-write mode, deselect it.

► *Modbus Gateway:*

If connecting the Modbus RTU devices to NX1 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 NX1 PDU.

1) To allow the Modbus TCP clients on the network to communicate with the Modbus RTU devices connected to the NX1 PDU, select the 'Enable Modbus gateway' checkbox.



Modbus Gateway

Enable Modbus gateway	☑
TCP port	503
Parity	Even ▼
Line speed	19200 ▼
Default address	1

2) Now configure the fields shown.

Field	Description
TCP port	Use the default port 503, or assign a different port. Valid range is 1 to 65535. Note: Port 502 is the default Modbus/TCP port for NX1 PDU, so you cannot use that port for the Modbus Gateway.
Parity, Line speed	Use the default values, or update if the Modbus RTU devices are using different communication parameters.

Default address	If the Modbus TCP client does not support Modbus RTU unit identifier addressing, enter a Default Address. If you must provide a unit identifier address: • Only one Modbus RTU device is supported. • The unit identifier address you provide is applied to the Modbus RTU device connected to NX1 PDU. Note that each Modbus RTU device's unit identifier address must be unique. 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.

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

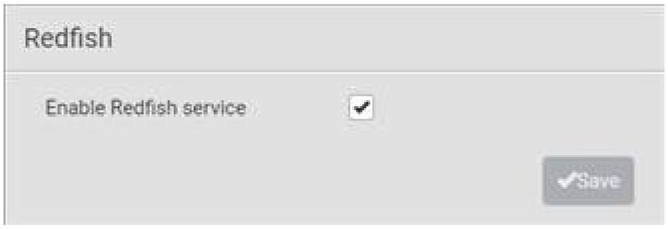
It also allows you to do the following actions

- 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.

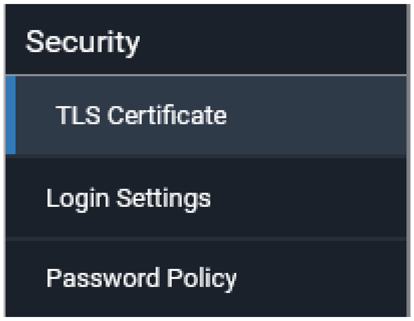


Redfish

Enable Redfish service ☑

Configuring Security Settings

The NX1 PDU 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.



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 NX1 PDU.

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.

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

- Make the NX1 PDU create a *self-signed* certificate.
- Appropriate, valid certificate and key files are already available, and you only need to import them.

Creating a CSR

Follow this procedure to create the CSR.

► *To create a CSR:*

1) Choose Device Settings > Security > TLS Certificate.
2) In the New TLS Certificate or 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.
Organization	The registered name of your company.
Organizational unit	The name of your department.
Common name	The fully qualified domain name (FQDN) of your NX1 PDU.
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: • 2048 bits • 3072 bits
Key Type/Elliptic Curve	Key type ECDSA requires you to select the elliptic curve: • NIST-P-256 • NIST P-384 • NIST P-521
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. This information is optional. The value should be 4 to 64 characters long. Case sensitive.

1) Click Create New TLS Key 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.

3) To store the newly-created private key on your computer, click Download Key in the New TLS Certificate 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 CSR.

After receiving the CA-signed certificate, install it onto the NX1 PDU.

► *To install the CA-signed certificate:*

1) Choose Device Settings > Security > TLS Certificate.

2) Click to navigate to the CA-signed certificate file.

3) Click Upload to install it.

4) 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 NX1 PDU 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.

Field	Description
Common name	The fully qualified domain name (FQDN) of your NX1 PDU.
Email address	An email address where you or another administrative user can be reached.
Key Type/Key Length	Key type RSA requires you to select Key Length: • 2048 bits • 3072 bits
Key Type/Elliptic Curve	Key type ECDSA requires you to select the elliptic curve: • NIST-P-256 • NIST P-384 • NIST P-521
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.

1) Click Create New TLS Key to create both the self-signed certificate and private key. This may take several minutes to complete.
2) Once complete, do the following:
   a. Double check the data shown in the New TLS Certificate 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.
3) (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 NX1 PDU for backup or file transfer. For example, you can install the files onto a replacement NX1 PDU, 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 NX1 PDU 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 NX1 PDU:*

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 NX1 PDU:*

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.

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, type a value or click ▼ to 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.' See *Time Units* .
3) In the 'Maximum number of failed logins' field, type a number. This is the maximum number of login failure the user is permitted before the user is blocked from accessing the NX1 PDU.
4) 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 NX1 PDU.
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.

Setting the Date and Time

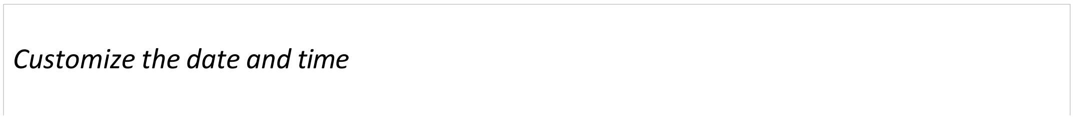
Set the internal clock manually, or link to a Network Time Protocol (NTP) server.

NX1 PDU 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 NX1 PDU to have the same date/time or NTP settings.

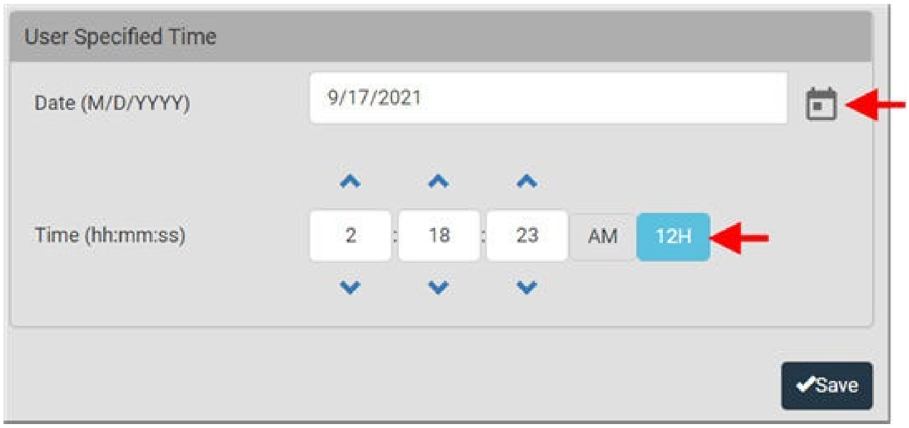
► *To set the date and time:*

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.



User Specified Time

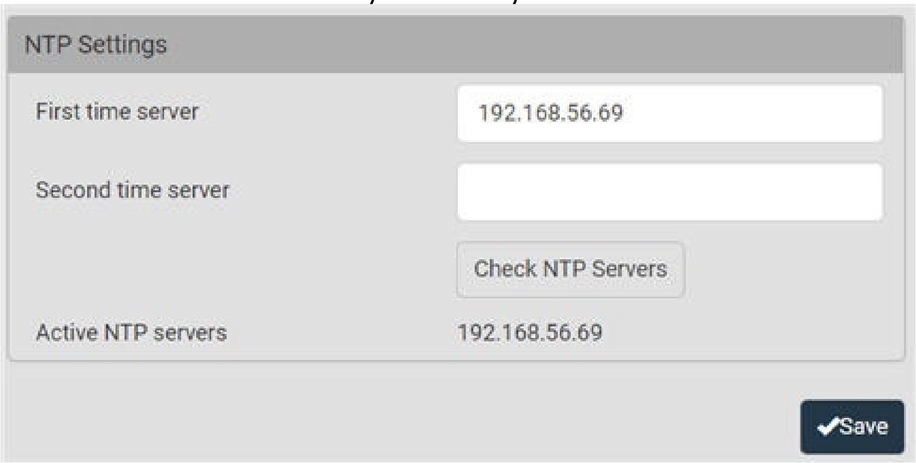
Date (M/D/YYYY) 9/17/2021

Time (hh:mm:ss) 2 : 18 : 23 AM 12H

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.



NTP Settings

First time server 192.168.56.69

Second time server

Active NTP servers 192.168.56.69

Windows NTP Server Synchronization Solution

The NTP client on the NX1 PDU follows the NTP RFC so the NX1 PDU 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 NX1 PDU.

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 NX1 PDU. 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.

Event Rules and Actions

Crete 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 NX1 PDU 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 NX1 PDU 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:*

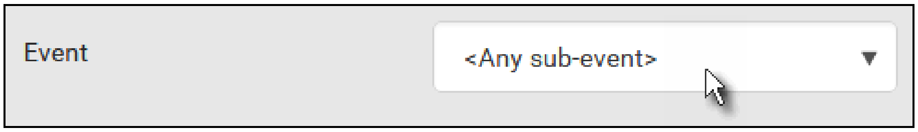
  This causes SNMP traps or informs to be sent to specified IP addresses or hosts when ANY event occurs to the NX1 PDU. It is disabled by default.
- *System Tamper Detection Alarmed:*

  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:*

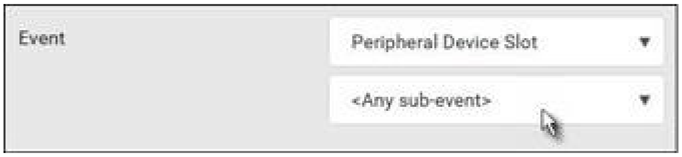
  This causes alarm notifications if a previously available tamper sensor is not detected. It is enabled by default.

► *Event rule configuration illustration:*

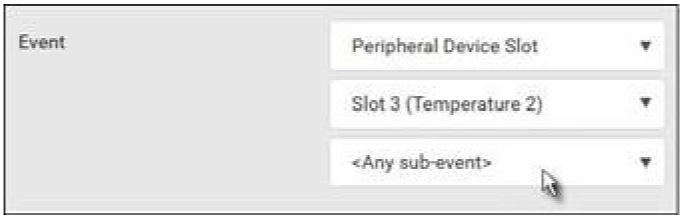
1) Choose Device Settings > Event Rules > New Rule.
2) Click the Event field to select an event type.
   - <Any sub-event> means all events shown on the list.
   - <Any Numeric Sensor> means all numeric sensors, including internal and environmental sensors. <Any Numeric Sensor> is especially useful if 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.

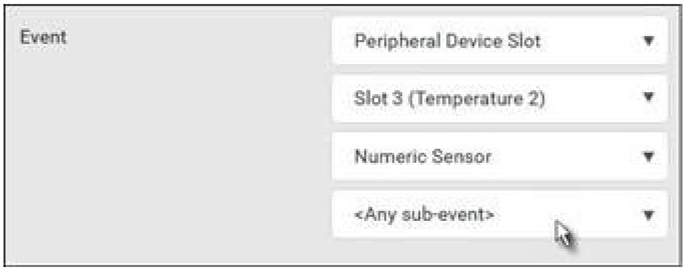


4) In this example, sensor ID 3 (Slot 3) is selected, which is a temperature sensor. Then a new field for this sensor appears. Click this field to specify the type of event(s) you want.



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.



Event

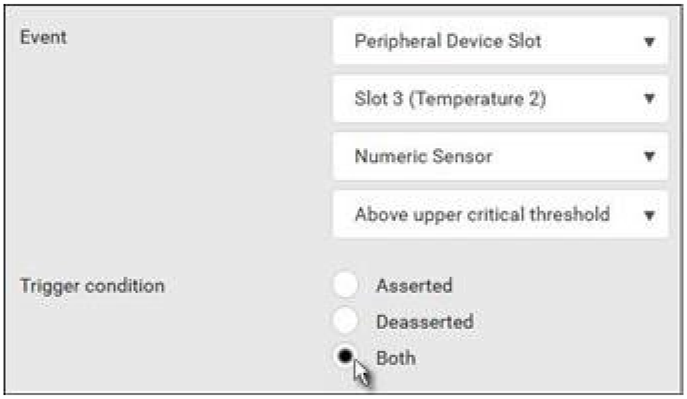
Peripheral Device Slot

Slot 3 (Temperature 2)

Numeric Sensor

<Any sub-event>

6) In this example, 'Above upper critical threshold' is selected because we want the NX1 PDU 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.



Event

Peripheral Device Slot

Slot 3 (Temperature 2)

Numeric Sensor

Above upper critical threshold

Trigger condition

○ Asserted

○ Deasserted

● Both

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 .

8) Add and/or remove actions to configure the rule. Select actions from the 'Available actions' list to create the Select actions list.

► *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	• Asserted: action occurs only when the selected event occurs. That is, the status of the event transits from FALSE to TRUE. • Deasserted: action occurs only when the selected event disappears or stops. That is, the status of the selected event transits from TRUE to FALSE. • Both: action occurs both when the event occurs (asserts) and when the event stops/disappears (deasserts).

Event types	Radio buttons
State sensor state change	• Alarmed/Open/On: action occurs only when the chosen sensor enters the alarmed, open or on state. • No longer alarmed/Closed/Off: action occurs only when the chosen sensor returns to the normal, closed, or off state. • Both: action occurs whenever the chosen sensor switches its state.
Sensor availability	• Unavailable: action occurs only when the chosen sensor is NOT detected and becomes unavailable. • Available: action occurs only when the chosen sensor is detected and becomes available. • Both: action occurs both when the chosen sensor becomes unavailable or available.
Network interface link state	• Link state is up: action occurs only when the network link state changes from down to up. • Link state is down: action occurs only when the network link state changes from up to down. • Both: action occurs whenever the network link state changes.
Function enabled or disabled	• Enabled: action occurs only when the chosen function is enabled. • Disabled: action occurs only when the chosen function is disabled. • Both: action occurs when the chosen function is either enabled or disabled.
Restricted service agreement	• Accepted: action occurs only when the specified user accepts the restricted service agreement. • Declined: action occurs only when the specified user rejects the restricted service agreement. • Both: action occurs both when the specified user accepts or rejects the restricted service agreement.
Server monitoring event	• Monitoring started: action occurs only when the monitoring of any specified server starts. • Monitoring stopped: action occurs only when the monitoring of any specified server stops. • Both: action occurs when the monitoring of any specified server starts or stops.

Event types	Radio buttons
Server reachability	• Unreachable: action occurs only when any specified server becomes inaccessible. • Reachable: action occurs only when any specified server becomes accessible. • Both: action occurs when any specified server becomes either inaccessible or accessible.
Device connection or disconnection, such as a USB-cascaded device	• Connected: action occurs only when the selected device is physically connected to it. • Disconnected: action occurs only when the selected device is physically disconnected from it. • Both: action occurs both when the selected device is physically connected to it and when it is disconnected.

Default Log Messages for All Products

Listed here are all default messages for all 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 deassetion	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 > 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]'		
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 [FORMATTEDEXTSENSORSLOT] asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	

Peripheral Device Slot > Numeric Sensor > Below lower warning threshold	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
Peripheral Device Slot > Numeric Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] has become unavailable.	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] is no longer unavailable; it is now [SENSORSTATENAME].	
Peripheral Device Slot > State Sensor > Alarmed	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] is [SENSORSTATENAME].	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] is [SENSORSTATENAME].	
Peripheral Device Slot > State Sensor > Switched by user	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] has been switched to [SENSORSTATENAME] by user '[USERNAME]' from host '[USERIP]'.		
Peripheral Device Slot > State Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] has become unavailable.	Peripheral device '[EXTSENSORNAME]' in [FORMATTEDEXTSENSORSLOT] 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 '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' 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 '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' 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 '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT]; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Critical	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' entered critical state.	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' exited critical state; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Failed	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' entered failed state.	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' exited failed state; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Normal	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' entered normal state.	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' exited normal state; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Open	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' is open. [OCPTRIPCAUSEINFO]	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' is no longer open; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Self-Test	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' started self test.	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' finished self test; it is now [SENSORSTATENAME].	
PDU > Overcurrent Protector > Sensor > Unavailable	Sensor '[OCPSENSOR]' on PDU [PDUNUMBER] overcurrent protector '[OCP]' has become unavailable.	Sensor '[OCPSENSOR]' 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 [FORMATTEDEXTPORT] is [FUSESTATENAME].	Fuse of [FORMATTEDEXTPORT] 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]'.		

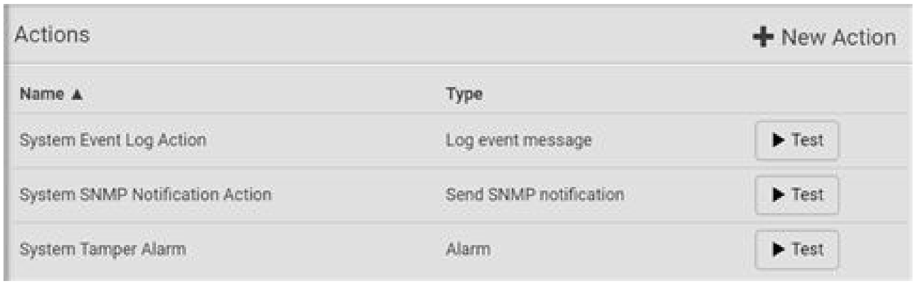
Available Actions

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).

► *To test an action:*

- Click the Test button next to the Action. The action is triggered and you can verify it.



Actions

Name ▲	Type	
System Event Log Action	Log event message	▶ Test
System SNMP Notification Action	Send SNMP notification	▶ Test
System Tamper Alarm	Alarm	▶ Test

► *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.

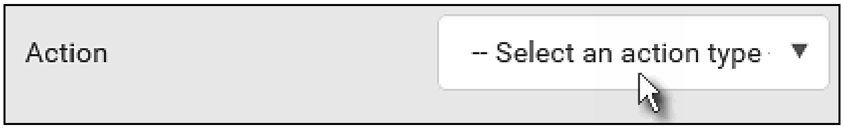
  Note: No IP addresses are specified for this notification action by default so you must enter IP addresses before applying this action to any event rule. Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa.

- *System Tamper Alarm:*

  This action causes the NX1 PDU 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 NX1 PDU 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 > ✚ New Action .
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:

- 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 NX1 PDU 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.

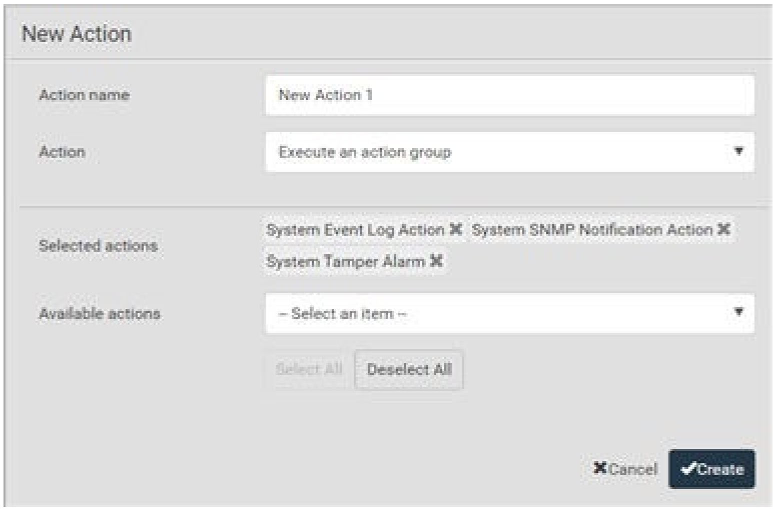
Action Group

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 > ✚ New Action .
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 it's X.
5) Click Create to save the action.



