

Lenovo Power Distribution Unit (PDU)

Operations Manual

LenovoTM

2019-02

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo. Google Chrome is a trademark of Google, Inc. HyperTerminal is a registered trademark of Hilgraeve. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Microsoft, Internet Explorer, Vista, and Windows are registered trademarks of Microsoft Corporation in the United States and other countries. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. National Electrical Code and NEC are registered trademarks of National Fire Protection Association, Inc. Phillips is a registered trademark of Phillips Screw Company. Rittal is a registered trademark of Rittal GmbH & Co. KG. All other trademarks are property of their respective companies.

©Copyright 2016–2019 Lenovo. All rights reserved. No part of this document may be reproduced in any way without the express written approval of Lenovo.

Class A EMC Statements

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

ICES-003

This Class A Interference Causing Equipment meets all requirements of the Canadian Interference Causing Equipment Regulations ICES-003.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

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



Special Symbols

The following are examples of symbols used on the PDU or accessories to alert you to important information:



RISK OF ELECTRIC SHOCK - Observe the warning associated with the risk of electric shock symbol.



CAUTION: REFER TO OPERATOR'S MANUAL - Refer to your operator's manual for additional information, such as important operating and maintenance instructions.



This symbol indicates that you should not discard waste electrical or electronic equipment (WEEE) in the trash. For proper disposal, contact your local recycling/reuse or hazardous waste center.

Table of Contents

1	INTRODUCTION	10
	Description	10
	Product Specifications	11
	Lenovo PDU Models	11
	LCD Interface	13
	Circuit Breakers	14
	Power Outlets	15
	Input Power Cord	15
	Accessories	15
	Environmental Monitoring Probe	15
	Features	16
	Ease of Use	16
	Communication	16
	Power Control Management	16
	Monitoring	16
	Configurability and Security	16
2	SAFETY WARNINGS	17
3	INSTALLATION	19
	Installation Precautions	19
	Inspecting the Equipment	20
	Package Contents	20
	Optional Environmental Monitoring Probe	22
	Installation Overview	23
	Tools	23
	Configurations	24
	IEC Outlet Grip Plug Retention Mechanism	25
	Installing PDUs in a Rack Cabinet	25
	Using Factory-installed Mounting Buttons (For Lenovo Racks 9360 and 9363 for Example)	26
	Using Mounting Buttons Installed on Clip Feet	27
	Using Clip Feet and Cage Nuts on a Square-hole Rack	28
	Using Mounting Brackets for Lenovo Rack 9307	30
	Using Mounting Brackets for Lenovo Rack 9308	31
	Using Mounting Buttons for Lenovo Rack 9360	32
	Using Mounting Buttons for Lenovo Rack 9363	33
	Grounding the PDU	34
	Network and Environmental Ports	34
	Connecting to a Computer Serial Port	35
	Connecting to a LAN Ethernet Port	36
	Connecting Multiple PDUs in a Daisy Chain	36
	Connecting Optional Environmental Monitoring Probe Equipment	38
	Connecting the Output Devices	39
	Operating the PDU	40

4	OPERATION OVERVIEW	41
	Operation Interfaces	41
	Local Operation Interface	41
	Remote Operation Interfaces	43
	Outlets and Circuit Breakers	43
	Ports, Operation Buttons, and LED Status Indicators	44
	Operation Concepts	45
	User Login and Access Policy	45
	Common Operations	46
	Starting the PDU	46
	Shutting Down the PDU	46
	Restarting the PDU Network Management and Control (eNMC) module.	46
5	NETWORK COMMUNICATION CONFIGURATION	48
	LCD — DHCP	48
	LCD— Static IP address	49
	Serial connection — Static IP address	50
	Verify Web Operation After Configuration	51
6	LCD INTERFACE OPERATION	52
	LCD Display and Control Buttons	52
	Operation Mode	54
	Screensaver Cycling Sequence	54
	Startup Screen	54
	Password Protected Menus	55
	Main Menu Selections	55
	Active Alarms Menu	57
	Alarms History Menu	57
	Meter Menu	58
	PDU Submenu	59
	Sections Submenu	60
	Outlets Submenu	61
	Environment Submenu	61
	Control Menu	62
	Settings Menu	62
	USB Flash Mode Submenu	63
	Display Submenu	68
	Daisy Chain Submenu	69
	IPv4 Submenu	72
	Language Submenu	72
	Factory Submenu	73
	PDU Info Menu	73
7	SERIAL INTERFACE OPERATION	74
	Supported Commands	74
	? command	75
	info command	76
	quit command	78
	get command	78

set command	80
pdu command	83
Error Messages	83
XML Object Tables	83
8 WEB INTERFACE OPERATION	84
Navigating the Web Interface	84
Languages	86
Accessing the Web Interface	87
Menu Selections	88
Power Management	89
Logs & Notifications	89
Settings	89
Network	90
Access Privileges	90
Administrator	90
Local or Remote Administrator	91
PDU-User	92
Outlet-User	93
Session Management	94
Overview	94
Review/Modify PDU Data	94
Branch Circuits	96
Review Branch Circuits	96
Change Groups Measurements Settings	96
Turn Sections On or Off	97
Change Individual Section Settings	97
Devices	98
Review Devices	98
Add Devices	99
Delete Devices	100
Turn Devices On or Off	100
Change Device Settings	100
Outlets	102
Review/Modify PDU Outlets	102
Environment	103
Configure Environment Sensor Settings	103
Power Schedule	104
Define a Power Schedule	104
Active Alarms	105
Review Active Alarms	105
Logs	106
Clear the Event Log	106
Download the Event Log as a Comma Separated Value File	106
Trap Notification	107
Define the Trap Receivers	107
Syslog	108
Retrieve or Modify Syslog Data	108

Access Accounts	109
Configure the SuperUser.	109
Configure the E-mail Notification Settings.	109
Configure the LCD Password	109
Configure Local User Access	110
Configure Remote Group Access	111
System.	111
Set General System Settings	112
Enable/Disable Firmware Upgrade	112
Configure PDU Network Management and Control Module.	113
Perform Firmware Upgrade.	113
PDU Configuration.	114
Date & Time	114
Manually Configure the Date and Time.	114
Automatically Configure the Date and Time	115
TCP/IP	115
Configure the Ethernet Link Speed and Duplex Mode	115
Configure the IPv4 Settings	116
Configure the IPv6 Settings	116
Configure the DNS	117
Configure the SMTP	117
SNMP	118
Enable/Disable the SNMP Agent.	118
Define SNMPv1 Users	118
Define SNMPv3 User-based Security Model Users	118
Access Lenovo PDU MIB Objects (Privileged Access Only).	119
Energy Wise	119
Enable Energy Wise	119
Disable Energy Wise.	119
Start/Stop Energy Wise Commands	120
Security	120
Enable/Disable SSL Encryption	120
Enable/Disable the Telnet Interface	121
Enable/Disable the SSH Interface	121
Enable/Disable FTP	122
Set Authentication Mode	122
Set LDAP Search Configuration	122
Authenticate LDAP Remote User	123
Set LDAP Server Global Parameters.	125
Modify LDAP Server Settings	125
Add RADIUS Server	126
Edit Parameters for a RADIUS Server.	126
9 MAINTENANCE AND ALARMS	127
Preventive Maintenance	127
Equipment Disposal.	127

- Firmware Upgrade 127
 - Upgrading Firmware with Hypertext Transfer Protocol 128
 - Upgrading the Firmware with FTP Protocol 130
 - Upgrading the Firmware with the USB Port 131
- Active Alarms 131
 - Defining the Alarm or Event Condition 132
 - Type Code 0 or 1 (OS or System) 133
 - Type Code 2 or 3 (PDU or User) 134
- 10 SERVICE AND SUPPORT 140**

Chapter 1 Introduction

Description

The Lenovo Power Distribution Unit (PDU) is an intelligent PDU that is designed to distribute power within a standard 19-inch rack. A wide range of models let you connect and manage a variety of outlets from a single power connection.

Figure 1 shows an example of the installed Lenovo PDU.