New Action

Action name: New Action 1

Action: Execute an action group

Selected actions: System Event Log Action ✖ System SNMP Notification Action ✖ System Tamper Alarm ✖

Available actions: -- Select an item --

Change Load Shedding State

The "Change load shedding state" action is available only when your NX1 PDU 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 > ✚ New Action .
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.

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 NX1 PDU is outlet- switching capable.

You can configure the NX1 PDU 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 NX1 PDU and the same NX1 PDU supplies power to it. See Monitoring Server Accessibility .

Tip: If the server has multiple power cords, make sure all of its power cords are connected to the same NX1 PDU 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 NX1 PDU 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 NX1 PDU to push sensor log to a remote server after a certain event occurs, including logs of internal sensors and environmental sensors.

If you have connected asset strips, you can also configure the NX1 PDU 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.

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 NX1 PDU 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 > + New Action .
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 NX1 PDU 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.
- Peripheral device sensors, which can be any environmental sensor packages connected to the NX1 PDU, such as temperature or humidity sensors.

See Send Sensor Report Example.

► *Operation:*

1) Choose Device Settings > Event Rules > + New Action .
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.

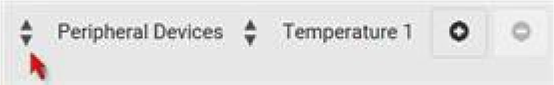
The messaging action types include:

- Log event message
- Syslog message
- Send email
- Send SMS message

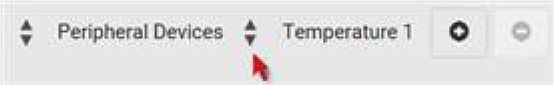
4) If no messaging actions are available, create them now.

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.

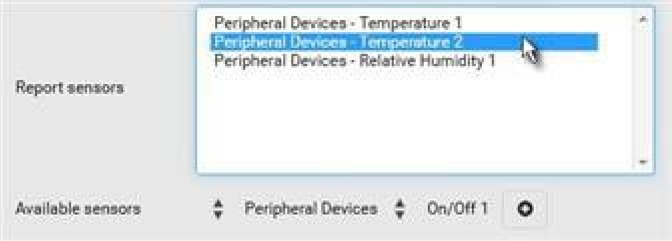


   c. Click ⊕ to add the selected sensor to the Report Sensors list box.

   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.


Report sensors
Peripheral Devices - Temperature 1
Peripheral Devices - Temperature 2
Peripheral Devices - Relative Humidity 1
Available sensors
Peripheral Devices
On/Off 1

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® GSM MC52i modem, must be plugged into the NX1 PDU in order to send SMS messages.

Note: The NX1 PDU 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 > ✚ New Action .
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 an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

► *Operation:*

1) Choose Device Settings > Event Rules > ✚ New Action .
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 NX1 PDU 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. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase

"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

Start or Stop a Lua Script

If you have created or loaded a Lua script file into the NX1 PDU, you can have that script automatically run or stop in response to a specific event.

See Lua Scripts

► 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 NX1 PDU 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 NX1 PDU is outlet-switching capable. This action turns on, off or power cycles a specific outlet.

► *Operation:*

1) Choose Device Settings > Event Rules > ✚ New Action .
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.

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.

NX1 PDU 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	• In the 'UDP port' field, type an appropriate port number. Default is 514. • Select the 'Legacy BSD syslog protocol' checkbox if applicable.

Transport protocols	**Next steps**
TCP	NO TLS certificate is required. Type an appropriate port number in the 'TCP port' field.
TCP+TLS	A TLS certificate is required. Do the following: a. Type an appropriate port number in the 'TCP port' field. Default is 6514. b. In the 'CA certificate' field, click Browse to select a TLS certificate. After importing the certificate, you may: • Click Show to view its contents. • Click Remove to delete it if it is inappropriate. c. Determine whether to select the 'Allow expired and not yet valid certificates' checkbox. • To always send the event message to the specified syslog server as long as a TLS certificate is available, select this checkbox. • To prevent the event message from being sent to the specified syslog server when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect this checkbox.

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 NX1 PDU 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.

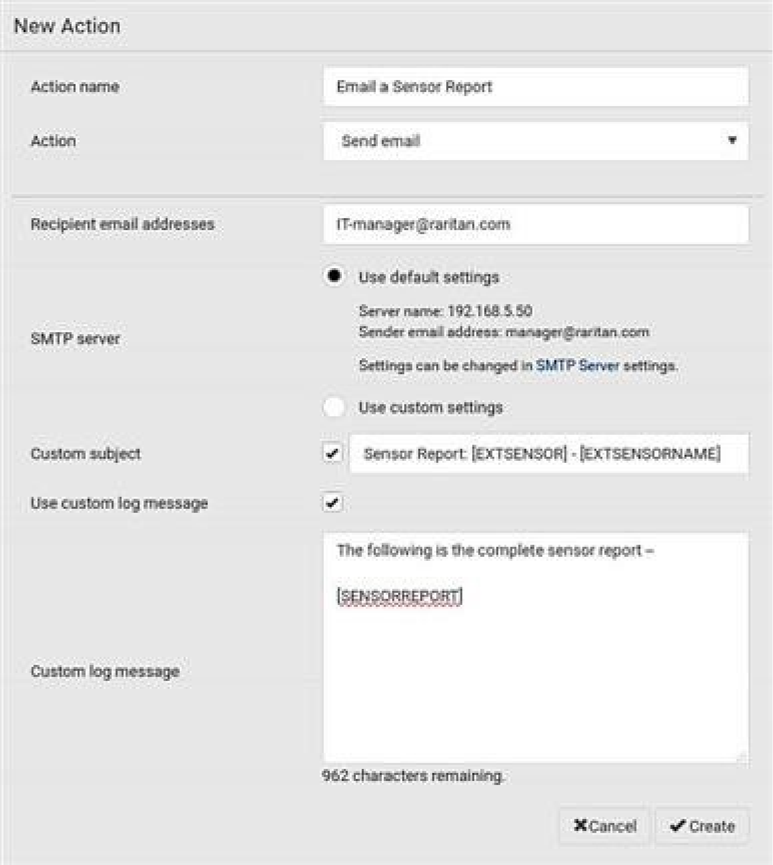
Send Sensor Report Example

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.

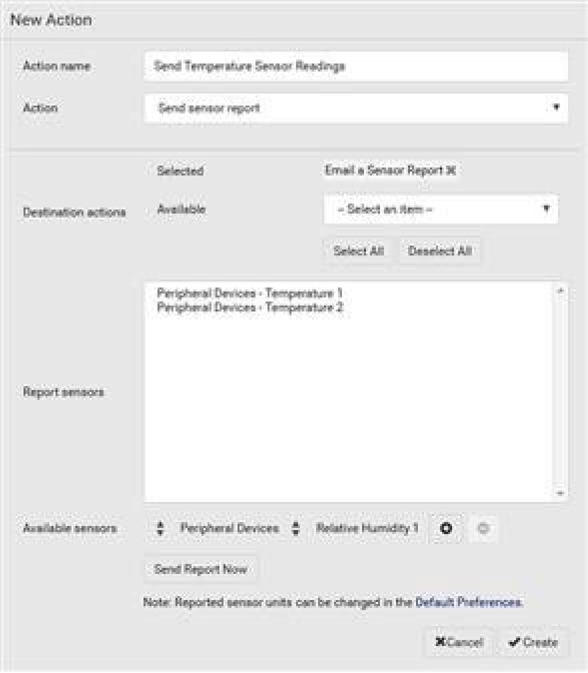


New Action

Action name	Email a Sensor Report
Action	Send email ▾
Recipient email addresses	IT-manager@raritan.com
SMTP server	● Use default settings Server name: 192.168.5.50 Sender email address: manager@raritan.com Settings can be changed in SMTP Server settings. ○ Use custom settings
Custom subject	☑ Sensor Report: [EXTSENSOR] - [EXTSENSORNAME]
Use custom log message	☑
Custom log message	The following is the complete sensor report – [SENSORREPORT] 962 characters remaining.

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: Email a Sensor Report ✖

Available: -- Select an item --

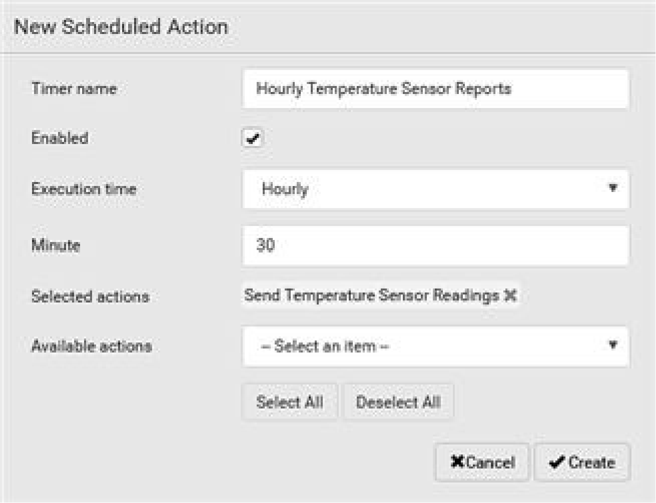
Report sensors:
Peripheral Devices - Temperature 1
Peripheral Devices - Temperature 2

Available sensors: Peripheral Devices / Relative Humidity 1

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.



New Scheduled Action

Timer name: Hourly Temperature Sensor Reports

Enabled: ☑

Execution time: Hourly

Minute: 30

Selected actions: Send Temperature Sensor Readings ✖

Available actions: -- Select an item --

- 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

Placeholder	Definition
[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 Note: 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.
[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

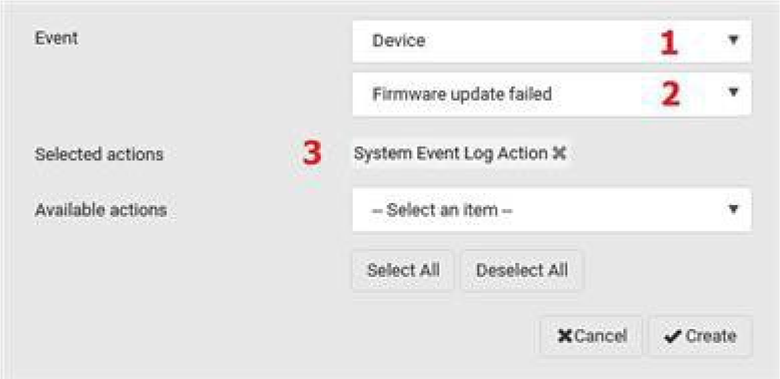
In this example, we want the NX1 PDU to record the firmware upgrade failure in the internal log when it happens.

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 NX1 PDU responds to the event related to firmware upgrade failure.
3) To make NX1 PDU record the firmware update failure event in the internal log, select "System Event Log Action" in the 'Available actions' field.



Event: Device 1 ▾

Firmware update failed 2 ▾

Selected actions 3 System Event Log Action ✖

Available actions: -- Select an item -- ▾

Sample Outlet-Level Event Rule

In this example, we want the NX1 PDU to send SNMP notifications to the SNMP manager for any sensor change event of outlet 3.

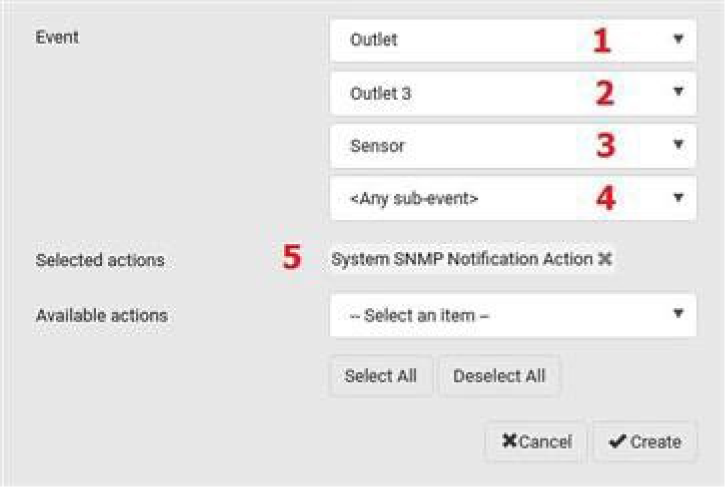
The event rule involves:

- 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 NX1 PDU 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.



Event: Outlet 1

Outlet 3 2

Sensor 3

<Any sub-event> 4

Selected actions 5: System SNMP Notification Action ✖

Available actions: -- Select an item --

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 NX1 PDU to send SNMP notifications to the SNMP manager for any sensor change event of the Inlet I1.

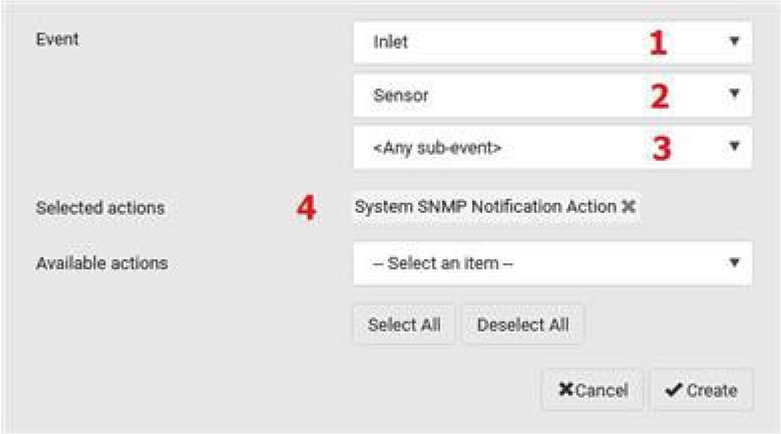
The event rule involves:

- 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 NX1 PDU 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.



Event: Inlet 1
Sensor 2
<Any sub-event> 3
Selected actions 4 System SNMP Notification Action ✖
Available actions – Select an item –

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.

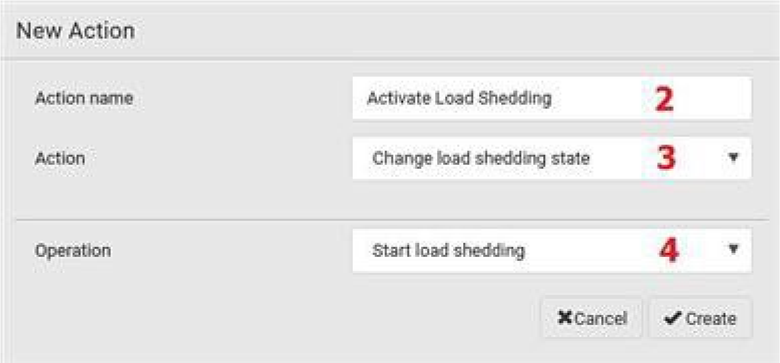
Sample Environmental-Sensor-Level Event Rule

This section applies to outlet-switching capable models only.

In this example, we want NX1 PDU 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."



New Action

Action name: Activate Load Shedding 2

Action: Change load shedding state 3

Operation: Start load shedding 4

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:

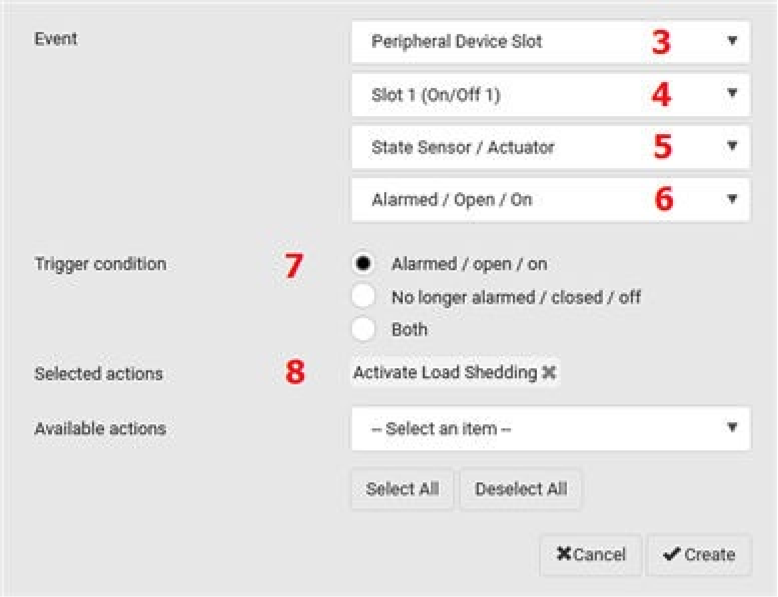
- Event: Peripheral Device Slot > Slot 1 > State Sensor > Alarmed/Open/On
- Trigger condition: Alarmed
- Action: Activate Load Shedding

► *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 are available on the Peripherals page.

5) Select "State Sensor " because the contact closure sensor is a state sensor.
6) Select "Alarmed" since we want the NX1 PDU 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 "Activate Load Shedding" from the 'Available actions' list.



Event: Peripheral Device Slot ▾ / Slot 1 (On/Off 1) ▾ / State Sensor / Actuator ▾ / Alarmed / Open / On ▾

Trigger condition: ● Alarmed / open / on ○ No longer alarmed / closed / off ○ Both

Selected actions: Activate Load Shedding ✖

Available actions: -- Select an item -- ▾

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 NX1 PDU 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 NX1 PDU 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 NX1 PDU 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 NX1 PDU to continuously power cycle outlets 1 and 2 in turn.

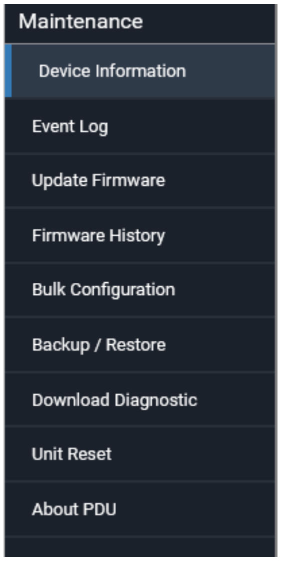
Event selected	Action included
Outlet > Outlet 1 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 2 (Switch outlets --> Cycle Outlet --> Outlet 2)
Outlet > Outlet 2 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 1 (Switch outlets --> Cycle Outlet --> 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 NX1 PDU does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the NX1 PDU uses. See "To De-assert" and Deassertion Hysteresis.

Maintenance

Click 'Maintenance' in the *Menu* to view the options.



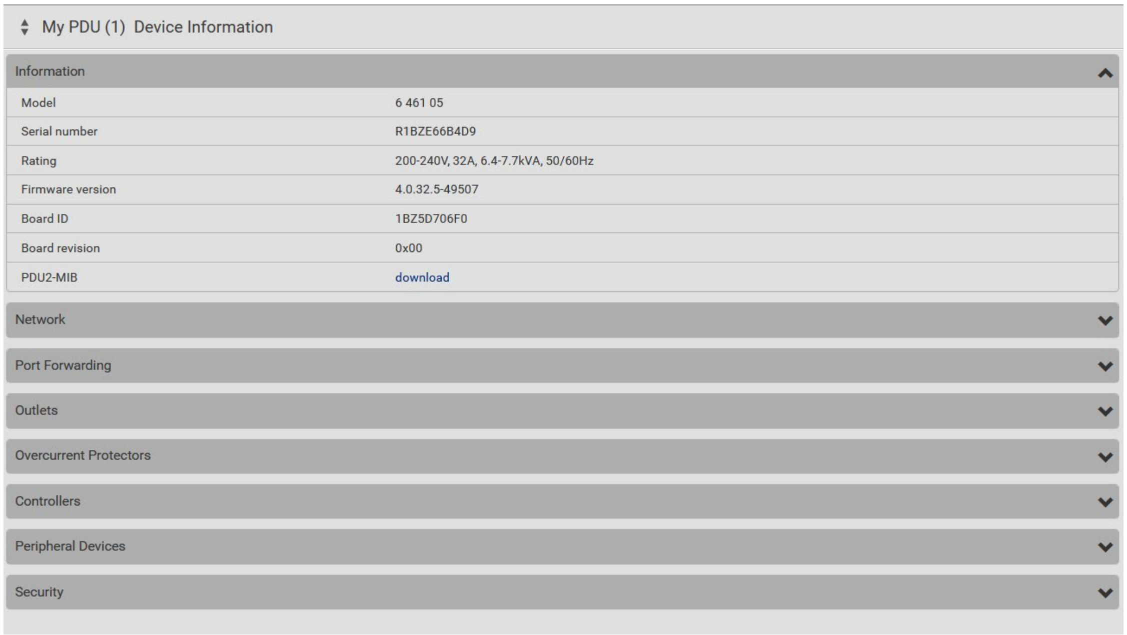
Device Information

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.



My PDU (1) Device Information

Information

Model	6 461 05
Serial number	R1BZE66B4D9
Rating	200-240V, 32A, 6.4-7.7kVA, 50/60Hz
Firmware version	4.0.32.5-49507
Board ID	1BZ5D706F0
Board revision	0x00
PDU2-MIB	download

Network

Port Forwarding

Outlets

Overcurrent Protectors

Controllers

Peripheral Devices

Security

Section title	Information shown
Information	General device information, such as model name, serial number, firmware version, hardware revision, MIB download link(s) and so on.
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.
Security	SSH host keys.

Viewing 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 clear the local log:*

1) Click Clear Log on the top-right corner.
2) Click Clear Log on the confirmation message.

Updating the Firmware

When performing the firmware update, the NX1 PDU 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.

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.

► *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.

- If anything is incorrect, click Discard Upload.

6) To proceed with the update, click Update Firmware.

Warning: Do NOT power off the NX1 PDU 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.
- 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 NX1 PDU 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 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.

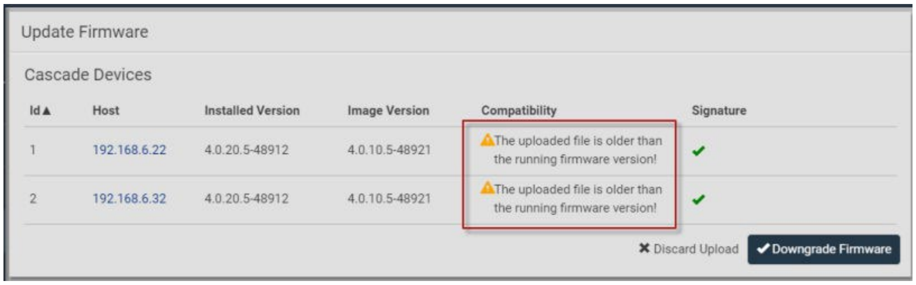
External factors include, but are not limited to: network throughput, firmware file size, and speed at which the firmware is retrieved from the storage location. Internal factors include: the necessity of upgrading the firmware on the microcontroller and the number of microcontrollers that require upgrade (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 NX1 PDU 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.

Downgrade Firmware (not supported)

Safety measures are added to prevent the downgrade of the NX1 PDU. You will see compatibility warnings about the older firmware version after uploading the firmware. A downgraded device may not function properly, and it may lose settings.

WARNING: Downgrades are not officially supported and must be discussed in advance with Technical Support.



Update Firmware

Cascade Devices

Id ▲	Host	Installed Version	Image Version	Compatibility	Signature
1	192.168.6.22	4.0.20.5-48912	4.0.10.5-48921	⚠The uploaded file is older than the running firmware version!	✓
2	192.168.6.32	4.0.20.5-48912	4.0.10.5-48921	⚠The uploaded file is older than the running firmware version!	✓

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 NX1 PDU 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 NX1 PDU device where the configuration file is downloaded/saved. A target device is the NX1 PDU 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.

► *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.

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 *not* be downloaded.
Included	The setting will be downloaded.

Option	Description
Inherited	The setting will follow its parent setting (that is, the upper-level setting). • If you select 'Excluded' for its upper-level setting, this setting will be also excluded. • If you select 'Included' for its upper-level setting, this setting will be also included. The option inherited from its parent setting will be enclosed in parentheses.
Built-in	The setting will follow the same setting of Raritan's built-in profile. • If 'Excluded' is selected in the built-in profile, this setting will be also excluded. • If 'Included' is selected in the built-in profile, this setting will be also included. The option inherited from the built-in profile will be enclosed in parentheses. *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.*

1) 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	• Partial content is base64 encoded. • Its content is encrypted using the AES-128 encryption algorithm. • The file is saved to the TXT format
Cleartext	• Content is displayed in clear text. • The file is saved to the TXT format.

1) 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.
2) 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 NX1 PDU devices, use the Bulk Configuration feature instead.

All NX1 PDU 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.

► *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	• Partial content is base64 encoded. • Its content is encrypted using the AES-128 encryption algorithm. • The file is saved to the TXT format
Cleartext	• Content is displayed in clear text. • The file is saved to the TXT format.

1) 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 NX1 PDU resets and the Login page re-appears, indicating that the restore is

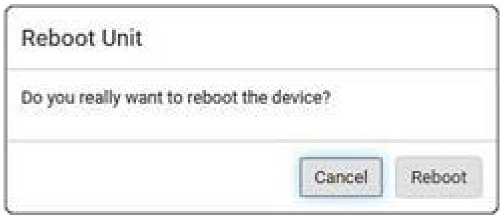
Rebooting

You can remotely reboot the NX1 PDU 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.

► *To reboot the device:*

1) Choose Maintenance > Unit Reset > Reboot Unit.



Reboot Unit

Do you really want to reboot the device?

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

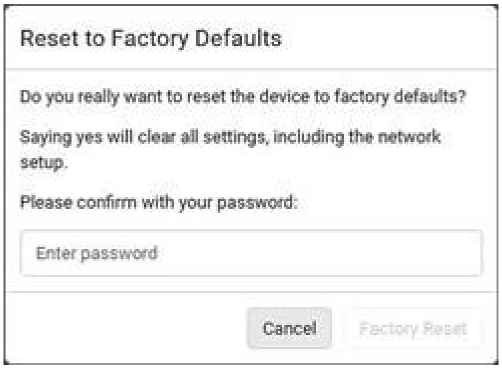
You must have the Administrator Privileges to reset all settings to factory defaults.

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.

► *To reset the device to factory defaults:*

1) Choose Maintenance > Unit Reset > Reset to Factory Defaults.



Reset to Factory Defaults

Do you really want to reset the device to factory defaults?

Saying yes will clear all settings, including the network setup.

Please confirm with your password:

Enter password

2) Type your password and then click Factory Reset.
3) A message appears, with a countdown timer showing the remaining time of the operation. It takes about two minutes to complete.
4) 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.

Using SNMP

This SNMP section helps you set up the NX1 PDU for use with an SNMP manager. The NX1 PDU 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

To communicate with an SNMP manager, you must enable SNMP protocols on the NX1 PDU. 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 NX1 PDU.

Important: You must download the SNMP MIB for your NX1 PDU to use with your SNMP manager.

► *To enable SNMP v1/v2c and/or v3 protocols:*

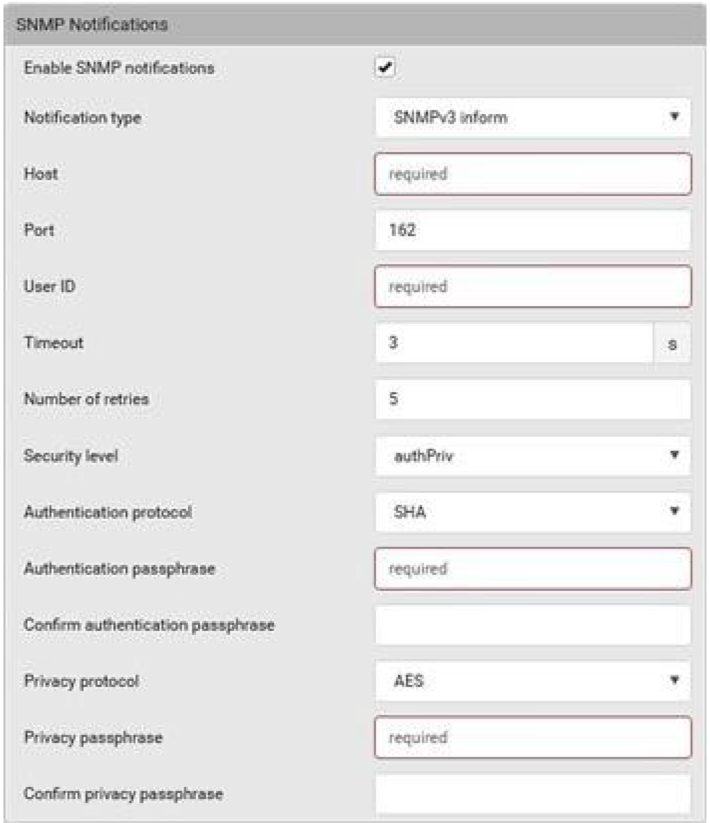
1) Choose Device Settings > Network Services > SNMP.
2) In the SNMP Agent section, enable SNMP v1/v2c or SNMP v3, and configure related fields, such as the community strings.
   - If SNMP v3 is enabled, you must determine which users shall have the SNMP v3 access permission.

► *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.



SNMP Notifications

Enable SNMP notifications	☑
Notification type	SNMPv3 inform ▾
Host	required
Port	162
User ID	required
Timeout	3 s
Number of retries	5
Security level	authPriv ▾
Authentication protocol	SHA ▾
Authentication passphrase	required
Confirm authentication passphrase	
Privacy protocol	AES ▾
Privacy passphrase	required
Confirm privacy passphrase	

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.

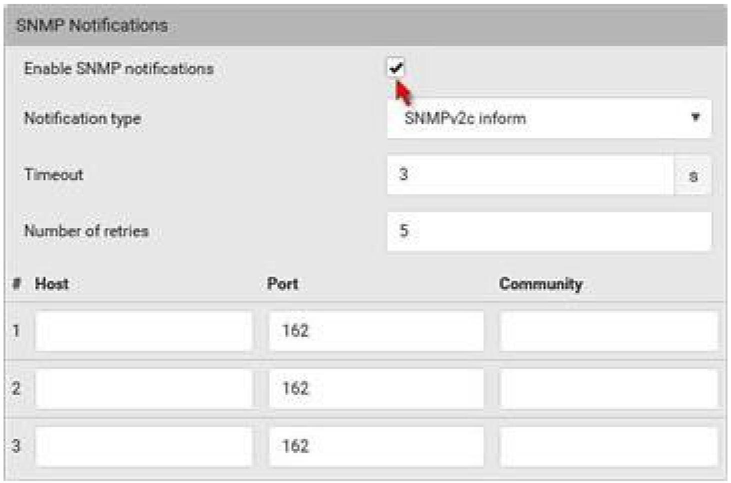
Field	**Description**
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent.
Port	The port number used to access the device(s).
User ID	User name for accessing the device. • Make sure the user has the SNMP v3 access permission.
Timeout	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.
Number of retries	Specify the number of times you want to resend the inform communication if it fails. • For example, inform communications are resent up to 5 times when the initial communication fails.

Field	Description
Security level	Three types are available. • noAuthNoPriv - neither authentication nor privacy protocols are needed. • authNoPriv - only authentication is required. • authPriv - both authentication and privacy protocols are required.
Authentication protocol, Authentication passphrase, Confirm authentication passphrase	The three fields are available when the security level is set to AuthNoPriv or authPriv. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase
Privacy protocol, Privacy passphrase, Confirm privacy passphrase	The three fields are available when the security level is set to authPriv. • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

1) 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.



SNMP Notifications

Enable SNMP notifications ☑

Notification type: SNMPv2c inform ▾

Timeout: 3 s

Number of retries: 5

#	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. • For example, resend a new inform communication once every 3 seconds.
Number of retries	The number of times you want to resend the inform communication if it fails. • For example, inform communications are resent up to 5 times when the initial communication fails.
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 NX1 PDU and all SNMP management stations.

1) Click Save.

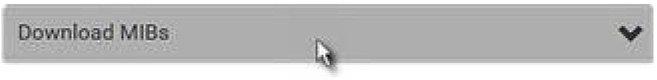
Downloading SNMP MIB

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 NX1 PDU.

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 NX1 PDU 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 NX1 PDU is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the NX1 PDU, 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 NX1 PDU device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The NX1 PDU does NOT support configuring IPv6-related parameters using the SNMP set requests.

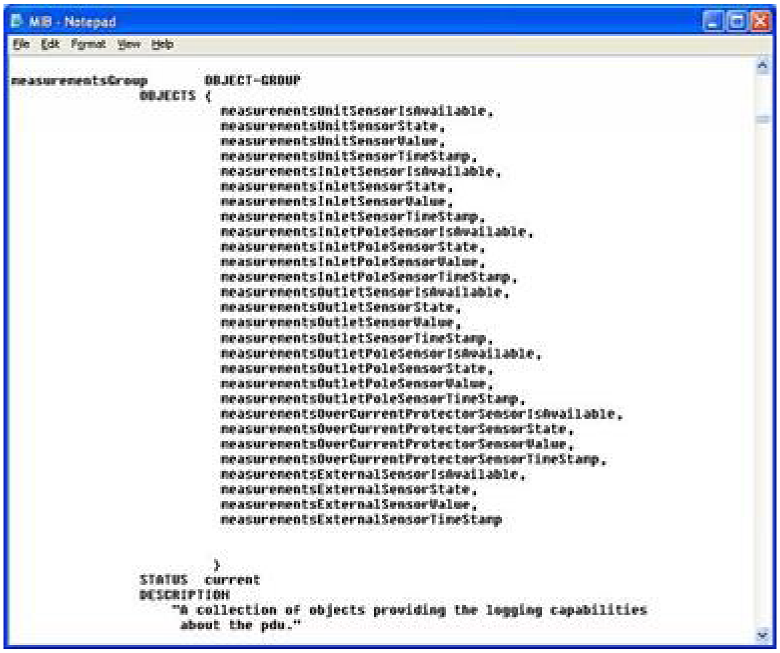
Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom NX1 PDU MIB.

The MIB File

An SNMP MIB file describes the SNMP functions.

Opening the MIB reveals the custom objects that describe the NX1 PDU 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.



```
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 NX1 PDU 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 NX1 PDU 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 NX1 PDU.

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

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 NX1 PDU. 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 NX1 PDU 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.

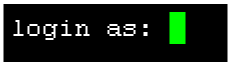
With SSH or Telnet

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.

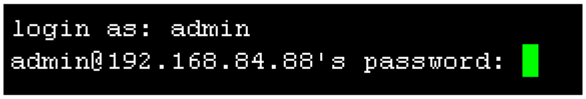


```
login as:
```

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 NX1 PDU 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.

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 NX1 PDU, the > prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the NX1 PDU, 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 NX1 PDU device and network configurations. See Configuring the Device and Network
- 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 .

Closing a Local Connection

Close the window or terminal emulation program when you finish accessing the NX1 PDU over the local connection.

When accessing or upgrading multiple NX1 PDU 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 NX1 PDU 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.

Network Configuration

This command shows all network configuration and all network interfaces' information, such as the IP address, MAC address and the Ethernet interfaces' duplex mode.

```
#       show network
```

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* or *BRIDGE*. Note that you must choose/configure the bridge interface if your NX1 PDU 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 does NOT function.

Interface	Description
eth1	Show the IP-related configuration of the ETH1 interface.
bridge	Show the IP-related configuration of the BRIDGE interface.
all	Show the IP-related configuration of all interfaces. Tip: You can also type the command without adding this option "all" to get the same data. That is, *show network ip interface*.

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* or *BRIDGE*. Note that you must choose/configure the bridge interface if your NX1 PDU 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 does NOT function.

Interface	**Description**
eth1	Show the IPv4 or IPv6 configuration of the ETH1 interface.
bridge	Show the IPv4 or IPv6 configuration of the BRIDGE interface.
all	Show the IPv4 or IPv6 configuration of all interfaces. Tip: You can also type the command without adding this option "all" to get the same data. That is, *show network ipv4 interface*.

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.

```
#   show network interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1* or *BRIDGE*. Note that you must choose/configure the bridge interface if your NX1 PDU 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 does NOT function.

Interface	**Description**
eth1	Show the ETH1 interface's non-IP settings.
bridge	Show the BRIDGE interface's non-IP settings.

all	Show the non-IP settings of all interfaces. Tip: You can also type the command without adding this option "all" to get the same data. That is, *show network interface*.

Network Service Settings

This command shows the network service settings only, including the TCP ports for HTTPS and Modbus/TCP services, and SNMP settings.

```
#  show network services <option>
```

Variables:

- <option> is one of the options: *all*, *https*, *snmp*, *modbus* and *zeroconfig*.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP. Tip: You can also type the command without adding this option "all" to get the same data.
https	Only displays the TCP port for the HTTPS 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.

Device Configuration

This command shows the device configuration, such as the device name, firmware version and model type.

```
#     show pdu
```

To show detailed information, add the parameter "details" to the end of the command.

```
#    show  pdu details
```

Note: Your product may not support all commands.

Outlet Information

This command syntax shows the outlet information.

```
#     show outlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#    show outlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all outlets. Tip: You can also type the command without adding this option "all" to get the same data.
A specific outlet number	Displays the information for the specified outlet only.

Displayed information:

- Without the parameter "details," only the outlet name and state are displayed.
- With the parameter "details," more outlet information is displayed in addition to the state, such as rated current, voltage, active power, active energy, and outlet settings.

Outlet Group Information

This command syntax shows the outlet group information.

```
#    show outletgroups <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#   show outletgroups <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all outlet groups. Tip: You can also type the command without adding this option "all" to get the same data.
A specific outlet group number	Displays the information for the specified outlet group only.

Displayed information:

- Without the parameter "details," only the group's name, the group's index number, member outlets and the group's power state (if it is a switched PDU) are displayed.
- With the parameter "details," more inlet information is displayed in addition to the above outlet group information, such as each member outlet's power state and the group's active energy.