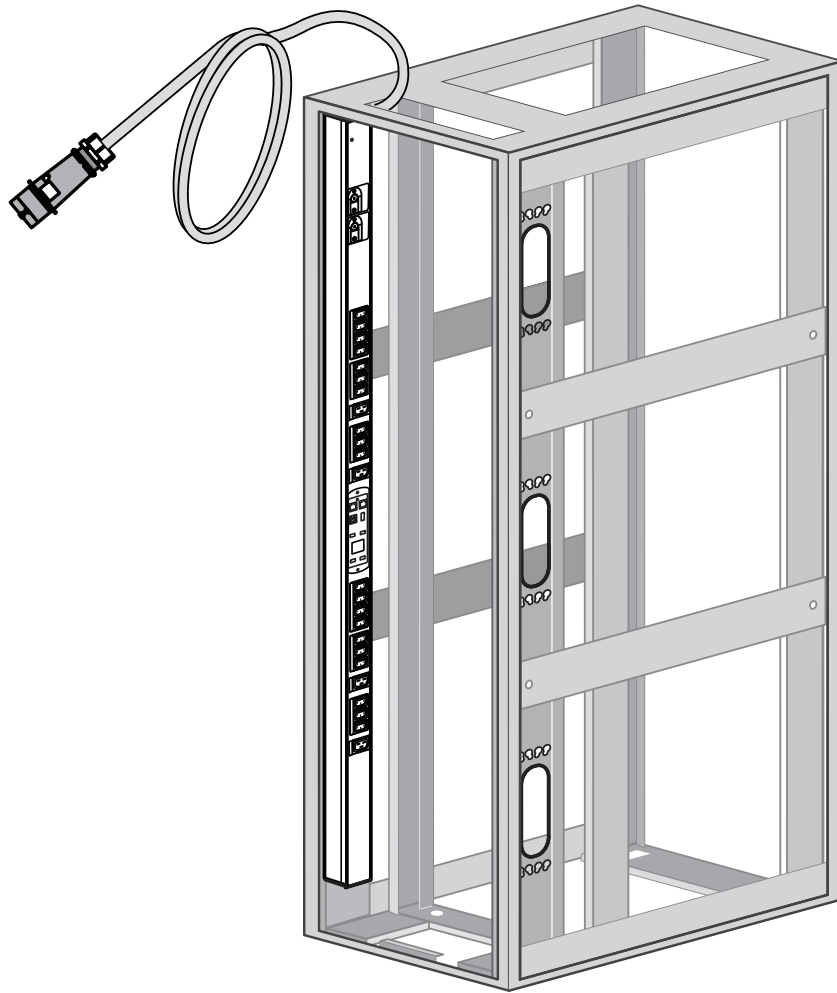


Figure 1. Example Lenovo PDU Installation

The Lenovo PDU family provides two different PDU topologies:

- Basic with no monitoring or intelligent controls
- Smart with monitoring at the input, branch, and individual outlet control and monitoring



NOTE

These capabilities are expressed in the model numbers of the PDUs.

Table 1 shows which main features are implemented or not implemented, depending on the topology:

Table 1. Monitoring and Management Features Available for PDU Topologies

Models	Input Metering	Branch Metering	Outlet Metering	Outlet Switching	Environmental Sensor Monitoring
Basic	—	—	—	—	—
Smart	•	•	•	•	•
NOTE Environmental sensor monitoring is only available if an Environmental Monitoring Probe (EMP) is attached.					

Product Specifications

Find product specifications, diagrams, part number and ordering matrix documents, and marketing collateral at <http://shop.lenovo.com/us/en/systems/servers/options/systemx/rack-power-infrastructure/power/>.

Lenovo PDU Models

The Lenovo PDU models support world-wide markets. These model types are defined primarily by the system management and monitoring capabilities, but the capabilities are also defined by the hardware configurations.

The PDU models support single-phase applications (or three-phase for Americas models) and can manage up to 42 outlets. Network-connected models feature an LCD display and LEDs to indicate status on communication connectors. Smart models contain LEDs to indicate outlet status. All PDUs have attached power cords and circuit breakers (see Figure 2).

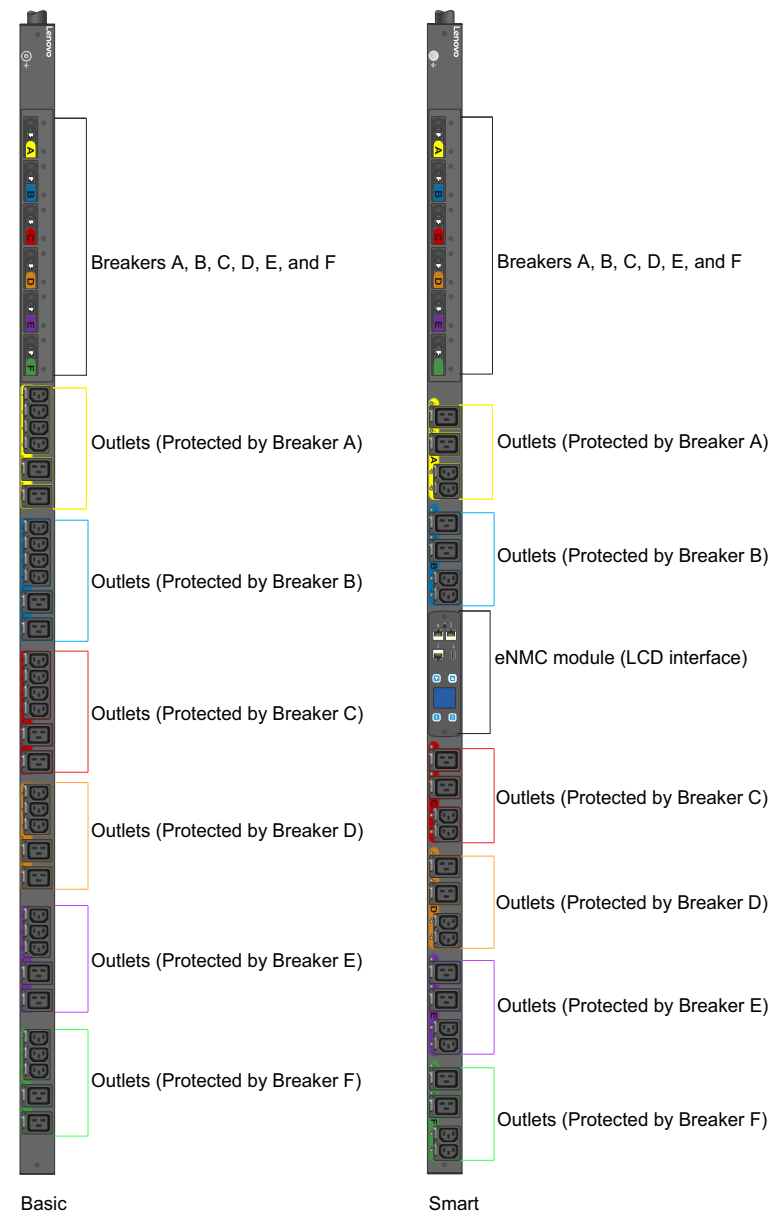


Figure 2. Example Lenovo PDU Products

LCD Interface

The LCD interface is operated using the LCD display, buttons, and ports of the embedded communications module (PDU Network Management and Control (eNMC) module). See Figure 3.

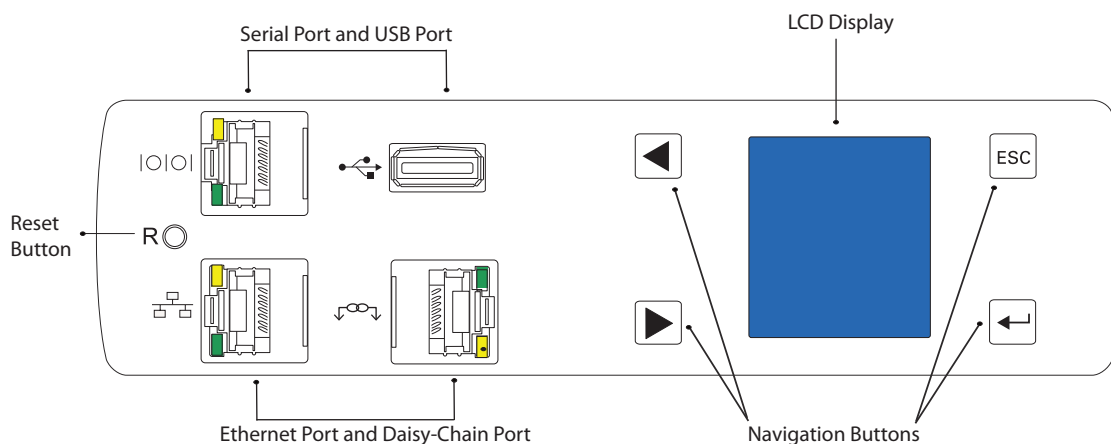


Figure 3. LCD Interface Front Panel

LCD Display

The LCD display provides information about load status, events, measurements, identification, and settings. The LCD interface also provides some basic configuration. For more information, see “Operation Interfaces” on page 41.