Tip: NX1 PDU allows you to assign the same name to diverse outlet groups. If this really occurs, you still can identify different groups through their unique index numbers.

Inlet Information

This command syntax shows the inlet information.

```
#     show inlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#    show inlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all inlets. Tip: You can also type the command without adding this option "all" to get the same data.
A specific inlet number	Displays the information for the specified inlet only. An inlet number needs to be specified only when there are more than 1 inlet on your PDU.

Displayed information:

- Without the parameter "details," only the inlet's name and RMS current are displayed.
- With the parameter "details," more inlet information is displayed in addition to the inlet name and RMS current, such as the inlet's RMS voltage, active power and active energy.

Overcurrent Protector Information

This command is only available for models with overcurrent protectors for protecting outlets.

This command syntax shows the overcurrent protector information, such as a circuit breaker or a fuse.

```
#       show ocp <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#    show ocp <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all overcurrent protectors. Tip: You can also type the command without adding this option "all" to get the same data.

Option	Description
A specific overcurrent protector number	Displays the information for the specified overcurrent protector only.

Displayed information:

- Without the parameter "details," only the overcurrent protector status and name are displayed.
- With the parameter "details," more overcurrent protector information is displayed in addition to status, such as the rating and RMS current value.

Date and Time Settings

This command shows the current date and time settings on the NX1 PDU.

```
#        show time
```

To show detailed information, add the parameter "details" to the end of the command.

```
#     show time details
```

Default Measurement Units

This command shows the default measurement units applied to the NX1 PDU 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 for the preferred measurement units for a specific user.

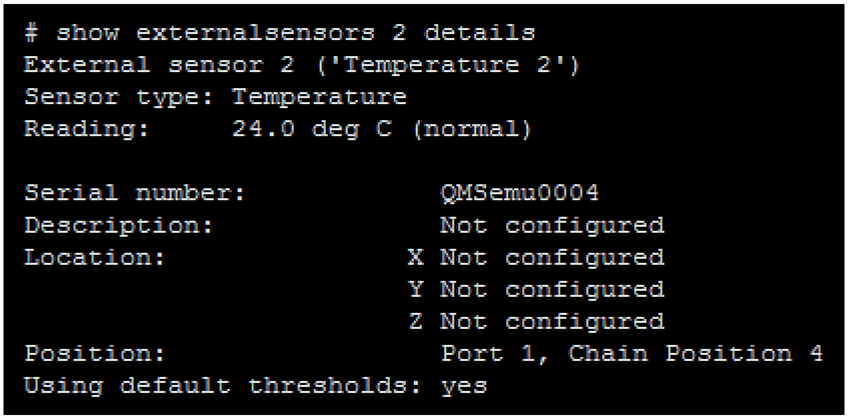
Environmental Sensor Information

This command syntax shows the environmental sensor's information.

```
#   show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#   show externalsensors <n> details
```



```
# 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. Tip: You can also type the command without adding this option "all" to get the same data.
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 NX1 PDU 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 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.

```
#   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
```

Inlet Sensor Threshold Information

This command syntax shows the specified inlet sensor's threshold-related information.

```
#  show sensor inlet <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show sensor inlet <n> <sensor type> details
```

Variables:

- <n> is the number of the inlet whose sensors you want to query. For a single-inlet PDU, <n> is always 1.
- <sensor type> is one of the following sensor types:

Sensor type	**Description**
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor
lineFrequency	Line frequency sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified inlet sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

Inlet Pole Sensor Threshold Information

This command is only available for a three-phase PDU.

This command syntax shows the specified inlet pole sensor's threshold-related information.

```
# show sensor inletpole <n> <p> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show sensor inletpole <n> <p> <sensor type> details
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to query. For a single-inlet PDU, <n> is always 1.
- <p> is the label of the inlet pole whose sensors you want to query.

Pole	**Label <p>**	**Current sensor**	**Voltage sensor**
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	**Description**
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified inlet pole sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.
- If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

Overcurrent Protector Sensor Threshold Information

This command is only available for models with overcurrent protectors for protecting outlets.

This command syntax shows the specified overcurrent protector sensor's threshold-related information.

```
#  show sensor ocp <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show sensor ocp <n> <sensor type> details
```

Variables:

- <n> is the number of the overcurrent protector whose sensors you want to query.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified overcurrent protector sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

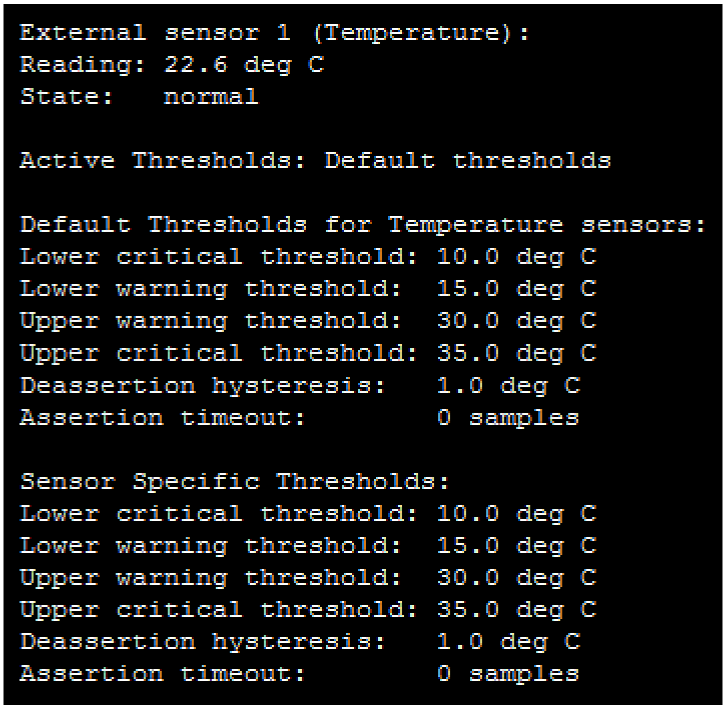
Environmental Sensor Threshold Information

This command syntax shows the specified environmental sensor's threshold-related information.

```
#  show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show sensor externalsensor <n> details
```



```
External sensor 1 (Temperature):
Reading: 22.6 deg C
State:   normal

Active Thresholds: Default thresholds

Default Thresholds for Temperature sensors:
Lower critical threshold: 10.0 deg C
Lower warning threshold:  15.0 deg C
Upper warning threshold:  30.0 deg C
Upper critical threshold: 35.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:        0 samples

Sensor Specific Thresholds:
Lower critical threshold: 10.0 deg C
Lower warning threshold:  15.0 deg C
Upper warning threshold:  30.0 deg C
Upper critical threshold: 35.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:        0 samples
```

Variables:

- <n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripherals page of the NX1 PDU web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

Note: For a state sensor, the threshold-related and accuracy-related data is NOT available.

Environmental Sensor Default Thresholds

This command syntax shows a certain sensor type's default thresholds, which are the initial thresholds applying to the specified type of sensor.

```
#  show defaultThresholds <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
# show defaultThresholds <sensor type> details
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors
all	All of the above numeric sensors Tip: You can also type the command without adding this option "all" to get the same data.

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.

Security Settings

This command shows the security settings of the NX1 PDU.

```
#     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).

Authentication Settings

► *General authentication settings:*

This command displays the authentication settings of the NX1 PDU, including both LDAP and Radius settings.

```
#    show authentication
```

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. Tip: You can also type the command without adding this option "all" to get the same data.
a specific user's name	This option shows the profile of the specified user only.

Displayed information:

- Without the parameter "details," only four pieces of user information are displayed: user name, user "Enabled" status, SNMP v3 access privilege, and role(s).
- With the parameter "details," more user information is displayed, such as the telephone number, e-mail address, preferred measurement units and so on.

Existing Roles

This command shows the data of one or all existing roles.

```
#    show roles <role_name>
```

Variables:

- <role_name> is the name of the role whose permissions you want to query. The variable can be one of the following options:

Option	Description
all	This option shows all existing roles. Tip: You can also type the command without adding this option "all" to get the same data.
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.

Load Shedding Settings

This section applies to outlet-switching capable models only.

This command shows the load shedding settings.

```
#     show loadshedding
```

Displayed information:

- The load shedding state is displayed along with non-critical outlets.

Note: The load shedding mode is associated with critical and non-critical outlets. To specify critical and non-critical outlets through CLI, see Specifying Non-Critical Outlets .

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.
- <device-name> is pdu.

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.
<device-name>	Displays <device-name>-related events.
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.
modem	Modem-related events.
timerEvent	Scheduled action events.
cardReader	Events for card reader management, if available.

Network Connections Diagnostic Log

This command shows the diagnostic log for the EAP authentication.

```
#    show network diagLog
```

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.

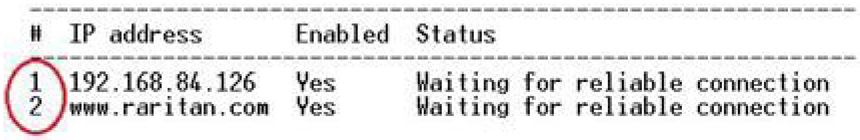
```
#   show serverReachability server <n>
```

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.

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
```

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.

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. Tip: You can also type the command without adding this option "0" to get all data.
A specific integer number	Displays the specified number of last entries in the reliability error log.

Reliability Hardware Failures

This command shows a list of detected hardware failures.

```
#   show reliability hwfailures
```

For details, see Hardware Issue Detection.

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 <device-name>. You can use the <device-name> configuration commands to change the settings that apply to the whole device. You must insert your specific <device-name> as shown.

- SRC <device-name>: src.
- All PDUs and Transfer Switches <device-name>: pdu.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Changing the Device Name

```
config:#      <device-name> 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.

You must insert your specific <device-name> as shown: Device Configuration Commands

Setting the Outlet Relay Behavior

This section applies to outlet-switching capable models only.

This command syntax determines the relay behavior of all outlets on a NX1 PDU model.

```
config:#  pdu relayBehaviorOnPowerLoss <option>
```

Variables:

- <option> is one of the options: *latching* or *nonLatching*

Setting the Outlet Power-On Sequence

This section applies to outlet-switching capable models only.

This command sets the outlet power-on sequence when the PDU powers up.

```
config:#     pdu outletSequence <option>
```

Variables:

- <option> is one of the options: *default*, or a comma-separated list of outlet numbers.

Option	Description
default	All outlets are switched ON in the ASCENDING order (from outlet 1 to the final outlet) when the NX1 PDU powers up.
A comma-separated list of outlet numbers	All outlets are switched ON in the order you specify using the comma-separated list. The list must include all outlets on the PDU.

Note: Power-on sequencing is disabled in the latching mode.

Setting the Outlet Power-On Sequence Delay

This section applies to outlet-switching capable models only.

This command sets the delays (in seconds) for outlets when turning on all outlets in sequence.

```
config:# pdu outletSequenceDelay <outlet1>:<delay1>;<outlet2>:<delay2>;
         <outlet3>:<delay3>;...
```

Separate outlet numbers and their delay settings with a colon. Outlets followed by delays are separated with a semicolon.

Variables:

- <outlet1>, <outlet2>, <outlet3> and the like are individual outlet numbers or a range of outlets using a dash. For example, *3-8* represents outlets 3 to 8.
- <delay1>, <delay2>, <delay3> and the like are the delay time in seconds.

Note: Power-on sequencing is disabled in the latching mode.

Setting the PDU-Defined Default Outlet State

This section applies to outlet-switching capable models only.

This command determines the initial power condition of all outlets after powering up the PDU. This setting is used in three scenarios:

- powering up the whole PDU
- powering up a single inlet in a multi-inlet PDU (on most, but not all, multi-inlet units the outlet boards are powered through the respective inlet)
- transfer switch switches on again after being off due to e.g. internal failure

```
config:#    pdu outletStateOnPowerUp <option>
```

Variables:

- <option> is one of the options: *off*, *on* or *lastKnownState*.

Option	**Description**
off	Switches OFF all outlets when the NX1 PDU powers up.
on	Switches ON all outlets when the NX1 PDU powers up.
lastKnownState	Restores all outlets to the previous status before powering down the NX1 PDU when the PDU powers up again.

Note: This feature does NOT take effect and cannot be configured on a NX1 PDU device after the outlet relay is set to the "Latching" mode.

Setting the PDU-Defined Cycling Power-Off Period

This section applies to outlet-switching capable models only.

This command sets the power-off period of the power cycling operation for all outlets.

```
config:#    pdu cyclingPowerOffPeriod <timing>
```

Variables:

- <timing> is the time of the cycling power-off period in seconds, which is an integer between 0 and 3600, or *pduDefined* for following the PDU-defined timing.

Setting the Inrush Guard Delay Time

This section applies to outlet-switching capable models only.

This command sets the inrush guard delay.

```
config:#     pdu inrushGuardDelay <timing>
```

Variables:

- <timing> is a delay time between 100 and 100000 milliseconds.

Setting the Outlet Initialization Delay

This section applies to outlet-switching capable models only.

This command determines the outlet initialization delay timing on device startup. See PDU for information on outlet initialization delay.

```
config:#    pdu outletInitializationDelayOnPowerUp <timing>
```

Variables:

- <timing> is a delay time between 1 and 3600 seconds.

Note: This feature does NOT take effect and cannot be configured on a NX1 PDU device after the outlet relay is set to the "Latching" mode.

Specifying Non-Critical Outlets

This section applies to outlet-switching capable models only.

This command determines critical and non-critical outlets. It is associated with the load shedding mode. See Load Shedding Mode.

```
config:#  pdu nonCriticalOutlets <outlets1>:false;<outlets2>:true
```

Separate outlet numbers and their settings with a colon. Separate each "false" and "true" setting with a semicolon.

Variables:

- <outlets1> is one or multiple outlet numbers to be set as critical outlets. Use commas to separate outlet numbers.

  Use a dash for a range of consecutive outlets. For example, *3-8* represents outlets 3 to 8.
- <outlets2> is one or multiple outlet numbers to be set as NON-critical outlets. Use commas to separate outlet numbers.

  Use a dash for a range of consecutive outlets. For example, *3-8* represents outlets 3 to 8.

Enabling or Disabling Data Logging

This command enables or disables the data logging feature.

```
config:#   <device-name> dataRetrieval <option>
```

You must insert your specific <device-name> as shown: Device Configuration Commands

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the data logging feature.
disable	Disables the data logging feature.

For more information, see Setting Data Logging.

Setting Data Logging Measurements Per Entry

This command defines the number of measurements accumulated per log entry.

```
config:# <device-name> measurementsPerLogEntry
         <number>
```

You must insert your specific <device-name> as shown: Device Configuration Commands

Variables:

- <number> is an integer between 1 and 600. The default is 60 samples per log entry.

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* or *BRIDGE*. Note that you must choose/configure the bridge interface if your NX1 PDU 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 does NOT function.

Interface	Description
eth1	Determine the IPv4 configuration mode of the ETH1 interface (wired 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.
Mode	**Description**
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* or *BRIDGE*. Note that you must choose/configure the bridge interface if your NX1 PDU 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 does NOT function.

Interface	Description
eth1	Determine the IPv4 preferred host name of the ETH1 interface (that is, wired 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 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the NX1 PDU.

```
config:#  network ipv4 interface <ETH> address <ip address>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1* or *BRIDGE*. Note that you must choose/configure the bridge interface if your NX1 PDU 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 does NOT function.

Interface	Description
eth1	Determine the IPv4 address of the ETH1 interface (that is, wired 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 NX1 PDU. Its format is "IP address/prefix". For example, *192.168.84.99/24*.

Setting the IPv4 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:# network ipv4 interface 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).
bridge	Determine the IPv4 address of the BRIDGE interface (that is, the bridging mode).

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 NX1 PDU 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* and *BRIDGE*. Type "bridge" only when your NX1 PDU 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* or *BRIDGE*. Note that you must choose/configure the bridge interface if your NX1 PDU 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 does NOT function.

Interface	Description
eth1	Determine the IPv6 configuration mode of the ETH1 interface (wired networking).
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 NX1 PDU 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 NX1 PDU 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 NX1 PDU will use SLAAC and use an IPv6 address based on that Prefix and its own MAC address. If the RA has the "otherconf" flag set, the NX1 PDU 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* or *BRIDGE*. Note that you must choose/configure the bridge interface if your NX1 PDU 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 does NOT function.

Interface	Description
eth1	Determine the IPv6 preferred host name of the ETH1 interface (wired networking).
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 NX1 PDU.

```
config:# network ipv6 interface <ETH> address <ip
         address>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1* or *BRIDGE*. Note that you must choose/configure the bridge interface if your NX1 PDU 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 does NOT function.

Interface	Description
eth1	Determine the IPv6 address of the ETH1 interface (wired 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 NX1 PDU. 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 <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. This value uses the IPv6 address format.

Interface	Description
eth1	Determine the IPv4 address of the ETH1 interface (that is, wired networking).

Interface	Description
bridge	Determine the IPv4 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 NX1 PDU 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 NX1 PDU 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* and *BRIDGE*. Type "bridge" only when your NX1 PDU 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 NX1 PDU. For example, <suffix1> can be *Raritan.com*, and <suffix2> can be *Raritan.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 -- *eth1*.

Option	Description
eth1	ETH1 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 -- *eth1*.

Option	Description
eth1	ETH1 port

- <option> is one of the options: *auto*, *10Mbps* or *100Mbps*.

Option	Description
auto	System determines the optimum LAN speed through auto-negotiation.
10Mbps	The LAN speed is always 10 Mbps.
100Mbps	The LAN speed is always 100 Mbps.

Changing the LAN Duplex Mode

This command determines the LAN interface duplex mode.

```
config:#        network ethernet <ETH> duplexMode <mode>
```

Variables:

- <ETH> is -- *eth1*.

Option	Description
eth1	ETH1 port

- <mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	The NX1 PDU selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the NX1 PDU) 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 -- eth1.
- <mtu> is the Maximum Transfer Unit. Enter a value from 1280-1500.

Setting the Ethernet Authentication Method

NX1 PDU 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 -- *eth1*.

Option	**Description**
eth1	ETH1 port

- <method> is one of the authentication methods: *NONE* or *EAP*.

Method	**Description**
NONE	The authentication method is set to NONE.
Method	**Description**
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 NX1 PDU 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.

▶ *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
```

▶ *Eable 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 -- *eth1*.

Option	Description
eth1	ETH1 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 NX1 PDU 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 NX1 PDU 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.

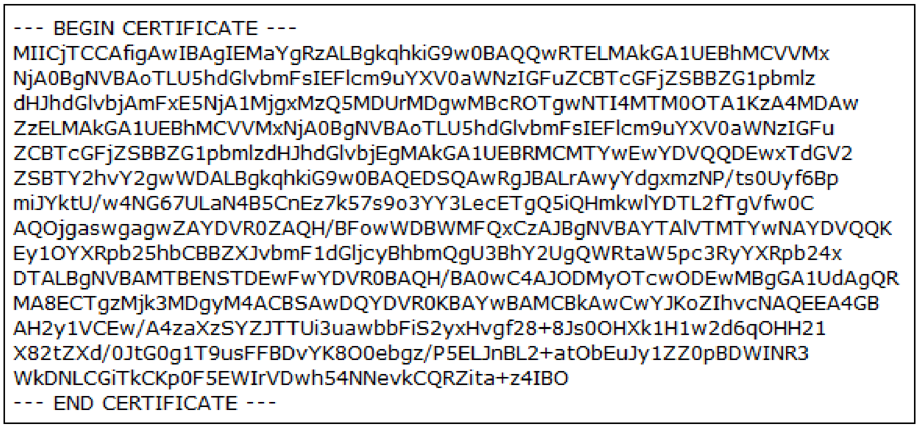
In addition, the procedure of uploading the client certificate and client private key in CLI is similar to the following example, except for the CLI command.

► *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 ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+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:#
```

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	ETH1 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	• The HTTP port is enabled. - OR - • HTTP redirection to HTTPS is enabled.

Option	Description
false	- The HTTP port is disabled. - OR - - HTTP redirection to HTTPS is disabled.

Setting the HTTPS Port

The commands used to configure the HTTPS port settings begin with *network services https*.

► *Change the HTTPS port:*

```
config:#    network services https port <n>
```

► *Enable or disable the HTTPS access:*

```
config:#  network services https enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Forces any access to the NX1 PDU via HTTP to be redirected to HTTPS.
false	No HTTP access is redirected to HTTPS.

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

► *Enabling or Disabling Telnet*

This command enables or disables the Telnet service.

```
config:#  network services telnet enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.
false	The Telnet service is disabled.

► *Changing the Telnet Port*

This command changes the Telnet port.

```
config:#    network services telnet port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

► *Enabling or Disabling SSH*

This command enables or disables the SSH service.

```
config:#   network services ssh enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

► *Changing the SSH Port*

This command changes the SSH port.

```
config:#     network services ssh port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default SSH port is 22.

► *Determining the SSH Authentication Method*

This command syntax determines the SSH authentication method.

```
config:#  network services ssh authentication <auth_method>
```

Variables:

- <option> is one of the options: *passwordOnly*, *publicKeyOnly* or *passwordOrPublicKey*.

Option	**Description**
passwordOnly	Enables the password-based login only.
publicKeyOnly	Enables the public key-based login only.
passwordOrPublicKey	Enables both the password- and public key-based login. This is the default.

If the public key authentication is selected, you must 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.

Option	Description
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 *2015-11-30* for November 30, 2015.
<hh:mm:ss>	Type the time in the format of hh:mm:ss in the 24-hour format. For example, type *13:50:20* for 1:50:20 pm.

Setting the Time Zone

The CLI has a list of time zones to configure the date and time for NX1 PDU.

```
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 NX1 PDU 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.

Option	Description
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: *new rule's number = the specified rule number*
insertBelow	Inserts the new rule below the specified rule number. Then: *new rule's number = the specified rule number + 1*

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Modifying a Firewall Rule

Depending on what to modify in an existing rule, the command varies.

- *IPv4 commands*

► *Modify an IPv4 rule's IP address and/or subnet mask:*

```
config:# security ipAccessControl ipv4 rule modify <direction>
         <rule_number> ipMask <ip_mask>
```

► *Modify an IPv4 rule's policy:*

```
config:# security ipAccessControl ipv4 rule modify <direction>
         <rule_number> policy <policy>
```

► *Modify all contents of an existing IPv4 rule:*

```
config:# security ipAccessControl ipv4 rule modify <direction>
         <rule_number> ipMask <ip_mask> policy <policy>
```

- *IPv6 commands*

► *Modify an IPv6 rule's IP address and/or prefix length:*

```
config:# security ipAccessControl ipv6 rule modify <direction>
         <rule_number> ipMask <ip_mask>
```

► *Modify an IPv6 rule's policy:*

```
config:# security ipAccessControl ipv6 rule modify <direction>
         <rule_number> policy <policy>
```

► *Modify all contents of an IPv6 existing rule:*

```
config:# security ipAccessControl ipv6 rule modify <direction>
         <rule_number> ipMask <ip_mask> policy <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to modify.
- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

► *IPv4 commands*

```
config:# security ipAccessControl ipv4 rule delete <direction>
         <rule_number>
```

► *IPv6 commands*

```
config:# security ipAccessControl ipv6 rule delete <direction>
         <rule_number>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.

Direction	Description
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.

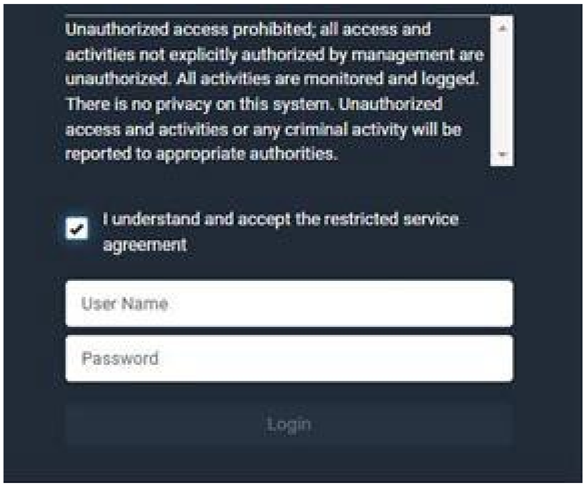
```
config:#  security restrictedServiceAgreement enabled <option>
```

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.



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.

☑ I understand and accept the restricted service agreement

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.
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 NX1 PDU 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.

Option	Description
false	Disables the strong password feature.

Minimum Password Length

This command determines the minimum length of the password.

```
config:#  security strongPasswords minimumLength <value>
```

Variables:

- <value> is an integer between 8 and 32.

Maximum Password Length

This command determines the maximum length of the password.

```
config:#  security strongPasswords maximumLength <value>
```

Variables:

- <value> is an integer between 16 and 64.

Lowercase Character Requirement

This command determines whether a strong password includes at least a lowercase character.

```
config:# security strongPasswords enforceAtLeastOneLowerCaseCharacter
         <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.
disable	No lowercase character is required.

Uppercase Character Requirement

This command determines whether a strong password includes at least a uppercase character.

```
config:# security strongPasswords enforceAtLeastOneUpperCaseCharacter
         <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one uppercase character is required.
disable	No uppercase character is required.

Numeric Character Requirement

This command determines whether a strong password includes at least a numeric character.

```
config:# security strongPasswords enforceAtLeastOneNumericCharacter
         <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one numeric character is required.
disable	No numeric character is required.

Special Character Requirement

This command determines whether a strong password includes at least a special character.

```
config:# security strongPasswords enforceAtLeastOneSpecialCharacter
         <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one special character is required.
disable	No special character is required.

Maximum Password History

This command determines the number of previous passwords that CANNOT be repeated when changing the password.

```
config:#   security strongPasswords passwordHistoryDepth <value>
```

Variables:

- <value> is an integer between 1 and 12.

Role-Based Access Control

In addition to firewall access control based on IP addresses, you can configure other access control rules that are based on both IP addresses and users' roles.

- An IPv4 role-based access control command begins with *security roleBasedAccessControl ipv4*.
- An IPv6 role-based access control command begins with *security roleBasedAccessControl ipv6*.

Modifying Role-Based Access Control Parameters

There are different commands for modifying role-based access control parameters.

- *IPv4 commands*

▶ *Enable or disable the IPv4 role-based access control feature:*

```
config:#  security roleBasedAccessControl ipv4 enabled <option>
```

▶ *Determine the IPv4 role-based access control policy:*

```
config:#  security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- *IPv6 commands*

▶ *Enable or disable the IPv6 role-based access control feature:*

```
config:#  security roleBasedAccessControl ipv6 enabled <option>
```

▶ *Determine the IPv6 role-based access control policy:*

```
config:#  security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the role-based access control feature.
false	Disables the role-based access control feature.

- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from all IP addresses regardless of the user's role.
deny	Drops traffic from all IP addresses regardless of the user's role.

Tip: You can combine both commands to modify all role-based access control parameters at a time.

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: *new rule's number = the specified rule number*
insertBelow	Inserts the new rule below the specified rule number. Then: *new rule's number = the specified rule number + 1*

- <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 NX1 PDU 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`

Tip: If your NX1 PDU 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
```

Outlet Configuration Commands

An outlet configuration command begins with *outlet*. Such a command allows you to configure an individual outlet.

Changing the Outlet Name

This command names an outlet.

```
config:#       outlet <n> name "<name>"
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Changing an Outlet's Default State

This section applies to outlet-switching capable models only.

This command determines the initial power condition of an outlet after the NX1 PDU powers up.

```
config:#     outlet <n> stateOnPowerUp <option>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <option> is one of the options: *off*, *on, lastKnownState* and *pduDefined.*

Option	**Description**
off	Turn off the outlet.
on	Turn on the outlet.
lastKnownState	Restore the outlet to the state prior to last PDU power down.
pduDefined	PDU-defined setting.

Note: Setting the outlet's default state to an option other than *pduDefined* overrides the PDU-defined default state on that outlet.

Setting an Outlet's Cycling Power-Off Period

This section applies to outlet-switching capable models only.

This command determines the power-off period of the power cycling operation for a specific outlet.

```
config:#   outlet <n> cyclingPowerOffPeriod <timing>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <timing> is the time of the cycling power-off period in seconds, which is an integer between 0 and 3600, or *pduDefined* for following the PDU-defined timing.

Note: This setting overrides the PDU-defined cycling power-off period on a particular outlet.

Example - Outlet Naming

The following command assigns the name "Win XP" to outlet 8.

```
config:#        outlet 8 name "Win XP"
```

Outlet Group Configuration Commands

An outlet group configuration command begins with *outletgroup*. Such a command allows you to configure or operate an outlet group.

Creating an Outlet Group

This command creates a new outlet group.

```
config:#   outletgroup add "<name>" <members>
```

Variables:

- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

  Tip: NX1 PDU allows you to assign the same name to diverse outlet groups. If this really occurs, you still can identify different groups through their unique index numbers.

- <members> is one or multiple member outlets' index numbers separated with commas. If the member outlets are consecutive outlets, you can type a hyphen between the initial and the final index number instead of using commas.

  For example, to assign outlets 3, 4, 5, 8 and 10 to the outlet group named "servers", you have two choices -- either use a hyphen for consecutive outlets 3 to 5, or use commas for all of member outlets:

  - `outletgroup add servers 3-5,8,10`

-- OR --

- `outletgroup add servers 3,4,5,8,10`

Managing an Outlet Group

You can modify an outlet group's name and member outlets, or simply remove any existing outlet group.

You can modify both the name and members of an outlet group at a time by combining multiple commands.

► *Modify an outlet group's name:*

```
config:#       outletgroup modify <ID> name "<name>"
```

► *Modify an outlet group's member outlets:*

```
config:#      outletgroup modify <ID> members <members>
```

► *Delete an outlet group:*

```
config:#             outletgroup delete <ID>
```

Variables:

- <ID> is an outlet group's index number.
- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.
- <members> is one or multiple member outlets' index numbers separated with commas. If the member outlets are consecutive outlets, you can type a hyphen between the initial and the final index number instead of using commas.

  For example, to assign outlets 3, 4, 5, 8 and 10 to the outlet group named "servers", you have two choices -- either use a hyphen for consecutive outlets 3 to 5, or use commas for all of member outlets:

  In the following examples, it is assumed that the "servers" outlet group's index number is 2.

  - `outletgroup modify 2 members 3-5,8,10`

    -- OR --

  - `outletgroup modify 2 members 3,4,5,8,10`

Powering On/Off/Cycle Outlet Groups

This section applies to outlet-switching capable models only.

You must perform this operation in the *administrator mode*.

► *Power on one outlet group:*

```
#   power outletgroup <ID> on
```

► *Power off one outlet group:*

```
#   power outletgroup <ID> off
```

► *Power cycle one outlet group:*

```
#   power outletgroup <ID> cycle
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

For example:

```
#   power outletgroup <ID> off /y
```

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

Variables:

- <ID> is an outlet group's index number.

Inlet Configuration Commands

An inlet configuration command begins with *inlet*. You can configure an inlet by using the inlet configuration command.

Changing the Inlet Name

This command syntax names an inlet.

```
config:#       inlet <n> name "<name>"
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always 1. The value is an integer between 1 and 50.
- <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 an Inlet (for Multi-Inlet PDUs)

Enabling or disabling an inlet takes effect on a multi-inlet PDU only.

This command enables or disables an inlet.

```
config:#      inlet <n> enabled <option>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always 1. The value is an integer between 1 and 50.
- <option> is one of the options: *true* or *false*.

Option	**Description**
true	The specified inlet is enabled.
false	The specified inlet is disabled.

Note: If performing this command causes all inlets to be disabled, a warning message appears, prompting you to confirm. When this occurs, press y to confirm or n to cancel the operation.

Example - Inlet Naming

The following command assigns the name "AC source" to the inlet 1. If your NX1 PDU contains multiple inlets, this command names the 1st inlet.

```
config:#      inlet 1 name "AC source"
```

Overcurrent Protector Configuration Commands

An overcurrent protector configuration command begins with *ocp.* The command configures an individual circuit breaker or fuse which protects outlets.

Changing the Overcurrent Protector Name

This command names a circuit breaker or a fuse which protects outlets on your NX1 PDU.

```
config:#        ocp <n> name "<name>"
```

Variables:

- <n> is the number of the overcurrent protector that you want to configure. The value is an integer between 1 and 50.
- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example - OCP Naming

The command assigns the name "Email servers CB" to the overcurrent protector labeled 2.

```
config:#     ocp 2 name "Email servers CB"
```

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 NX1 PDU prompts you to assign a password to the newly-created user. Then:

1) Type the password and press Enter.
2) Re-type the same password for confirmation and press Enter.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable CANNOT contain spaces.
- <option> is one of the options: *enable* or *disable*.

Option	**Description**
enable	Enables the newly-created user profile.
disable	Disables the newly-created user profile.

- <roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Modifying a User Profile

A user profile contains various parameters that you can modify.

Tip: You can combine all commands to modify the parameters of a specific user profile at a time.

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 NX1 PDU 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.

Option	Description
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 NX1 PDU 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 options: *MD5* or *SHA-1*.

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.

- <option6> is one of the options: *DES* or *AES-128*.

Option	Description
DES	DES privacy protocol is applied.
AES-128	AES-128 privacy protocol is applied.

- 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
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
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
Privilege	**Description**

** 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*.
- <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*.

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 option: *local*

Option	Description
local	Enable Local 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.

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.

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 NX1 PDU 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.
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 NX1 PDU 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 NX1 PDU 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 NX1 PDU 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.

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
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
```

Sensor Threshold Configuration Commands

A sensor configuration command begins with *sensor*. You can use the commands to configure the threshold, hysteresis and assertion timeout values for any sensor associated with the following items:

- Outlets
- Outlet groups
- Inlets
- Inlet poles (for three-phase PDUs only)
- Overcurrent protectors
- Environmental sensors

It is permitted to assign a new value to the threshold at any time regardless of whether the threshold has been enabled.

Note: Your product may not support all commands.

Commands for Inlet Sensors

A sensor configuration command for inlets begins with *sensor inlet*.

You can configure various inlet sensor threshold settings at a time by combining multiple commands.

► *Set the Upper Critical threshold for an inlet sensor:*

```
config:#  sensor inlet <n> <sensor type> upperCritical <option>
```

► *Set the Upper Warning threshold for an inlet sensor:*

```
config:#  sensor inlet <n> <sensor type> upperWarning <option>
```

► *Set the Lower Critical threshold for an inlet sensor:*

```
config:#  sensor inlet <n> <sensor type> lowerCritical <option>
```

► *Set the Lower Warning threshold for an inlet sensor:*

```
config:#  sensor inlet <n> <sensor type> lowerWarning <option>
```

► *Set the deassertion hysteresis for an inlet sensor:*

```
config:#  sensor inlet <n> <sensor type> hysteresis <hy_value>
```

► *Set the assertion timeout for an inlet sensor:*

```
config:#  sensor inlet <n> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor

powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor
lineFrequency	Line frequency sensor

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	**Description**
enable	Enables the specified threshold for a specific inlet sensor.
disable	Disables the specified threshold for a specific inlet sensor.
A numeric value	Sets a value for the specified threshold of a specific inlet sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified inlet sensor.
- <as_value> is a numeric value that is assigned to the assertion timeout for the specified inlet sensor.

Commands for Inlet Pole Sensors

A sensor configuration command for inlet poles begins with *sensor inletpole*. This type of command is available on a three-phase PDU only.

You can configure various inlet pole sensor threshold settings at a time by combining multiple commands.

► *Set the Upper Critical Threshold for an Inlet Pole:*

```
config:#  sensor inletpole <n> <p> <sensor type> upperCritical <option>
```

► *Set the Upper Warning Threshold for an Inlet Pole:*

```
config:#  sensor inletpole <n> <p> <sensor type> upperWarning <option>
```

► *Set the Lower Critical Threshold for an Inlet Pole:*

```
config:#  sensor inletpole <n> <p> <sensor type> lowerCritical <option>
```

► *Set the Lower Warning Threshold for an Inlet Pole:*

```
config:#  sensor inletpole <n> <p> <sensor type> lowerWarning <option>
```

► *Set the Inlet Pole's Deassertion Hysteresis:*

```
config:#  sensor inletpole <n> <p> <sensor type> hysteresis <hy_value>
```

► *Set the Inlet Pole's Assertion Timeout:*

```
config:# sensor inletpole <n> <p> <sensor type> assertionTimeout
         <as_value>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure. For a single-inlet PDU, <n> is always 1.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentEnergy	Apparent Energy sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
L-L Voltage	Voltage is measured per line

Note: If the requested sensor type is not supported, the "Sensor is not available" message is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the specified threshold for the specified inlet pole sensor.
disable	Disables the specified threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the specified threshold of the specified inlet pole sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified inlet pole sensor.
- <as_value> is a number in samples that is assigned to the assertion timeout for the specified inlet pole sensor.

Commands for Overcurrent Protector Sensors

A sensor configuration command for overcurrent protectors begins with *sensor ocp*.

You can configure various overcurrent protector threshold settings at a time by combining multiple commands.

► *Set the Upper Critical threshold for an overcurrent protector:*

```
config:#  sensor ocp <n> <sensor type> upperCritical <option>
```

► *Set the Upper Warning threshold for an overcurrent protector:*

```
config:#  sensor ocp <n> <sensor type> upperWarning <option>
```

► *Set the Lower Critical threshold for an overcurrent protector:*

```
config:#  sensor ocp <n> <sensor type> lowerCritical <option>
```

► *Set the Lower Warning threshold for an overcurrent protector:*

```
config:#  sensor ocp <n> <sensor type> lowerWarning <option>
```

► *Set the deassertion hysteresis for an overcurrent protector:*

```
config:#  sensor ocp <n> <sensor type> hysteresis <hy_value>
```

► *Set the assertion timeout for an overcurrent protector:*

```
config:#  sensor ocp <n> <sensor type> assertionTimeout <as_value>
```

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.