Navigation Buttons

Navigate through the display with buttons. For more information, see “Ports, Operation Buttons, and LED Status Indicators” on page 44.

Reset Button

Restart (reset) the PDU Network Management and Control (eNMC) module through this button. Insert and retract a probe in the reset button opening to perform a communications module restart.



NOTE Resetting the PDU does not affect the power to the outlets.

Connectivity and Serial Ports

- ▮ **Serial or Environmental Monitoring Probe (EMP) Port.** Connects to the serial (COM) RS-232 connector on a computer with a DB9-to-RJ-45 cable, allowing the computer to act as a configuration console. As an alternative, the connection can be used to connect an optional EMP in order to collect temperature and humidity data.
- ▮ **Ethernet Port Connector.** Connects to a LAN, allowing configuration through a 10/100 autosensing network connection.
- ▮ **Daisy-Chain Port Connector.** Used to daisy-chain up to eight PDUs together to use a single Ethernet connection.
- ▮ **USB Port.** Used for firmware upgrade.

Circuit Breakers

Circuit breakers activate if the load current rating of an outlet section exceeds 16A (Europe) / 20A (US). Power to the outlet turns off automatically. To reset the circuit breaker, turn the breaker from Off to On.

NOTE 1 The On/Off positions are indicated on the circuit breakers.



NOTE 2 To manually disconnect power to a device that is connected to the PDU, disconnect the device power cord from the PDU outlet.

Figure 4 shows circuit breaker examples.

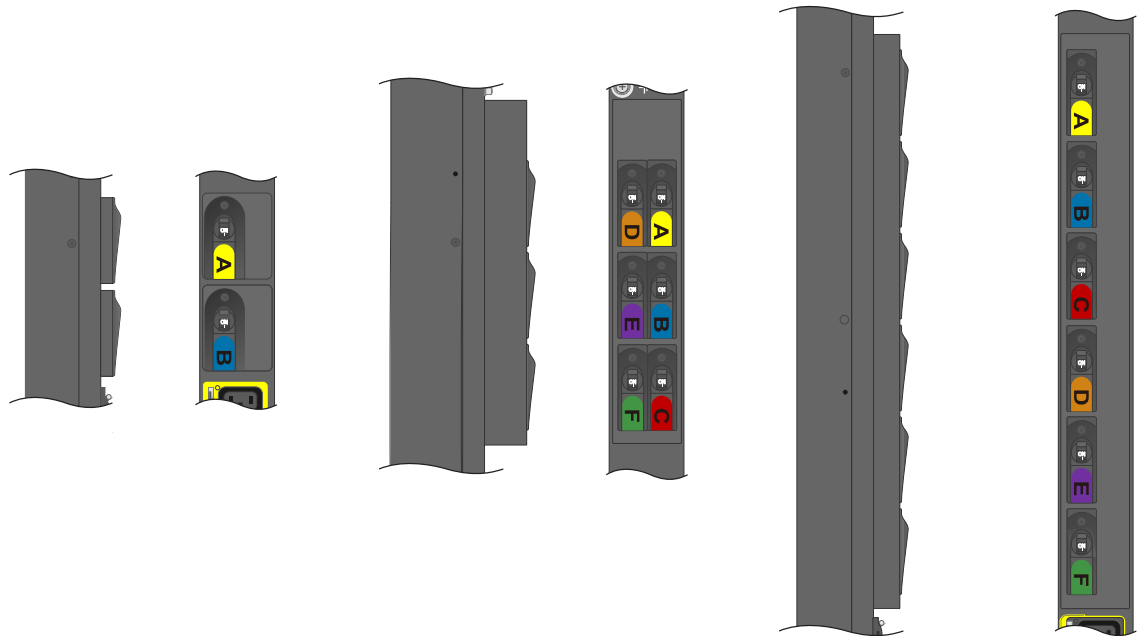


Figure 4. Circuit Breakers

Power Outlets

Each model has a specific configuration of standard IEC 60320 and IEC 60309 outlets.

The outlets are grouped in sets called sections. Outlet sections are preset groups of individual outlets that you can identify and monitor through the different interfaces that are available with the PDU.

The outlets are color-coded and labeled. The circuit breakers that are associated with the outlets have corresponding labels (see Figure 5).

You can connect one device to each outlet. For more information, see “Outlets and Circuit Breakers” on page 43.

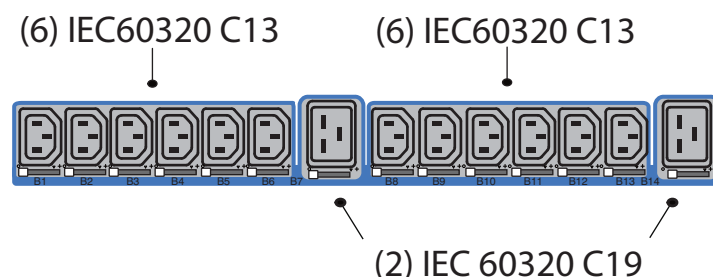


Figure 5. Example Outlet Types

Input Power Cord

Use the input power cords to connect to the power source. Input power cords are permanent for all models.

Accessories

Environmental Monitoring Probe

The Environmental Monitoring Probe (EMP) accessory is optional and must be purchased separately. The optional EMP provides monitoring of external temperature, humidity, and the status of two contact devices, providing greater power management control and flexible monitoring. The EMP has the following features:

- Simplified installation lets you install the EMP safely without turning off power to the PDU or to the devices that are connected to it.
- The EMP monitors temperature and humidity information of any environment, protecting your critical equipment. The EMP measures temperatures between 0°C and 80°C (32°F and 176°F) with an accuracy of $\pm 1^\circ\text{C}$. The EMP measures relative humidity between 10% and 90% with an accuracy of $\pm 5\%$.
- The EMP can be located away from the PDU with a Category 5 network cable up to 20m (65.6 ft) long.
- The EMP monitors the status of two user-supplied contact devices.
- Temperature, humidity, and contact closure status can be displayed through a variety of interfaces.
- User-selectable alarm thresholds let you define acceptable temperature or humidity limits.
- You can use e-mail client software to set up e-mail notification through Simple Network Management Protocol (SNMP) when acceptable alarm limits are exceeded or contact status changes.
- Changes in external contact status are logged in the PDU event history log.
- When temperature and humidity values exceed user-selectable limits, the event is logged in the PDU event history log.



NOTE

For information updates, refer to the Lenovo PDU catalog or go to <http://shop.lenovo.com/us/en/systems/servers/options/systemx/rack-power-infrastructure/power/>.

Features

The Lenovo PDUs provide outstanding performance and reliability, including some or all of these benefits (varies by model):

Ease of Use

- ▮ Easy and flexible rack installation
- ▮ Easy-to-use interface to display input and output status
- ▮ Color-coded outlets and circuit breakers for easy correlation
- ▮ A visual alarm (blinking LED) to indicate outlet current overload
- ▮ User-friendly firmware updates

Communication

- ▮ Comprehensive power management and flexible configuration through a Web browser or a serial connection, a Telnet connection, SNMP, or a console emulator such as HyperTerminal®.
- ▮ Compatibility with Lenovo and third party network management software is facilitated by SNMP protocol or CLI scripts. Lenovo UPS Power Manager (UPM) uses XML to communicate to the PDU.