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 NX1 PDU 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 NX1 PDU 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

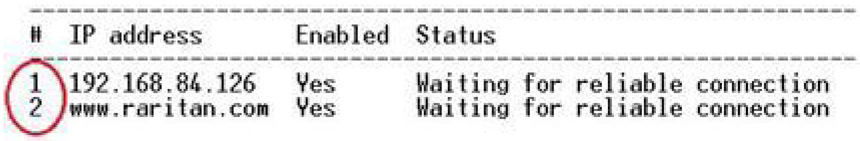
This command removes a monitored IT device from the server reachability list.

```
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 pinging after declaring "Unreachable":*

```
config:# serverReachability modify <n> waitTimeBeforeResumingPinging
         <resume>
```

► *Modify the number of consecutive "Unreachable" declarations before disabling the ping monitoring feature:*

```
config:# serverReachability modify <n> numberOfFailuresToDisable
         <disable_count>
```

Variables:

- <n> is a number representing the sequence of the IT device in the server monitoring list.
- <IP_host> is the IP address or host name of the IT device whose settings you want to modify.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the monitored device.
false	Disables the ping monitoring feature for the monitored device.

- <succ_number> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.
- <fail_number> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.
- <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
- <fail_wait> is the wait time to send the next ping after 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
externalSensorsZCoordinateFormat	Keyword	Z coordinate refers to the height of sensors.
rackUnits / freeForm	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.
deviceAltitude	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.
number1	Enter an integer number from -425 up to 3000 when using Meters.	Negative numbers indicate altitude below sea level.
peripheralDeviceAutoManagement	Keyword	Enable or disable the automatic management feature for sensors.

enable / disable	Enter one of these values	
activePoweredDryContactLimit	Keyword	You need either 'Change Peripheral Device Configuration' privilege or 'Administrator Privileges'.
number2	Enter an integer number from 0 - 24.	An "active" actuator is turned ON, or, if with a door handle connected, is OPENED.
muteOtherDoorHandle	Keyword	
enable / disable	Enter one of these values	

► *Examples:*

```
config:# peripheralDevicesSetup

externalSensorsZCoordinateFormat freeForm

deviceAltitude 3

peripheralDeviceAutoManagement enable

activePoweredDryContactLimit 2

muteOtherDoorHandle disable
```

Load Shedding Configuration Commands

This section applies to outlet-switching capable models only.

A load shedding configuration command begins with *loadshedding*.

Unlike other CLI configuration commands, the load shedding configuration command is performed in the *administrator mode* rather than the configuration mode.

Enabling or Disabling Load Shedding

This section applies to outlet-switching capable models only.

This command determines whether to enter or exit from the load shedding mode.

```
#    loadshedding <option>
```

After performing the above command, NX1 PDU prompts you to confirm the operation. Press `y` to confirm or `n` to abort the operation.

To skip the confirmation step, you can add the "/y" parameter to the end of the command so that the operation is executed immediately.

```
#   loadshedding <option> /y
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
start	Enter the load shedding mode.
stop	Quit the load shedding mode.

► *Example*

The following command has the NX1 PDU enter the load shedding mode.

```
config:#          loadshedding start
```

Power Control Operations

This section applies to outlet-switching capable models only.

Outlets can be turned on or off, or power cycled through the CLI.

You can also cancel the power-on process while the system is powering on ALL outlets.
You must perform this operation in the *administrator mode*.

Turning On the Outlet(s)

This section applies to outlet-switching capable models only.

This command turns on one or multiple outlets.

```
 #   power outlets <numbers> on
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
 #   power outlets <numbers> on /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Switches ON all outlets.
A specific outlet number	Switches ON the specified outlet.
A comma- separated list of outlets	Switches ON multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type: `outlets 2,4,9,11-13,15`.
A range of outlets with a hyphen in between	Switches ON multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type: `outlets 3-8`.

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

If you have configured outlet switching sequence and/or delay, NX1 PDU will prompt you with one more question:

```
Should outlet sequence order and delays be used during switching?
```

- Type `y` to apply the current outlet sequence and delay settings when switching on outlets. See Setting Outlet Power-On Sequence and Delay.
- Type `n` to apply the default sequence and delays.

Turning Off the Outlet(s)

This section applies to outlet-switching capable models only.

This command turns off one or multiple outlets.

```
#   power outlets <numbers> off
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#   power outlets <numbers> off /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	**Description**
all	Switches OFF all outlets.
A specific outlet number	Switches OFF the specified outlet.
A comma- separated list of outlets	Switches OFF multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type: `outlets 2,4,9,11-13,15`.

Option	Description
A range of outlets with a hyphen in between	Switches OFF multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type: `outlets 3-8`.

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

Power Cycling the Outlet(s)

This section applies to outlet-switching capable models only.

This command power cycles one or multiple outlets.

```
#  power outlets <numbers> cycle
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#  power outlets <numbers> cycle /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Power cycles all outlets.
A specific outlet number	Power cycles the specified outlet.
A comma- separated list of outlets	Power cycles multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type: `outlets 2,4,9,11-13,15`.

Option	Description
A range of outlets with a hyphen in between	Power cycles multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type: `outlets 3-8`.

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

If you have configured outlet switching sequence and/or delay, NX1 PDU will prompt you with one more question:

```
Should outlet sequence order and delays be used during switching?
```

- Type `y` to apply the current outlet sequence and delay settings when switching on outlets. See Setting Outlet Power-On Sequence and Delay.
- Type `n` to apply the default sequence and delays.

Canceling the Power-On Process

This section applies to outlet-switching capable models only.

After issuing the command to power on ALL outlets, you can use the following command to stop the power-on process.

```
#    power cancelSequence
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#   power cancelSequence /y
```

Example - Power Cycling Specific Outlets

The following command power cycles these outlets: 2, 6, 7, 8, 10, 13, 14, 15 and 16.

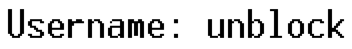
```
#  power outlets 2,6-8,10,13-16 cycle
```

Unblocking a User

If any user is blocked from accessing, you can unblock them at the local console.

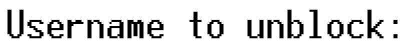
► *To unblock a user:*

1) Access the CLI interface using any terminal program via a local connection.
2) When the Username prompt appears, type `unblock` and press Enter.



```
Username: unblock
```

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 NX1 PDU

You can reset the NX1 PDU to factory defaults or simply restart it using the CLI commands.

Restarting the NX1 PDU

This command restarts the NX1 PDU. It is not a factory default reset.

► *To restart the NX1 PDU:*

1) Ensure you have entered administrator mode and the # prompt is displayed.
2) Type either of the following commands to restart the NX1 PDU.

```
#       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 Energy Readings

You can reset either one energy sensor or all energy sensors at a time to restart the energy accumulation process.

Only users with the "Admin" role assigned can reset energy readings.

► *To reset all energy counters:*

All counters includes inlets, outlets, and PDU (for multi-inlet models).

```
#     reset energy pdu
```

-- OR --

```
#     reset energy pdu /y
```

► *To reset one inlet's energy readings:*

```
#    reset energy inlet <n>
```

-- OR --

```
#    reset energy inlet <n> /y
```

If you entered the command without "/y", a message appears prompting you to confirm the operation. Type y to confirm the reset or n to abort it.

Variables:

- <n> is the inlet number.

Resetting to Factory Defaults

The following commands restore all settings of the NX1 PDU to factory defaults.

► *To reset NX1 PDU settings after login, use either command:*

```
#    reset factorydefaults
```

-- OR --

```
#    reset factorydefaults /y
```

► *To reset NX1 PDU 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 NX1 PDU 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 NX1 PDU 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
```

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 NX1 PDU to make sure that PDU is properly operating all the time, and the NX1 PDU 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 NX1 PDU 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 ✚ Monitor New Server .
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 NX1 PDU 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 NX1 PDU 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
Number of consecutive unsuccessful pings for failure	3

   - To make the NX1 PDU stop pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared, enter the following data. After 60 seconds, the NX1 PDU 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 ✚ New Rule .
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 NX1 PDU react only when the target PDU becomes inaccessible.

5) Select the System SNMP Notification Action.

Specifications

► *Max Ambient Operating Temperature:*

- 60 degrees Celsius

► *RS-485 Port Pinouts*

RS-485 Pin/signal definition

Pin No.	***Signal***	***Direction***	***Description***
1	—	—	—
2	—	—	—
3	***D+***	***bi-directional***	***Data +***
4	—	—	—
5	—	—	—
6	***D-***	***bi-directional***	***Data -***
7	—	—	—
8	—	—	—

Equipment Setup Worksheet Sample

- ► *NX1 PDU Model* ______________________________________

- ► *NX1 PDU 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

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 using any method OTHER THAN THE WEB INTERFACE is NOT supported by default.

To downgrade using any of these methods, a special parameter is required—see further instructions for each method.

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
2) Prepare required configuration files. See Configuration Files.
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 Raritan device.
- Your NX1 PDU must run firmware version 4.0.30 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

- fwupdate.cfg:

  This file MUST always be present for performing configuration or firmware upgrade tasks. See fwupdate.cfg.
- config.txt:

  This file is used for configuring device settings. See config.txt.
- devices.csv:

  This file is required only when there are device-specific settings to configure for multiple devices. See devices.csv.

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=raritan
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 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.

► *allow_downgrade*

- This parameter is required for any firmware downgrade via *USB drive*. If the parameter is not found, the process will fail.
- Add this parameter to this configuration file and set its value to *yes*.

Tip: Only firmware downgrade via USB is disabled by default. To downgrade firmware using other methods is still feasible by default, such as firmware downgrade via web interface.

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 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'

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.

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

- 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:raritan`

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 NX1 PDU running 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 any NX1 PDU running version 3.2.20 or later. See Logging in to CLI.
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>
   ```

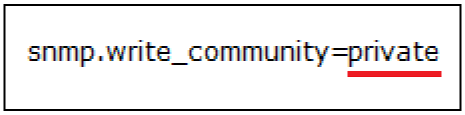
   -- OR --

   ```
   # 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 3 to 6 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 any NX1 PDU running version 3.2.20 or later. See *Configuration or Firmware Upgrade with a USB Drive*.

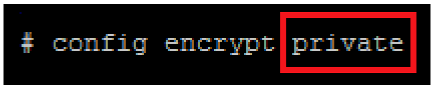
► *Illustration:*

In this example, we will encrypt the word "private", which is the value of the SNMP write community in the "config.txt" file.



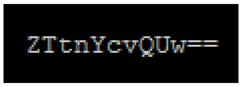
```
snmp.write_community=private
```

1) In the CLI, type the following command to encrypt "private."



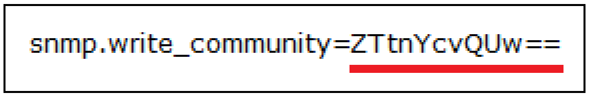
```
# config encrypt private
```

2) The CLI generates and shows the encrypted form of "private."



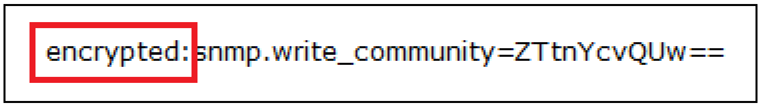
```
ZTtnYcvQUw==
```

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 NX1 PDU, 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 NX1 PDU:*

1) Create 2 files :
   - A "fwupdate.cfg" configuration file. It's a txt file that you rename. Below is an example

     user=admin

     password=legrand

     logfile=log.txt

     firmware=pdug4-ixg4-040033-49667.bin

- A “log.txt” file. It's a txt file that you create and that is empty. It is enriched with the history (the logs) of each PDU firmware update.

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 NX1 PDU.
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.

Bulk Configuration or Firmware Upgrade via DHCP/TFTP

If a TFTP 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 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 using any method OTHER THAN THE WEB INTERFACE is NOT supported by default.

To downgrade using any of these methods, a special parameter is required—see further instructions for each method.

► *Steps of using DHCP/TFTP for bulk configuration/upgrade:*

1) Create configuration files specific to your NX1 PDU 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 server properly.
3) Copy ALL required configuration files into the TFTP 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 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) Re-boot 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.

TFTP Requirements

To perform bulk configuration or firmware upgrade successfully, your TFTP 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 root directory. See *Bulk Configuration/ Upgrade Procedure*.

If you are going to upload any NX1 PDU diagnostic file or create a log file in the TFTP server, the first of the following requirements is also required.

- 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

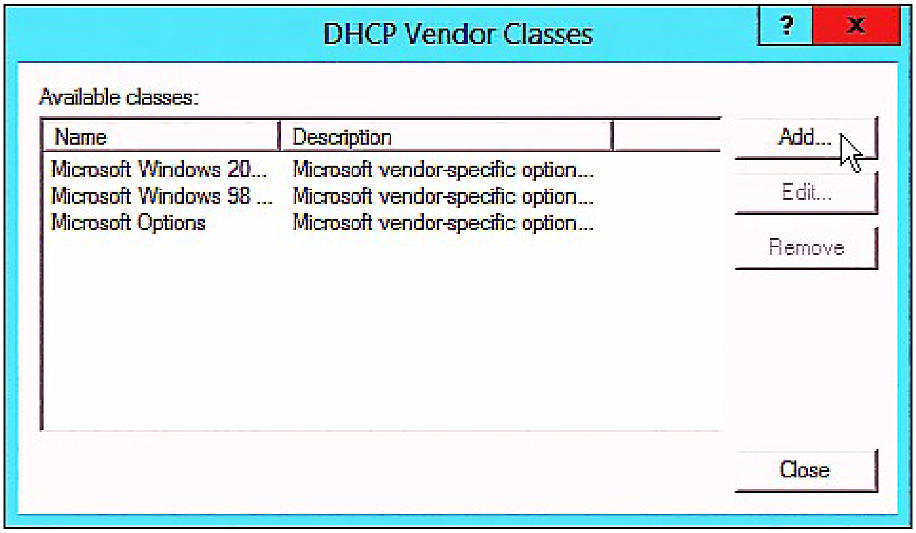
For those NX1 PDU devices using IPv4 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

► *Required Windows IPv4 settings in DHCP:*

1) Add a new vendor class for Raritan's NX1 PDU under IPv4.

   a. Right-click the IPv4 node in DHCP to select Define Vendor Classes.

   b. Click Add to add a new vendor class.



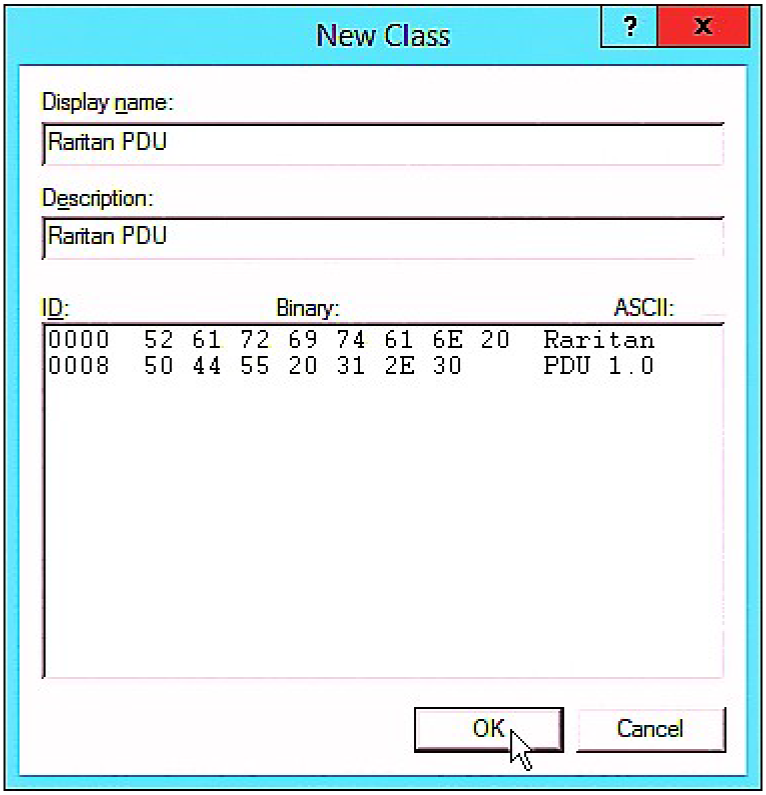
DHCP Vendor Classes

Available classes:

Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...

   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.



Raritan PDU

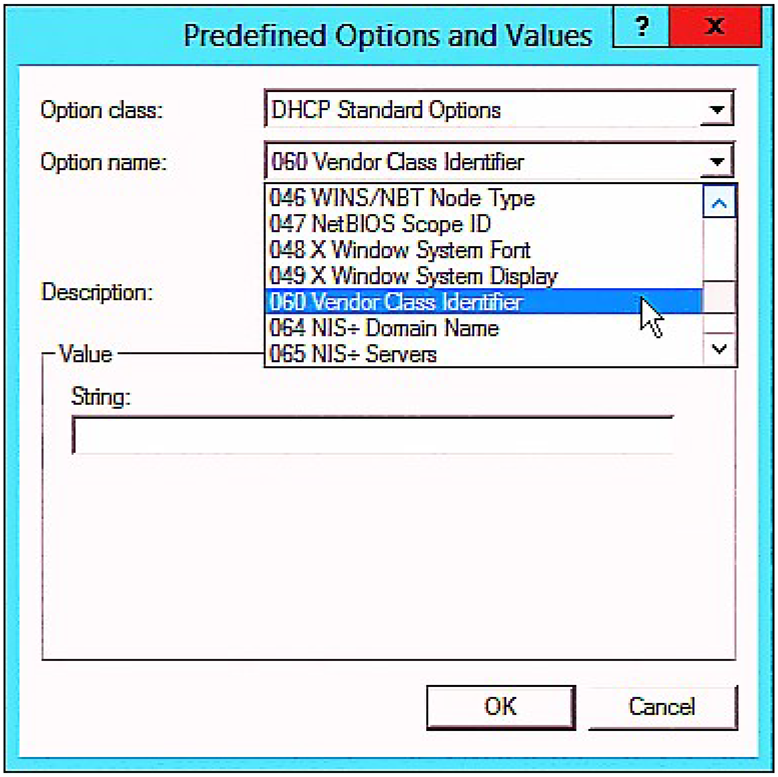
Raritan PDU