Power Control Management

- ▮ Control of outlets for Smart PDUs, both collectively and individually
- ▮ The ability to power on, power off, and reboot the devices connected to each outlet
- ▮ Fully shrouded local branch circuit breakers on products rated over 16A (Europe) / 20A (US) to protect connected equipment against overload and short circuits
- ▮ Configuring and monitoring the power schedule of outlets

Monitoring

- ▮ Monitoring of the following:
 - Root Square Mean (RMS) current
 - Crest factor
 - Power factor
 - Maximum and minimum thresholds for current or voltage
 - RMS voltage
 - Active power
 - Apparent power
 - Energy
- ▮ Monitoring of the PDU locally or remotely through a console or network
- ▮ Remote monitoring of connected devices and sensors
- ▮ Daily history report through e-mail
- ▮ Dual color LCD for higher visibility on local alarms

Configurability and Security

- ▮ Configurable alarm thresholds
- ▮ Enterprise security using LDAP or RADIUS

Chapter 2 Safety Warnings

IMPORTANT SAFETY INSTRUCTIONS — SAVE THESE INSTRUCTIONS

This manual contains important instructions that you should follow during installation and operation of the Lenovo Power Distribution Unit (PDU). Please read all instructions before operating the equipment and save this manual for future reference.

DANGER

This PDU contains **HAZARDOUS VOLTAGES**. All repairs and service should be performed by **AUTHORIZED SERVICE PERSONNEL ONLY**. There are **NO USER SERVICEABLE PARTS** inside the PDU. **SYSTEMS SHOULD ONLY BE INSTALLED, TESTED, AND CONFIGURED BY A COMPETENT PERSON. IT IS ESSENTIAL THAT THIS EQUIPMENT IS CONNECTED TO AN ELECTRICAL SUPPLY THAT HAS PROTECTIVE GROUND CONDUCTOR.**

CAUTION

- ▮ To reduce the risk of fire or electric shock, install this PDU in a temperature and humidity controlled, indoor environment, free of conductive contaminants. Do not operate near water or excessive humidity (95% maximum).
 - ▮ Both the room and rack air temperature must be within the operating range of the selected model.
 - ▮ Do not use a two-wire power cord in any product configuration.
 - ▮ Test AC outlets at your computer and monitor for proper polarity and grounding. Use only with grounded outlets at both the computer and monitor.
 - ▮ The installation power outlet used for the power supply to this equipment must be installed near the equipment and must be easily accessible.
 - ▮ When installing this product, it is essential that the distribution circuit supplying the product is protected by a branch circuit protection device with a maximum rating to suit the product maximum rating.
 - ▮ TO ISOLATE THIS EQUIPMENT, DISCONNECT ALL OF THE POWER SUPPLY PLUGS.
 - ▮ This product has been designed to conform to the latest safety requirements. In addition to compliance with standards for general use, it has been factory configured for use in rack mounting environments, aiding the installer in providing systems compliant with relevant standards.
 - ▮ Only use supplied PDU mounting hardware and accessories. If necessary, contact your customer service representative for replacement parts.
 - ▮ This equipment is intended for installation in Restricted Access Locations such as computer rooms, network closets, and equipment racks.
-

**CAUTION**

This product contains a lithium battery on the internal PDU Network Management and Control (eNMC) module:

- ▮ The battery is not user-replaceable. There is risk of explosion if battery is replaced by an incorrect type.
 - ▮ Ensure that used batteries are disposed of according to the instructions. For more information, contact your local recycling/reuse or hazardous waste center for proper disposal information.
-

Chapter 3 Installation

All Lenovo Power Distribution Unit (PDU) models are mounted vertically inside rack structures. Use the information in this chapter to prepare, install, and connect the PDU and optional accessories.

Installation Precautions

Before you install or connect the PDU in a rack cabinet, observe the following precautions:

- Only a competent service person should install, test, or configure the PDU and its optional accessories. It is the installer's responsibility to ensure that the selected product is installed to meet national and local safety regulations.
- Read and understand all warnings and cautions listed in "Safety Warnings" on page 17.
- Review the documentation that comes with your rack cabinet for safety and cabling information. Follow all installation and operation safety information provided.



NOTE

Removing the rack cabinet doors and side panels might make installation easier. See the rack cabinet documentation for more information.

-
- Verify that the room and rack air temperature is within the operating range of the selected model.
 - Take all necessary precautions to handle the weight of the devices.
 - Connect all power cords to properly wired and grounded electrical outlets.



CAUTION

The installation power outlet used for the power supply to this equipment must be installed near the equipment and must be easily accessible.

- Do not overload the power outlet when you install multiple devices in the rack cabinet.
- To reduce the risk of fire, connect only to a circuit provided with branch circuit overcurrent protection with an A (ampere) rating in accordance with the NEC (National Electrical Code), ANSI/NFPA 70 or your local electrical code.
- Verify that all equipment is unplugged from PDU outlets before performing any testing.
- The circuit breaker controls whether there is output power:
 - If the circuit breakers are on, there is output power, the LCD display is on, and the network communications module is operational.
 - If the circuit breakers are off, there is no output power, but the LCD display is on, and the network communications module is operational.
 - To turn off the PDU, unplug it.

Inspecting the Equipment

If any equipment has been damaged during shipment, keep the shipping cartons and packing materials for the carrier or place of purchase, and file a claim for shipping damage. If you discover damage after acceptance, file a claim for concealed damage.

To file a claim for shipping damage or concealed damage: 1) File with the carrier within 15 days of receipt of the equipment; 2) Send a copy of the damage claim within 15 days to your service representative.

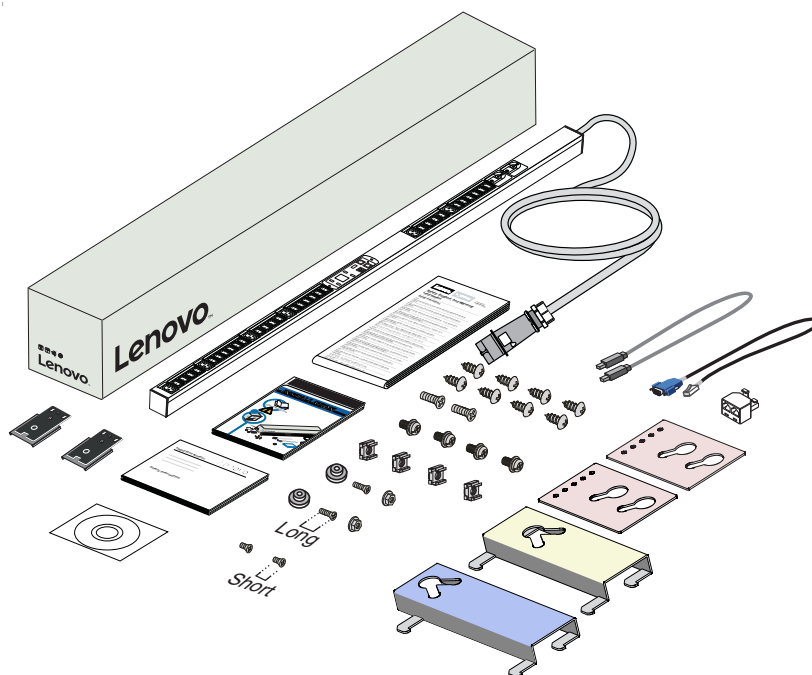


Figure 6. Example Shipping Carton and Contents

Package Contents

Table 2 lists the accessory parts that are included in the shipping carton with the PDUs.