```
0000   52 61 72 69 74 61 6E 20   Raritan
0008   50 44 55 20 31 2E 30      PDU 1.0
```

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.



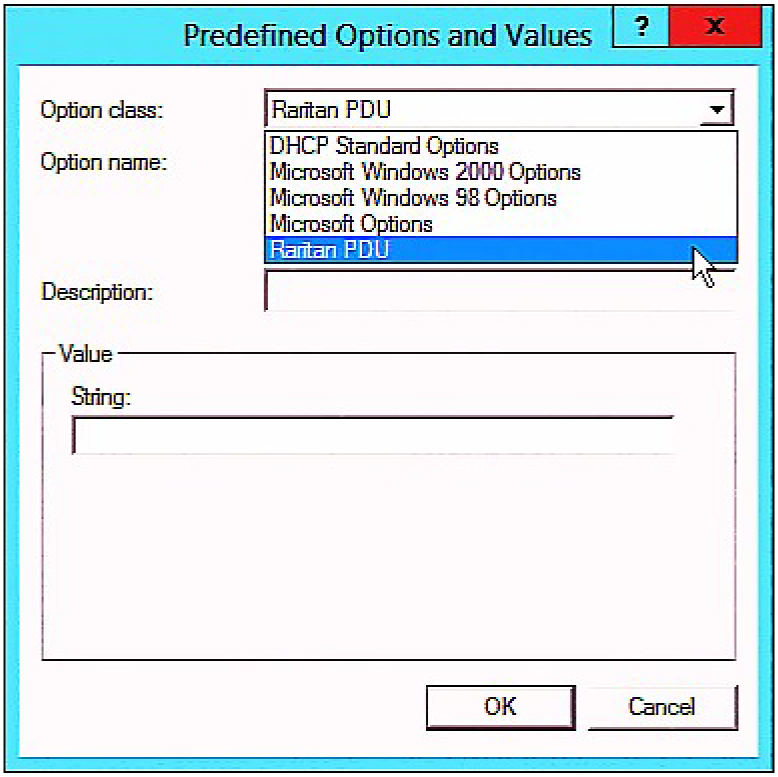
Option class: DHCP Standard Options

Option name: 060 Vendor Class Identifier

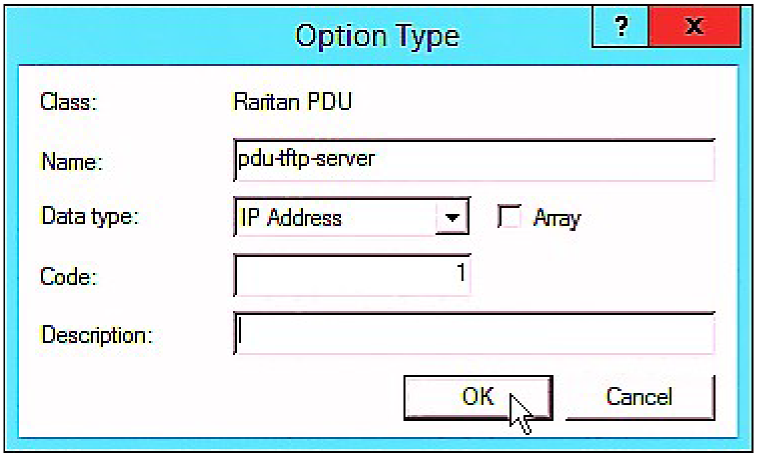
046 WINS/NBT Node Type
047 NetBIOS Scope ID
048 X Window System Font
049 X Window System Display
060 Vendor Class Identifier
064 NIS+ Domain Name
065 NIS+ Servers

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" in the Name field, select IP Address as the data type, and type 1 in the Code field.



Class: Raritan PDU

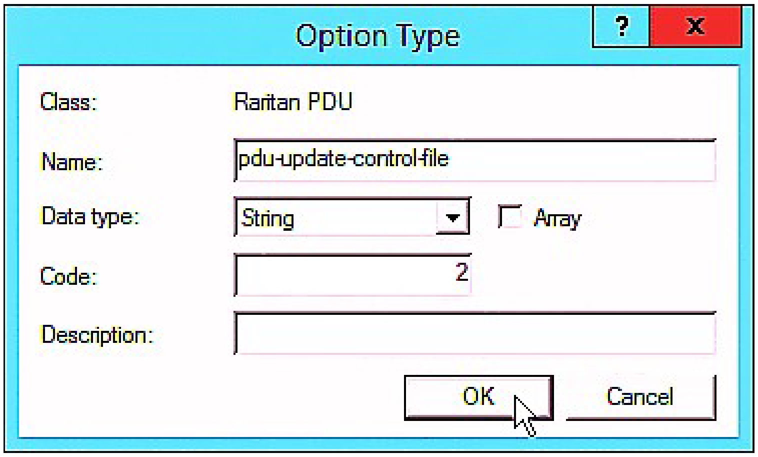
Name: pdu-tftp-server

Data type: IP Address □ Array

Code: 1

Description:

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

Class: Raritan PDU

Name: pdu-update-control-file

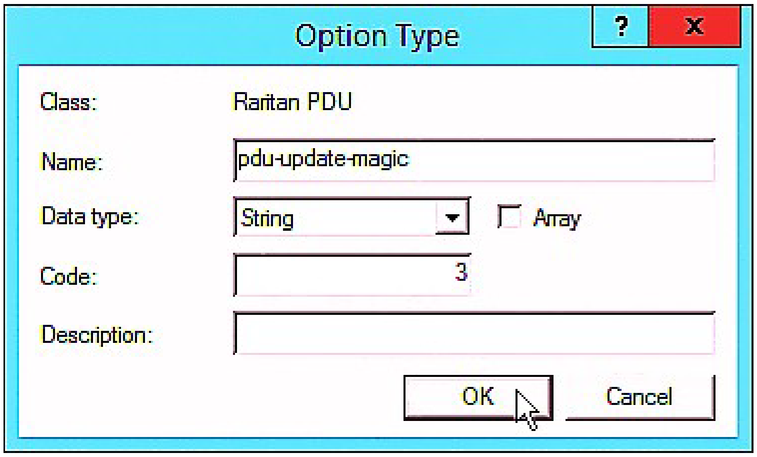
Data type: String

☐ Array

Code: 2

Description:

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

Class: Raritan PDU

Name: pdu-update-magic

Data type: String

☐ Array

Code: 3

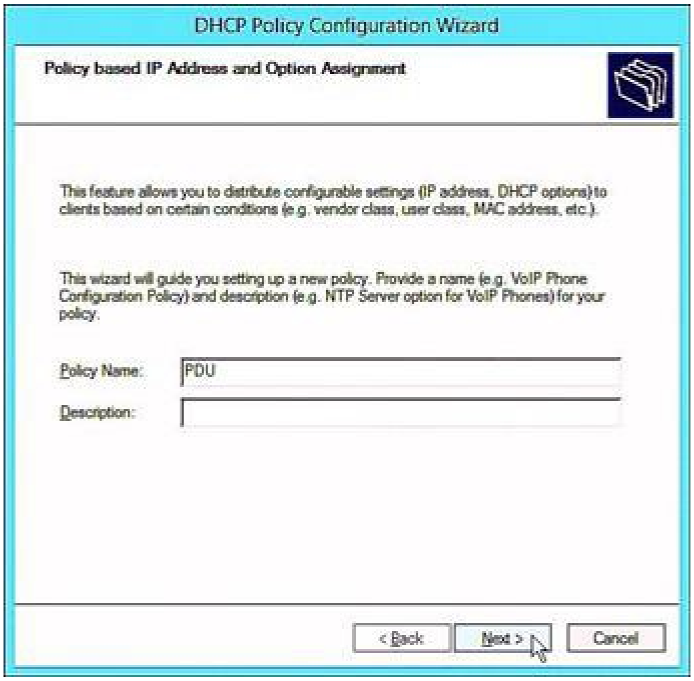
Description:

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.).

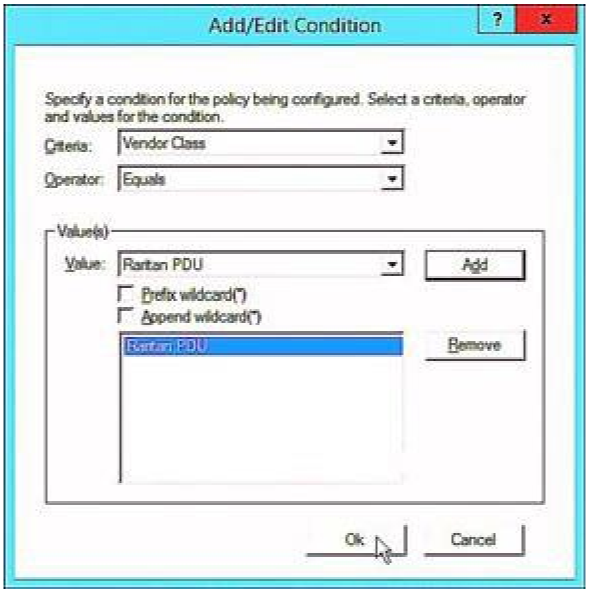
This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.

Policy Name: PDU

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: Vendor Class

Operator: Equals

Value(s)

Value: Raritan PDU

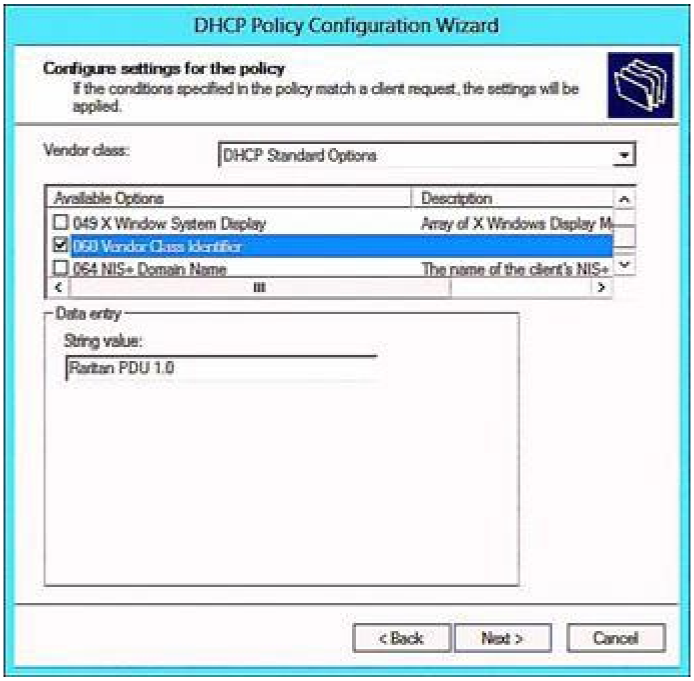
□ Prefix wildcard(*)

□ Append wildcard(*)

Raritan PDU

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.

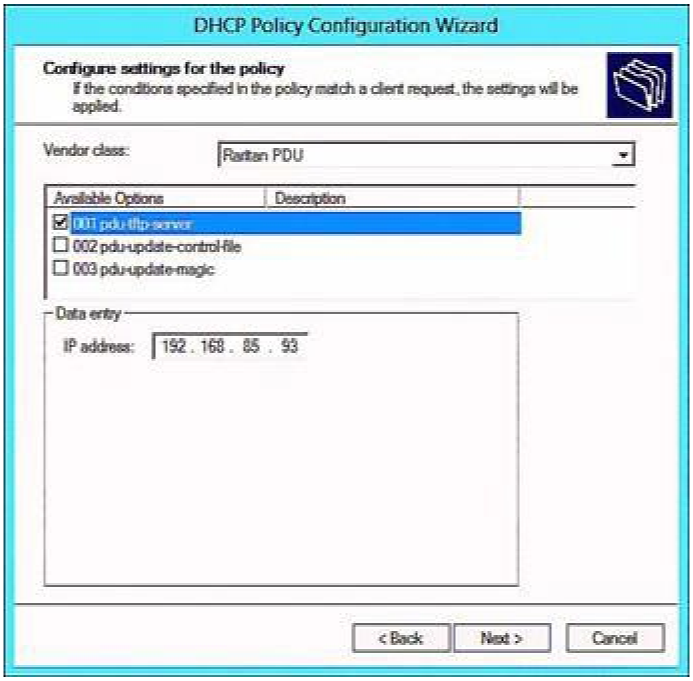
Vendor class: DHCP Standard Options

Available Options	Description
☐ 049 X Window System Display	Array of X Windows Display M
☑ 060 Vendor Class Identifier	
☐ 064 NIS+ Domain Name	The name of the client's NIS+

Data entry

String value: Raritan PDU 1.0

g. Select the "Raritan PDU" in the "Vendor class" field, select "001 pdu-tftp-server" from the Available Options list, and type your TFTP 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.

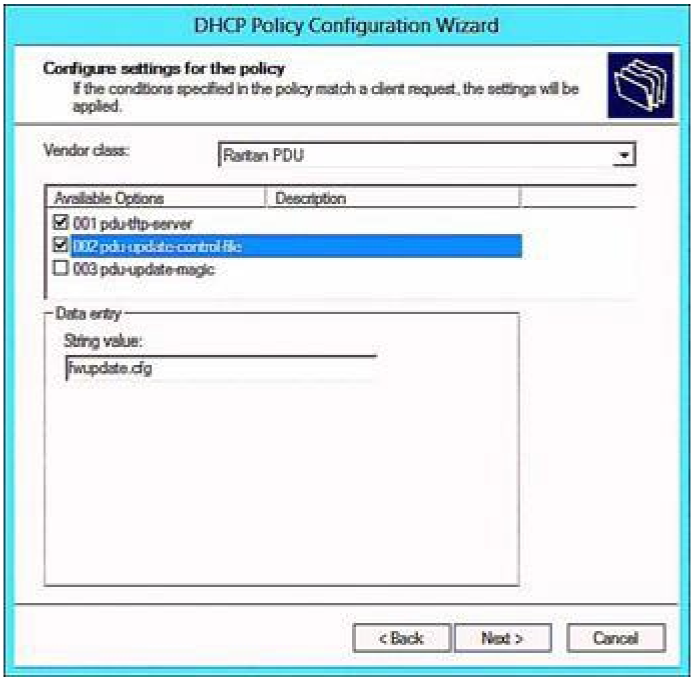
Vendor class: Raritan PDU

Available Options	Description
☑ 001 pdu-tftp-server	
☐ 002 pdu-update-control-file	
☐ 003 pdu-update-magic	

Data entry

IP address: 192 . 168 . 85 . 93

h. Select "002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" 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: Raritan PDU

Available Options	Description
☑ 001 pdu-tftp-server	
☑ 002 pdu-update-control-file	
□ 003 pdu-update-magic	

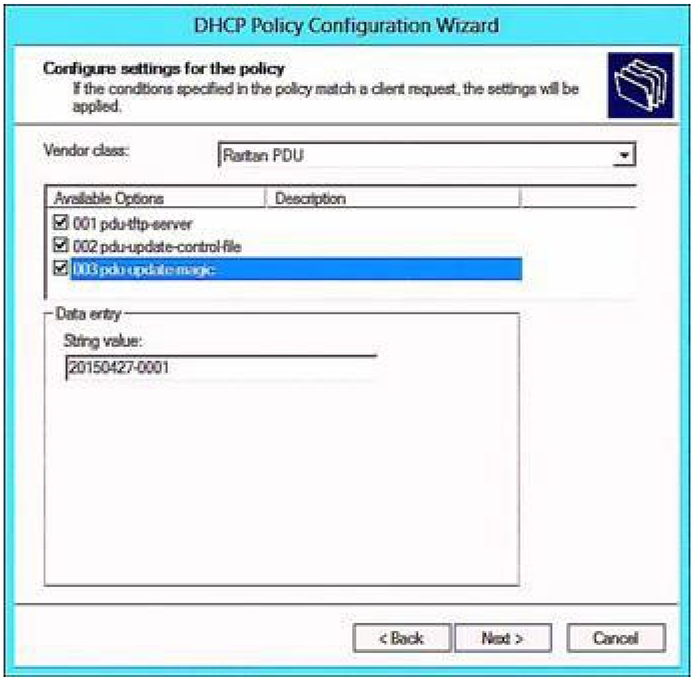
Data entry

String value: fwupdate.cfg

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 NX1 PDU at the time of executing the "fwupdate.cfg" commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in NX1 PDU. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.



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: Raritan PDU

Available Options	Description
☑ 001 pdu-tftp-server	
☑ 002 pdu-update-control-file	
☑ 003 pdu-update-magic	

Data entry

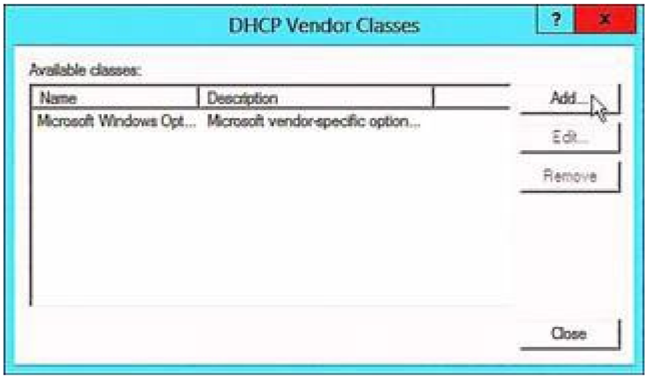
String value: 20150427-0001

DHCP IPv6 Configuration in Windows

For those NX1 PDU 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 NX1 PDU under IPv6.
   a. Right-click the IPv6 node in DHCP to select Define Vendor Classes.
   b. Click Add to add a new vendor class.



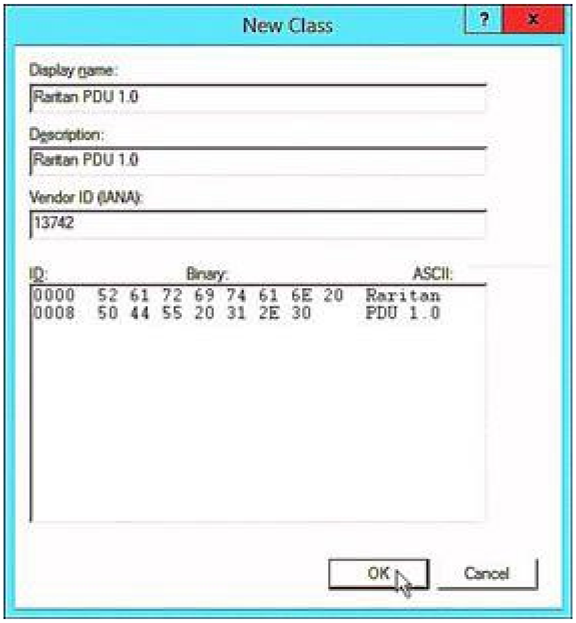
DHCP Vendor Classes

Available classes:

Name	Description
Microsoft Windows Opt...	Microsoft vendor-specific option...

   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.



Display name:
Raritan PDU 1.0

Description:
Raritan PDU 1.0

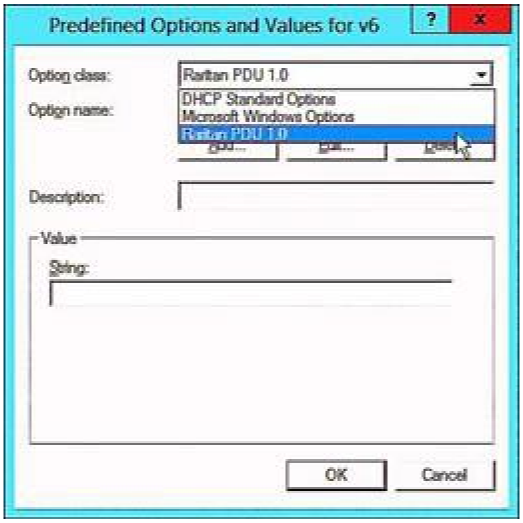
Vendor ID (IANA):
13742