Table 2. Shipped with the PDU in the Shipping Carton

Quantity	Description
1	<i>Lenovo Smart PDU Installation and Connectivity Quick Start</i> 
1	<i>Lenovo Important Notices</i> 

Table 2. Shipped with the PDU in the Shipping Carton (Continued)

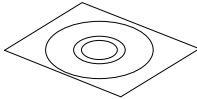
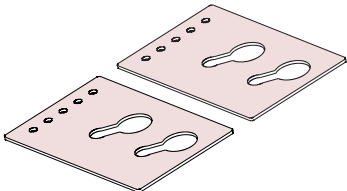
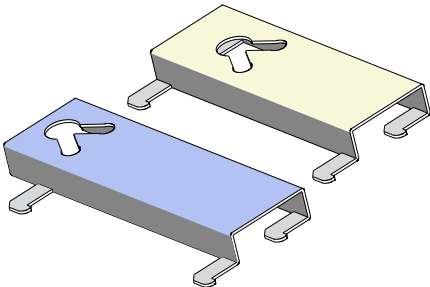
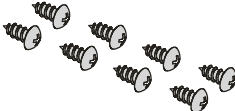
Quantity	Description	
1	<i>Lenovo Safety, Support, and Warranty Information</i>	
1	Lenovo Documentation CD	
2	Brackets for Lenovo Rack 9307	
2	Brackets for Lenovo Rack 9308	
2	Clip Feet	
2	Mounting Buttons	
8	Thread-forming Screws for Lenovo Rack 9307	
2	M6 Flat-head Screws	
4	M6 SEMS Screws	
4	M6 Cage Nuts	

Table 2. Shipped with the PDU in the Shipping Carton (Continued)

Quantity	Description
2	M4 Nuts
2	M4 Flat-head Long Screws
2	M4 Flat-head Short Screws
1	Network Pack for Network-connected models only: (1) Serial cable used for RS-232 connection between the PDU and a PC (1) RJ-45 Cable (60cm - shielded) used for Ethernet or daisy-chain connection between the PDU and a PC SEE NOTE (Americas models only) (1) Y Splitter installed in the Daisy-Chain port and used for daisy-chaining up to eight PDUs together,



NOTE The Ethernet cable is intended for setup or daisy chain.

Optional Environmental Monitoring Probe

Optional Environmental Monitoring Probe (EMP) equipment with sensors can be connected to the PDU as an accessory. The equipment is customer-supplied and should be installed using the manufacturer’s instruction manual.

 IMPORTANT

Follow all installation and operation safety information provided in the manufacturer’s instruction manual for the EMP equipment. Use only supplied accessories.

Installation Overview



NOTE 1 Power cords for the devices that you connect to the PDU are not included.

NOTE 2 Depending on your choice of installation method, some parts may not be used.

NOTE 3 Use only the supplied screws for installation. Hand tighten the screws. Do not overtighten to avoid stripping the screws.

NOTE 4 The mounting button screws are thread forming. When tightening or removing a thread-forming screw initially, the fit may be tighter than usual. A thread-formed aluminum hole must not be used with a different type of screw than the one used initially or it will damage the thread.

NOTE 5 If a square-hole rack is used, cage nuts must be installed.



IMPORTANT

Use great care in handling the PDU during installation. Avoid unnecessary contact between the PDU and the rack.

Tools

The PDU is designed to be mounted without the use of tools. Mounting buttons are pre-installed on the rear of the PDU at the factory. If you wish to use a different mounting option, such as the clip foot or side mounting, tools are not provided, but may be required as follows:

- ▮ Phillips cross-head screwdriver
- ▮ Flat-blade screwdriver
- ▮ 7 mm wrench
- ▮ M6 cage nut insertion tool

Configurations

You can install one or two PDUs on each side of the rack (see Figure 7).

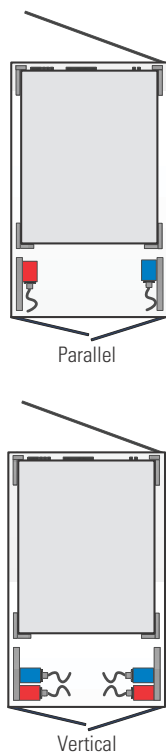


Figure 7. Parallel and Vertical PDU Configurations

IEC Outlet Grip Plug Retention Mechanism

The Lenovo PDUs have a mechanism integrated with the outlets to retain a plug inside its outlet. This system is a lever-actuated grip that prevents the plug from accidentally being bumped out or vibrating out of the outlet. It is not a locking device so the plug can still be removed in an emergency.

To operate the outlet grip plug retention mechanism:

1. Make sure the locking lever is on the "O" position before inserting the plug.
2. Plug in the power cord.
3. Gently rotate the lever to the "+" position. You should hear a "click" sound as the plug retention mechanism engages.
4. To remove the plug, gently rotate the lever to the "O" position. Remove the plug.

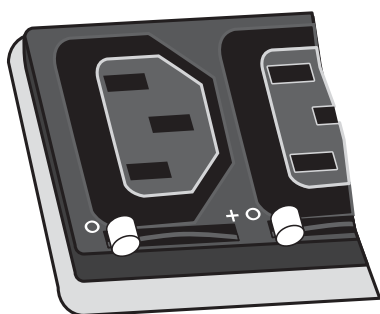


Figure 8. Plug Retention Mechanism



NOTE 1 Only unplug the power cord when the grip plug retention mechanism is in the "+" position in the event of an emergency.

NOTE 2 If you choose, you can further secure the plug with a cable tie.

Installing PDUs in a Rack Cabinet

Regardless of the configuration you choose, there are three mounting methods available for installing the PDU in a rack cabinet:

- Using factory-installed buttons on the PDU to mount the PDU in keyhole openings in the rack frame
- Using buttons on clip feet to mount the PDU in keyhole openings in the rack frame
- Using clip feet and cage nuts secured to the rack to mount the PDU onto the clip

Review the installation methods described in this section and choose the method appropriate for your environment.



NOTE If you need to remove the PDU from clip feet, hold on to the PDU and use a flat-blade screwdriver to unsnap it from the clip.

Using Factory-installed Mounting Buttons (For Lenovo Racks 9360 and 9363 for Example)

To install the PDU with mounting buttons directly attached to the PDU:

1. Carefully move the PDU into position against the rail.
2. Insert the top and bottom mounting buttons into the keyhole slots on the rack post that correspond with the position of the top and bottom mounting buttons.
3. Push down to secure the PDU in position (see Figure 9).
4. Continue to “Grounding the PDU” on page 34 if you are installing a ground screw and grounding cable. Otherwise, go to “Network and Environmental Ports” on page 34.

**NOTE**

The PDU will fit tight and it may require minor force to engage in the slot. This is a friction fit to hold the PDU in the slot.

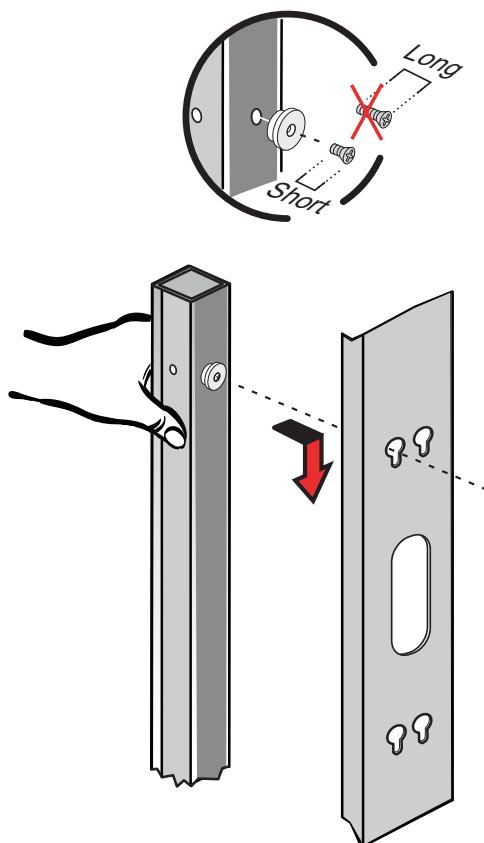


Figure 9. Securing the PDU

Using Mounting Buttons Installed on Clip Feet

To install the PDU with mounting buttons installed on the mounting clip feet:

1. Locate the two mounting clip feet, M4 flat-head long screws (M4×13L), two spare mounting buttons, and M4 hex nuts. Using a Phillips screwdriver and a 7 mm wrench, assemble the mounting buttons and clip feet (see Figure 10).