```
ID:              Binary:                    ASCII:
0000   52 61 72 69 74 61 6E 20   Raritan
0008   50 44 55 20 31 2E 30      PDU 1.0
```

2) Add three options to the "Raritan PDU 1.0" vendor class.

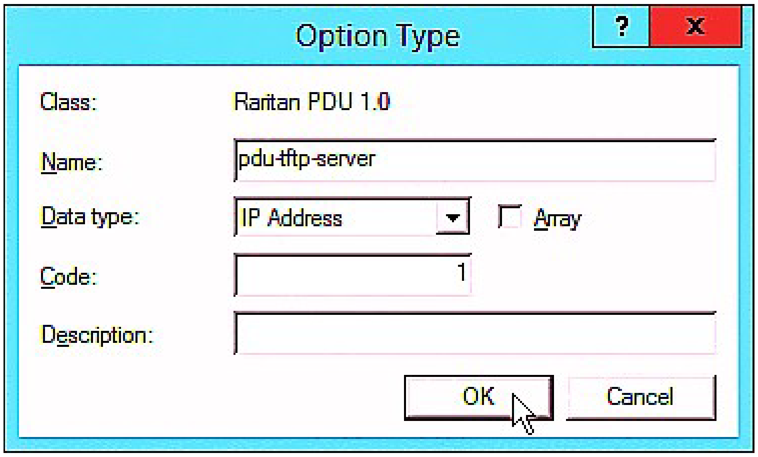
a. Right-click the IPv6 node in DHCP to select Set Predefined Options.

b. Select Raritan PDU 1.0 in the "Option class" field.



Option class: Raritan PDU 1.0

c. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.



Class: Raritan PDU 1.0

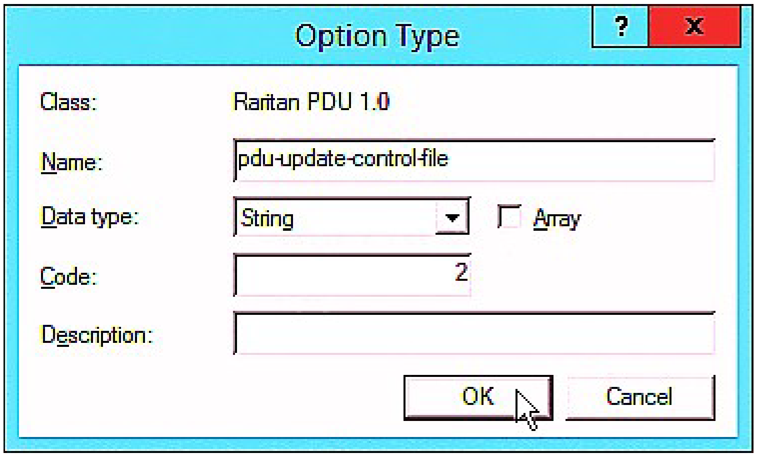
Name: pdu-tftp-server

Data type: IP Address ☐ Array

Code: 1

Description:

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.



Class: Raritan PDU 1.0

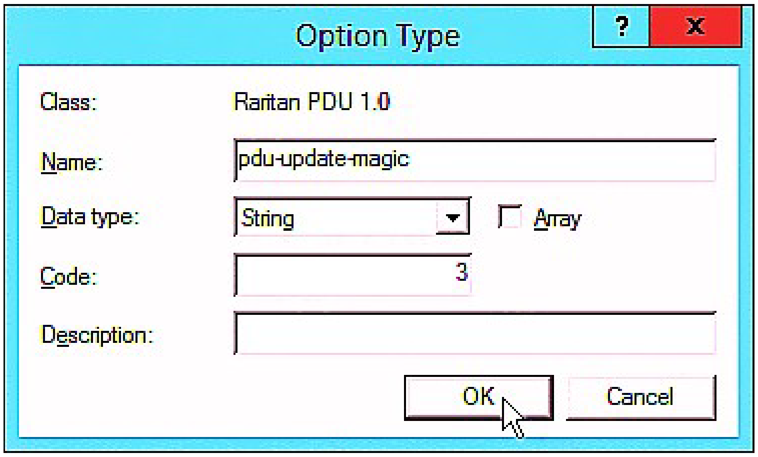
Name: pdu-update-control-file

Data type: String ☐ Array

Code: 2

Description:

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.



Option Type

Class: Raritan PDU 1.0

Name: pdu-update-magic

Data type: String ☐ Array

Code: 3

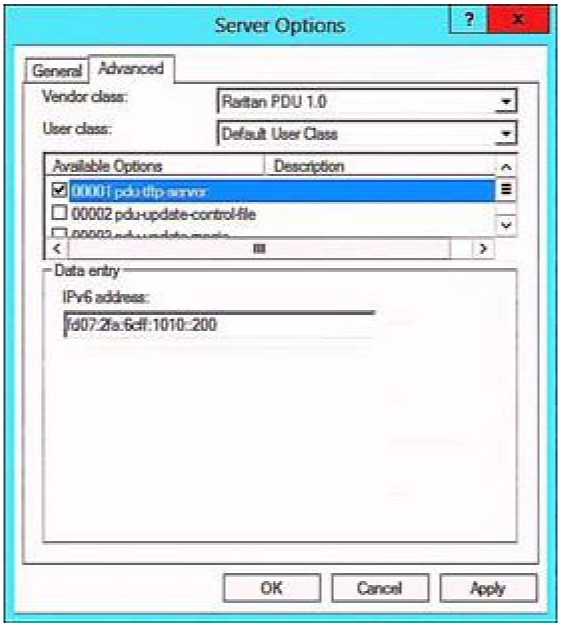
Description:

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" from the Available Options list, and type your TFTP server's IPv6 address in the "IPv6 address" field.



Server Options

General | Advanced

Vendor class: Raritan PDU 1.0

User class: Default User Class

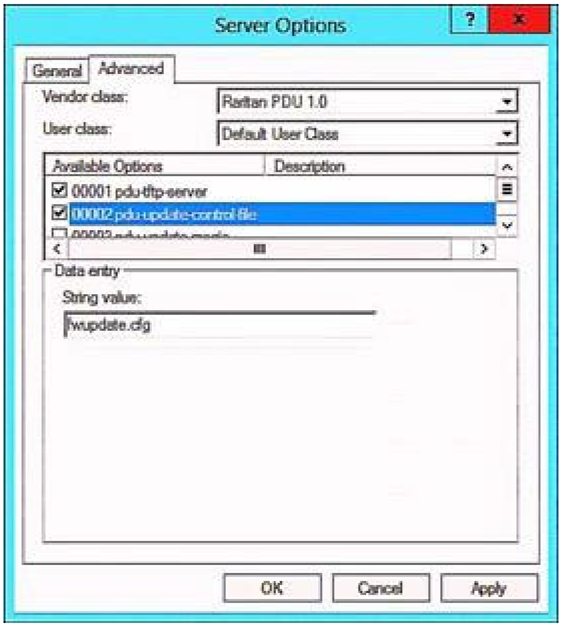
Available Options	Description
☑ 00001 pdu-tftp-server	
☐ 00002 pdu-update-control-file	
☐ 00003 pdu-update-magic	

Data entry

IPv6 address:

fd07:2fa:6cff:1010::200

d. Select "00002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.



Vendor class: Raritan PDU 1.0

User class: Default User Class

Available Options	Description
☑ 00001 pdu-tftp-server	
☑ 00002 pdu-update-control-file	
□ 00003 pdu-update-magic	

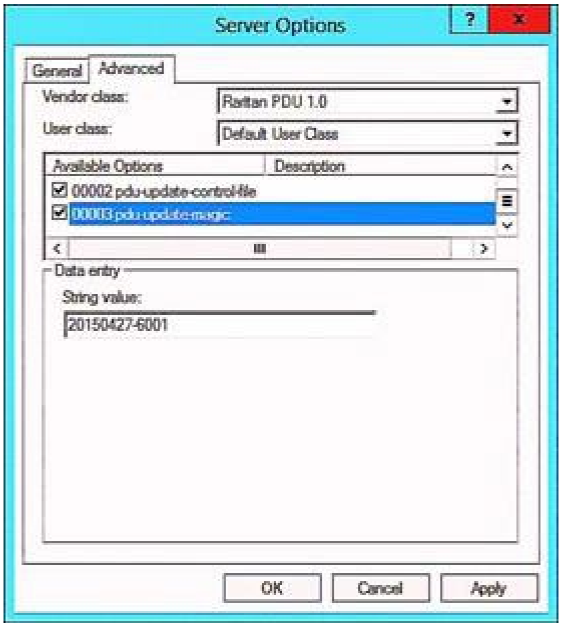
Data entry

String value: fwupdate.cfg

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 NX1 PDU at the time of executing the "fwupdate.cfg" commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in NX1 PDU. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.



Vendor class: Raritan PDU 1.0

User class: Default User Class

Available Options	Description
☑ 00002 pdu-update-control-file	
☑ 00003 pdu-update-magic	

Data entry

String value: 20150427-6001

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 NX1 PDU will provide the following value of the vendor-class-identifier option (option 60).
   - vendor-class-identifier = "Raritan PDU 1.0"

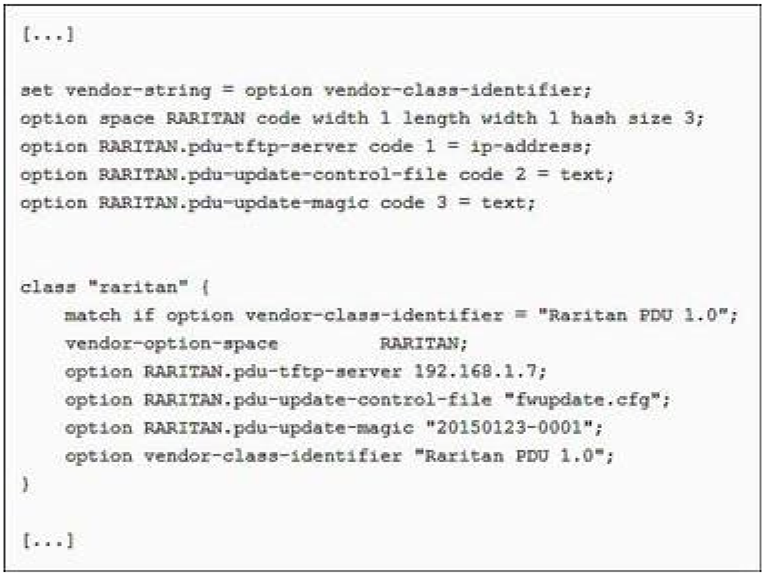
   Configure the same option in DHCP accordingly. The NX1 PDU accepts the configuration or firmware upgrade only when this value in DHCP matches.
3) Set the following three sub-options in the "vendor-encapsulated-options" (option 43).
   - code 1 (pdu-tftp-server) = the TFTP server's IPv4 address
   - code 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 NX1 PDU at the time of executing the "fwupdate.cfg" commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in NX1 PDU. 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;


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-update-control-file "fwupdate.cfg";
    option RARITAN.pdu-update-magic "20150123-0001";
    option vendor-class-identifier "Raritan PDU 1.0";
}

[...]
```

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:*

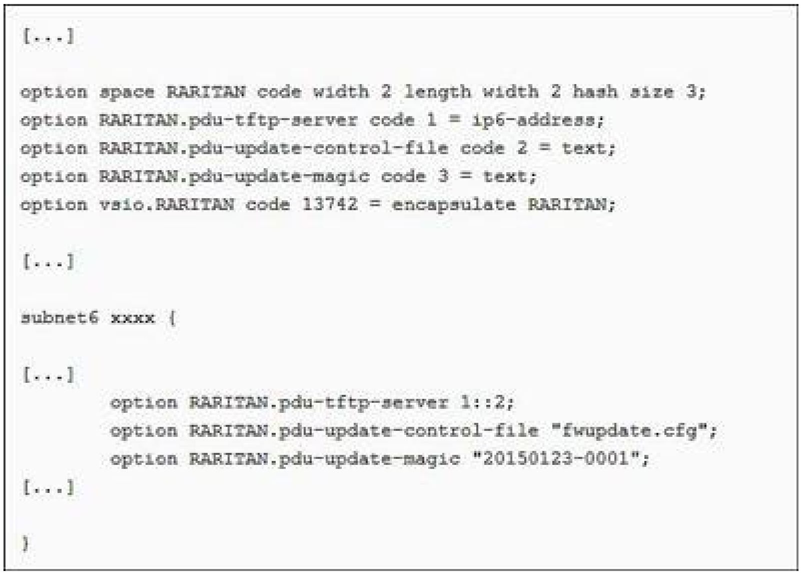
1) Locate and open the "dhcpd6.conf" file of the DHCP server.
2) The NX1 PDU will provide the following values to the "vendor-class" option (option 16). Configure related settings in DHCP accordingly.
   - 13742 (Raritan's IANA number)
   - Raritan PDU 1.0
   - 15 (the length of the above string "Raritan 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
   - 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 NX1 PDU at the time of executing the "fwupdate.cfg" commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in NX1 PDU. 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 vsio.RARITAN code 13742 = encapsulate RARITAN;

[...]

subnet6 xxxx {

[...]
        option RARITAN.pdu-tftp-server 1::2;
        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
- 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.

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:raritan@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.

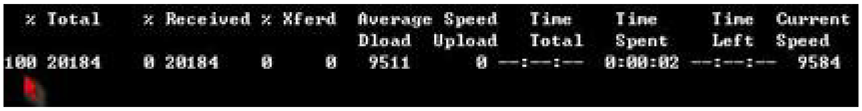
► *To download raw configuration via curl:*

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:raritan@192.168.84.114/cgi-bin/
raw_config_download.cgi > config.txt
```

Uploading Raw Configuration

There are two upload methods:

- *SCP or PSCP command:* SeeRaw Configuration Upload and Download .
- *CURL command:* See Upload via Curl.

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 NX1 PDU 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 NX1 PDU devices to update.
- When there are device-specific settings involved for updating more than one NX1 PDU 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 NX1 PDU whose raw configuration you want to upload.
`<config file>`	Filename of the configuration file. • For the syntax, see *config.txt*.

1) 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.

2) After several seconds, NX1 PDU 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. • 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*.

Parameter	Description
`<dev_list file>`	Filename of the device list file in CSV format. • For the content format, see *devices.csv*.
`<dev_col>`	`<dev_col>` comprises "serial:" or "mac:" and the number of the column where the serial number or MAC address of each NX1 PDU 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`.

1) NX1 PDU 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:raritan@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:raritan@192.168.84.114/cgi-bin/raw_config_download.cgi
```

Curl Upload Return Codes

After performing raw configuration *Upload via Curl*, 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.

Code	Description
5	Invalid raw configuration file provided.
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.

► *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 NX1 PDU 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
```

► *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 NX1 PDU, 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 NX1 PDU whose settings you want to back up.

2) Type the user password when prompted.
3) The system saves the settings from the NX1 PDU 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 NX1 PDU 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 NX1 PDU, 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.

Scenario 1: Use the default SCP port and default filename

- SSH/SCP port is the default (22), and the accessed NX1 PDU 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 NX1 PDU 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 NX1 PDU 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 NX1 PDU is a Port-Forwarding expansion device.
- Renaming the diagnostic file is wanted.

```
scp -P <port> <user name>@<device ip>:/diag-data.zip <filename>
```

- *<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 NX1 PDU 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.

1) Type the password when prompted.
2) The system downloads the specified data from the NX1 PDU 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.

► *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.

1) Type the password when prompted.
2) 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 NX1 PDU 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 NX1 PDU. That is, they should be either not available or remain commented out in the configuration file you will upload.

Comment syntax	Description
#INTERNAL#	Internal use only. They are NOT user configurable settings.
#OLD/INVALID#	These keys are old or invalid ones.

Resetting to Factory Defaults

Important: Exercise caution before resetting the NX1 PDU to its factory defaults.

This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only energy data and firmware upgrade history are retained.

In This Chapter

Factory Default Settings

Only secure access--physical or by secure network protocols--is enabled by default.

During the first login, before any service can be used, you are forced to change the default password.

► *Default configuration:*

The factory default configuration disables these services:

- SNMP Agent (remains disabled even after default password is changed)
- SCP interface (disabled until default password is changed)

The factory default configuration enables these services:

- Both Ethernet ports are IPv4 enabled for DHCP with access to APIPA link local address
- HTTPS Server
- SSH Server
- Console (not applicable to PX4/PRO4X models)

► *Default password change requirement:*

The default password must be changed upon first use, before any other configuration changes or device access are allowed. In factory default configuration, the following protocols and tools, with the following restrictions, allow you to first update the default password:

- HTTPS Server Web User Interface: Restricted to a password change page/form only.
- HTTPS Server (JSON API Web Service): API limited to a password change for the default account.
- SSH Server: Prompts for a password change.
- Console: Prompts for a password change.

Note: Once the default password is changed, the restrictions are removed and the device resumes normal operations for the protocols and tools listed above. Upon any reset to factory defaults, the restrictions will again be enforced and a change to the default password will again be required.

Using the CLI Command

The Command Line Interface (CLI) provides a reset command for resetting to factory defaults.

► *To reset to factory defaults after logging in to the CLI:*

1) Log in to the CLI by typing the user name "admin" and its password.
2) After the # system prompt appears, type either of the following commands and press Enter.

```
#    reset factorydefaults
```

-- OR --

```
#    reset factorydefaults /y
```

3) If you entered the command without "`/y`" , a message appears prompting you to confirm the operation. Type y to confirm the reset.
4) Wait until the reset is complete.

► *To reset to factory defaults without logging in to the CLI:*

You can also reset the product to factory defaults in the CLI prior to login. This option requires physical access to the unit, either at the console (for older models) or using a USB configuration method.

1) Connect to the NX1 PDU and launch a terminal emulation program.
2) At the Username prompt in the CLI, type "factorydefaults" and press Enter.

```
Username:              factorydefaults
```

3) Type `y` on a confirmation message to perform the reset.

Third Party Licenses

This appendix contains third party licenses for software used that require including the license in documentation.

For information on open source software, see raritan.com/about-us/legal/open-source-software-statement

Licenses - Angular

@angular-devkit/build-angular

MIT

The MIT License

@angular-devkit/core

MIT

The MIT License

@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.

@angular/platform-browser

MIT

@angular/router

MIT

@babel/runtime

MIT

MIT License

@ctrl/ngx-chartjs

MIT

MIT License

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

0BSD

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 bellow.

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-Kougyou-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.

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 McKerrell 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.

tinyxml

Yves Berquin

As of release 0.6 the tinyxml library is included (unchanged) as part of the distribution.

tinyxml (v2.5.1)

http://www.sourceforge.net/projects/tinyxml

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 forstacktraces. 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 strlcat() (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.

strlcat() 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.

* 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 reimplementation 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). 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.

Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

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.

Part 14: USC/Information Sciences Institute copyright notice (BSD) -----

Licenses - Open LDAP

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.

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

(eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

---------------

Copyright (C) 1995-1998 Eric Young (eay@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 aheared 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 rouines 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