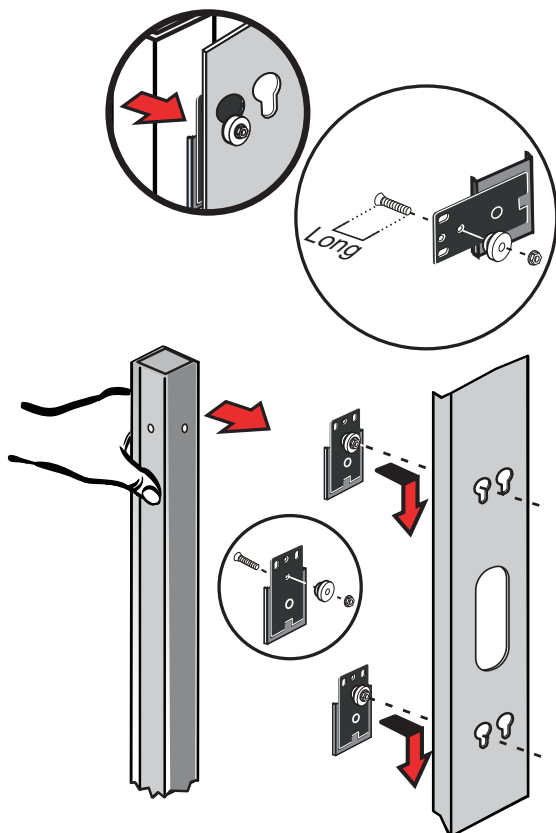


Figure 10. Attaching the Mounting Buttons to the Mounting Clip Feet

2. Mount the two clip assemblies in keyholes spread far enough apart to stabilize the top and bottom of the PDU when mounted on the rail.
3. Carefully move the PDU into position against the rail.
4. Snap the clip feet onto the PDU at the desired vertical position.
5. Align the clip feet and slide the mounting button into the keyhole slots.
6. Push down to make sure the PDU is secured into position.
7. Continue to "Grounding the PDU" on page 34 if you are installing a ground screw and grounding cable. Otherwise, go to "Network and Environmental Ports" on page 34.

Using Clip Feet and Cage Nuts on a Square-hole Rack

**NOTE**

You can install the mounting clip feet vertically or horizontally.

**NOTE**

If a square-hole rack is used, cage nuts must be installed. Use a cage nut insertion tool or a flat-blade screwdriver to install the cage nuts.

To install the PDU with clip feet secured by cage nuts:

1. Locate the cage nuts (supplied).
2. Are you mounting the PDU in line with the rail or away from the rail (offset)?
 - If in line with the rail, go to Step 3.
 - If away from the rail, go to Step 4.
3. **PDU in line with the rail.** Position and lock two cage nuts far enough apart to stabilize the top and bottom of the PDU when mounted on the rail. Insert the cage nuts with a flat-blade screwdriver (see Figure 11).
4. Using two clip feet (supplied) and use flat-head M6 countersunk screws (not supplied), position one mounting clip foot at a cage nut and secure the mounting clip foot to the rail with a screw. Repeat for the second mounting clip. Tighten the screws. Go to Step 8.

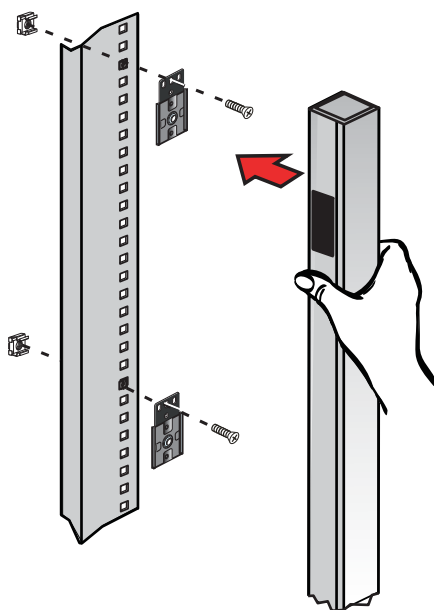


Figure 11. Attaching the Clip Feet and Cage Nuts

5. **PDU away from the rail (offset).** Position and lock two cage nuts far enough apart to stabilize the top and bottom of the PDU when mounted on the rail. Insert the cage nuts into the square rail hole with a flat-blade screwdriver.
6. Locate the two clip feet and four M6 screws (supplied). Turn the straight part of the bracket 90° (see Figure 12).
7. Position one mounting clip foot at a cage nut and secure the mounting clip foot to the rail with a screw. Repeat for the second mounting clip. Tighten the screws.

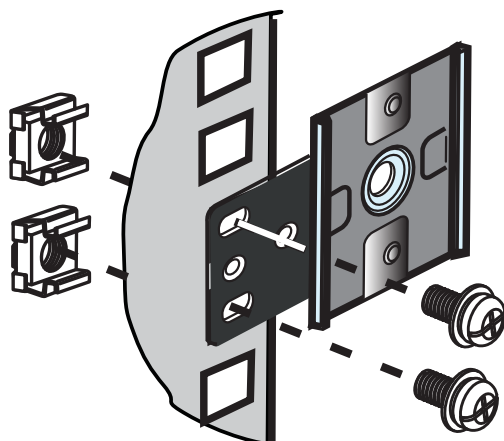


Figure 12. Attaching the Rotated Clip to the Rail

8. Snap the PDU into the mounting clip feet. When you hear a clicking sound for each mounting clip foot, the PDU is secure.
9. Continue to "Grounding the PDU" on page 34 if you are installing a ground screw and grounding cable. Otherwise, go to "Network and Environmental Ports" on page 34.

Using Mounting Brackets for Lenovo Rack 9307

To install the PDU in a Lenovo Rack 9307 using mounting brackets:

1. For each PDU you will install, locate two mounting brackets and eight thread-forming screws.
2. Position the bracket as shown in Figure 13.
3. Attach the bracket to the rack with two thread-forming screws.
4. Repeat for the second bracket.
5. Carefully move the PDU into position against the brackets.
6. Insert the top and bottom mounting buttons into the keyhole slots on the brackets that correspond with the position of the top and bottom mounting buttons.
7. Push down to secure the PDU in position.
8. Continue to “Grounding the PDU” on page 34 if you are installing a ground screw and grounding cable. Otherwise, go to “Network and Environmental Ports” on page 34.



NOTE

The PDU will fit tight and it may require minor force to engage in the slot. This is a friction fit to hold the PDU in the slot.

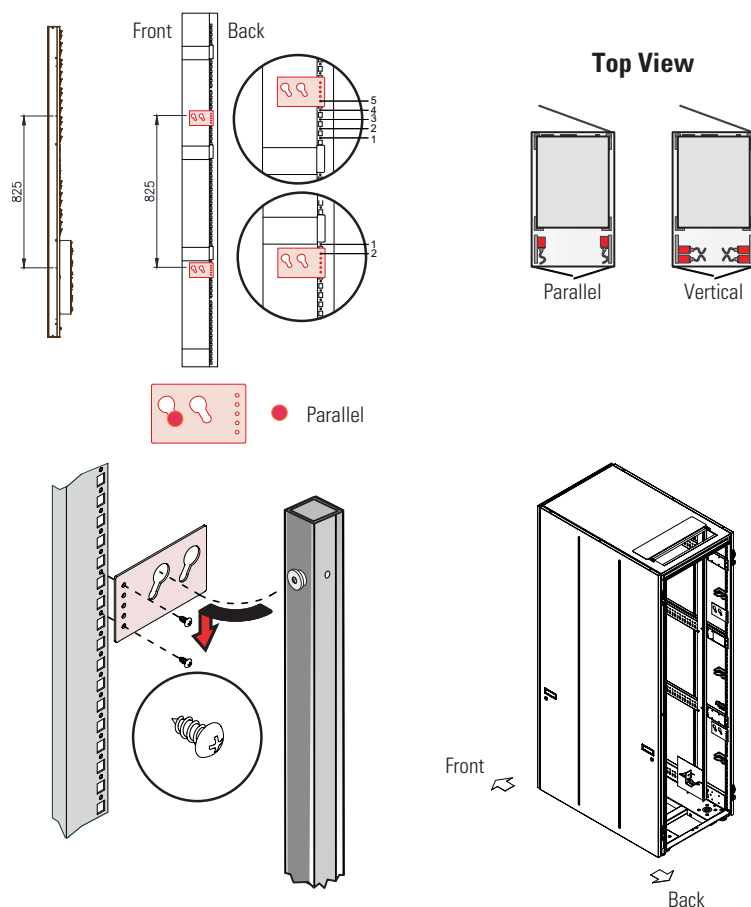


Figure 13. Lenovo Rack 9307 Bracket Installation

Using Mounting Brackets for Lenovo Rack 9308

To install the PDU in a Lenovo Rack 9308 using mounting brackets:

1. For each PDU you will install, locate two mounting brackets.
2. Position and install the brackets as shown in Figure 14.
3. Carefully move the PDU into position against the brackets.
4. Insert the top and bottom mounting buttons into the keyhole slots on the brackets that correspond with the position of the top and bottom mounting buttons.
5. Push down to secure the PDU in position.
6. Continue to “Grounding the PDU” on page 34 if you are installing a ground screw and grounding cable. Otherwise, go to “Network and Environmental Ports” on page 34.



NOTE

The PDU will fit tight and it may require minor force to engage in the slot. This is a friction fit to hold the PDU in the slot.

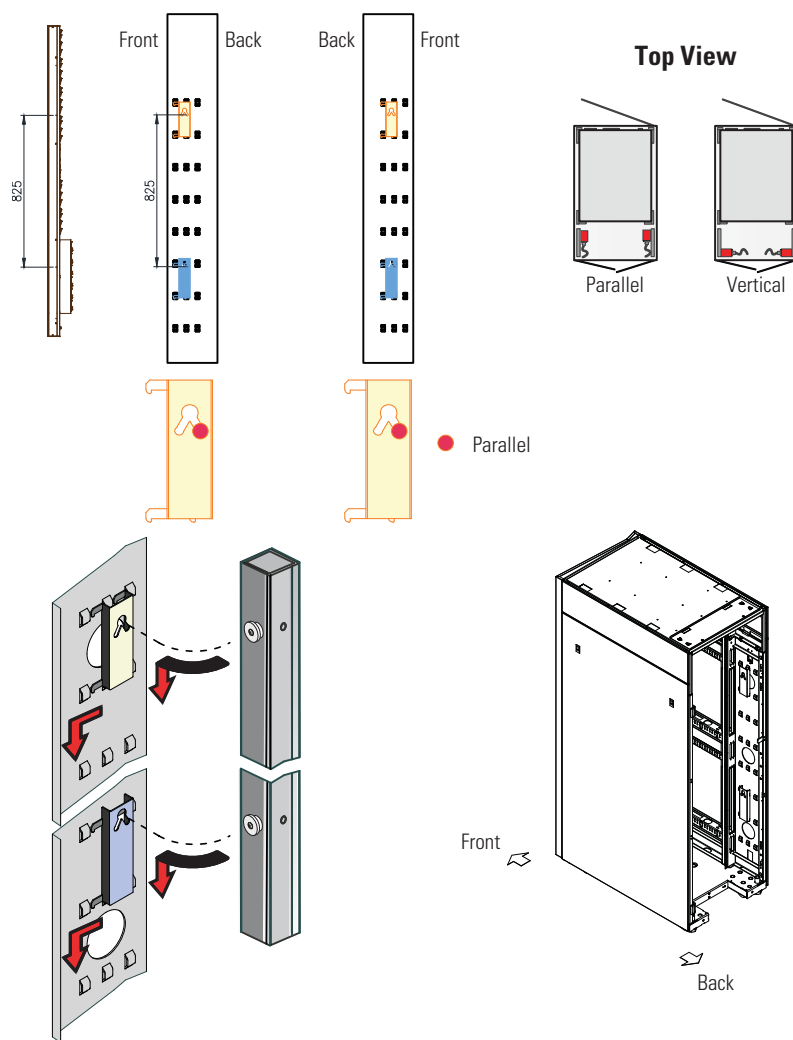


Figure 14. Lenovo Rack 9308 Bracket Installation

Using Mounting Buttons for Lenovo Rack 9360

To install the PDU in a Lenovo Rack 9360 using mounting buttons:

1. For each PDU you will install, locate two mounting buttons and two M4 flat-head short screws.
2. Position and install the buttons as shown in Figure 15.
3. Carefully move the PDU into position against the rail.
4. Insert the top and bottom mounting buttons into the keyhole slots on the rack post that correspond with the position of the top and bottom mounting buttons.
5. Push down to secure the PDU in position.
6. Continue to “Grounding the PDU” on page 34 if you are installing a ground screw and grounding cable. Otherwise, go to “Network and Environmental Ports” on page 34.



NOTE

The PDU will fit tight and it may require minor force to engage in the slot. This is a friction fit to hold the PDU in the slot.

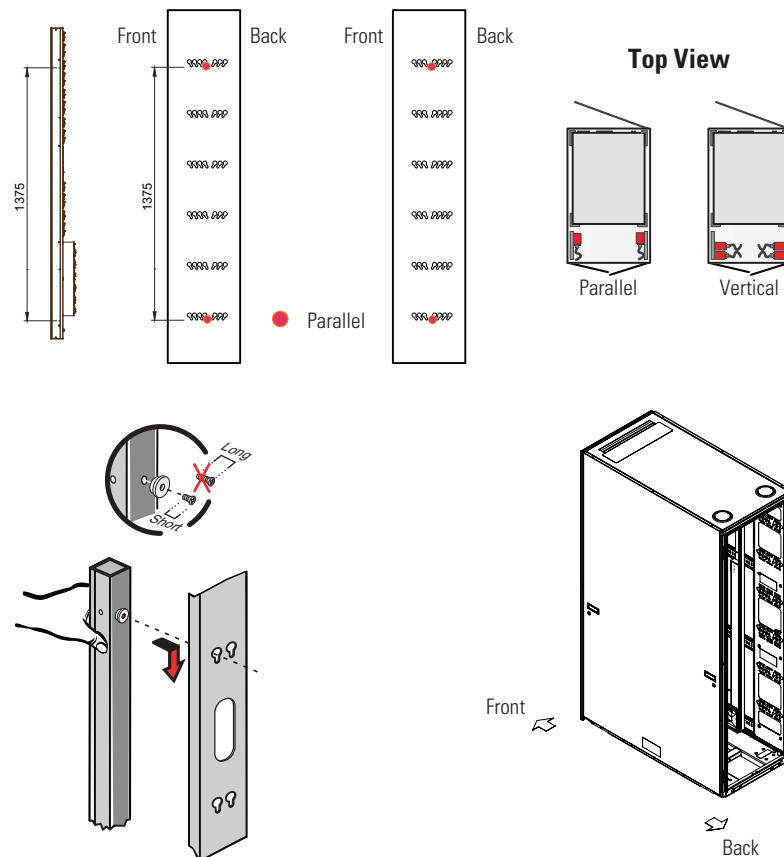


Figure 15. Lenovo Rack 9360 Mounting Button Installation

Using Mounting Buttons for Lenovo Rack 9363

To install the PDU in a Lenovo Rack 9363 using mounting buttons:

1. For each PDU you will install, locate two mounting buttons and two M4 flat-head short screws.
2. Position and install the buttons as shown in Figure 16.
3. Carefully move the PDU into position against the rail.
4. Insert the top and bottom mounting buttons into the keyhole slots on the rack post that correspond with the position of the top and bottom mounting buttons.
5. Push down to secure the PDU in position.
6. Continue to “Grounding the PDU” on page 34 if you are installing a ground screw and grounding cable. Otherwise, go to “Network and Environmental Ports” on page 34.



NOTE

The PDU will fit tight and it may require minor force to engage in the slot. This is a friction fit to hold the PDU in the slot.

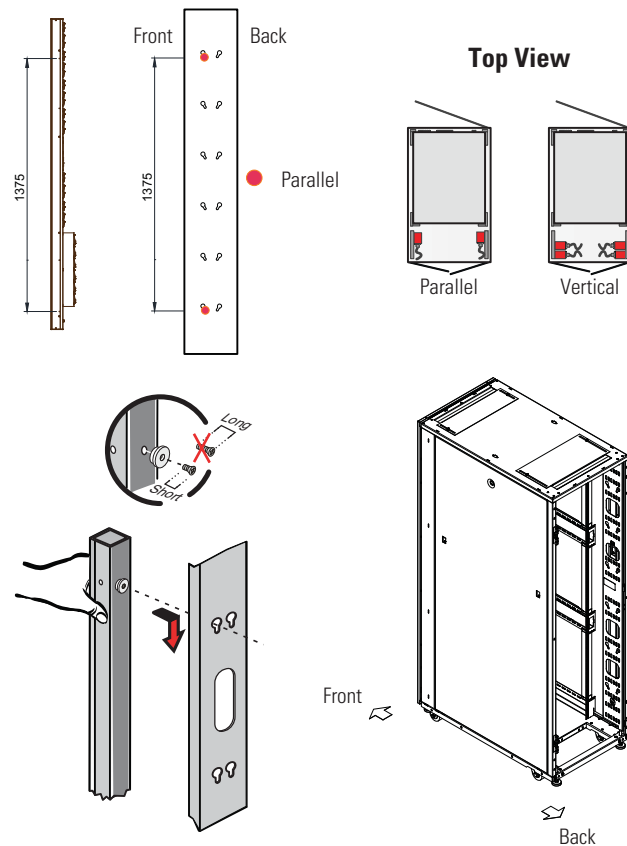


Figure 16. Lenovo Rack 9363 Mounting Button Installation

Grounding the PDU

**NOTE**

Grounding the PDU is optional but recommended.

The PDU is grounded through the input plug and an M6 ground screw is provided for auxiliary rack grounding. Conductors can be connected to the ground screw for functional grounding or bonding of ungrounded metal parts within the rack. The grounding screw is sized to safely conduct the fault current of the single largest output breaker. There is no paint on the screw or the chassis surface to ensure contact with bare metal instead of a painted surface. The ground symbol is impressed in the chassis above the earth bonding screw.

To ground the PDU, connect a grounding cable (not supplied) from earth to the grounding screw shown in Figure 17. The internal diameter of the ground strap ring is M6 (6 mm).

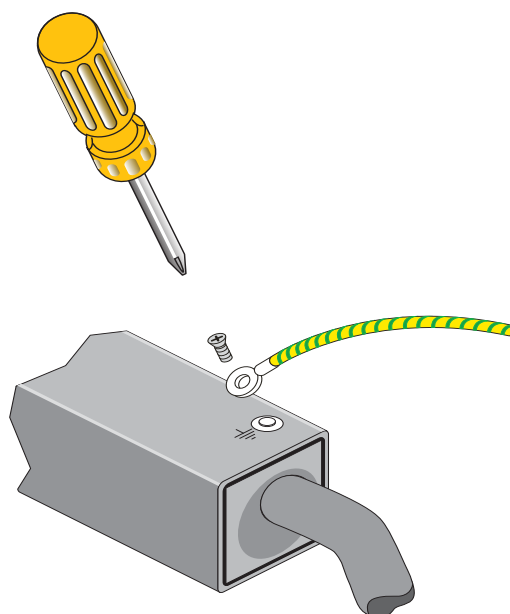


Figure 17. Grounding Screw Location

Network and Environmental Ports

The PDU provides four types of ports for network connectivity and environmental sensor monitoring.

- ▮ To connect the PDU to a serial port on a computer, go to the next section, “Connecting to a Computer Serial Port”.
- ▮ To connect the PDU to a 10/100 MB Ethernet-capable port and the Local Area Network (LAN), go to “Connecting to a LAN Ethernet Port” on page 36.
- ▮ To daisy-chain PDUs, go to “Connecting Multiple PDUs in a Daisy Chain” on page 36.
- ▮ To connect the PDU to EMP equipment, go to “Connecting Optional Environmental Monitoring Probe Equipment” on page 38.

Connecting to a Computer Serial Port

Connecting the PDU to a computer allows communication through a serial connection.

To connect the PDU to a computer:

1. Verify that the computer has a communication program such as HyperTerminal, Telnet, or SSH.
2. Locate the DB9-to-RJ-45 cable (supplied).
3. Connect the RJ-45 end of the cable to the RS-232 connector on the front panel of your PDU model (see Figure 18). Connect the DB9 end of the cable to the serial connector on the computer.

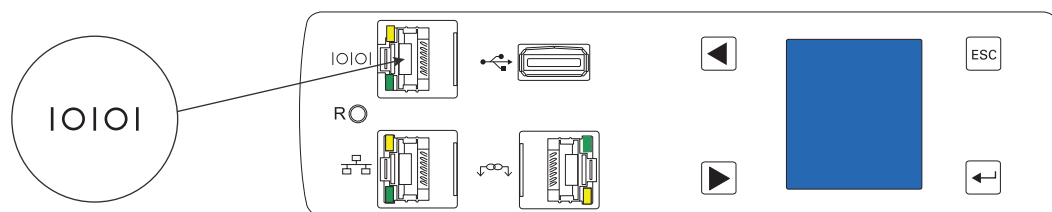


Figure 18. Connecting to a Computer Serial Port



NOTE

If your computer does not have a DB9 serial connector, obtain a DB9-to-USB converter. Follow the manufacturer's instructions to install the converter cable device drivers and to connect the converter cable to your computer.

Connecting to a LAN Ethernet Port

Connecting the PDU to a LAN provides communication through an Internet or Intranet connection. You can monitor the PDU from any computer connected to the same network. (The network card is 10/100 MB-compatible.)

To connect the PDU to a LAN:

1. Locate the Ethernet cable (supplied).



NOTE

A network cable is supplied in the network accessory pack. This cable is useful for setup or can be used where the network switch is in close proximity to the PDU. Any standard network cable can be used if longer lengths are needed.

2. Connect one end of the cable to the Ethernet connector on the PDU (see Figure 19). Connect the other end of the cable to the Ethernet connector on the router (or other LAN device).

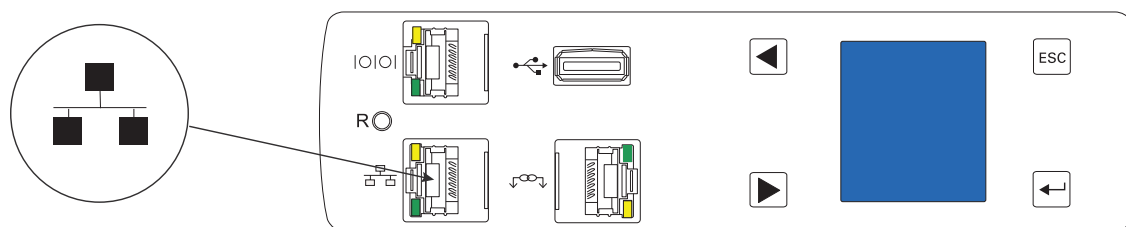


Figure 19. Connecting the PDU to a LAN

Connecting Multiple PDUs in a Daisy Chain

Two to eight PDUs can be chained together using an Ethernet cable between the Daisy-Chain ports located on the front panel. Daisy chain uses Eaton's patented RS-485 daisy chain (strapping) technology. This allows access to the PDU data of multiple PDUs from the same network connection. One PDU is defined as the Host. This is the PDU with a connection to the network. The other PDU (or PDUs) are Device(s).



NOTE

You should connect the daisy-chained group only to the PDU defined as the Host.

To physically connect PDUs in a Daisy Chain:

1. Locate an Ethernet cable or cables (one cable is supplied).

NOTE

When daisy-chaining PDUs, observe the following:



- ▮ For two PDUs, you do not need a splitter.
- ▮ For three or more PDUs, you use Y splitters.
- ▮ The maximum distance between units is 5m (16 ft). For example, when connecting one host and seven devices, this means that the total maximum distance between the first and last PDUs is 35m (115 ft).

2. How many PDUs are you daisy-chaining?
 - If daisy-chaining two PDUs (1+1), go to Step 3
 - If daisy-chaining three PDUs or more (2+1 to 7+1), go to Step 5
3. Connect one end of the cable to the Daisy Chain connector on one PDU. Connect the other end of the cable to the Daisy Chain connector on the other PDU as shown in Figure 20.
4. Go to Step 7 to configure the daisy-chained PDUs.

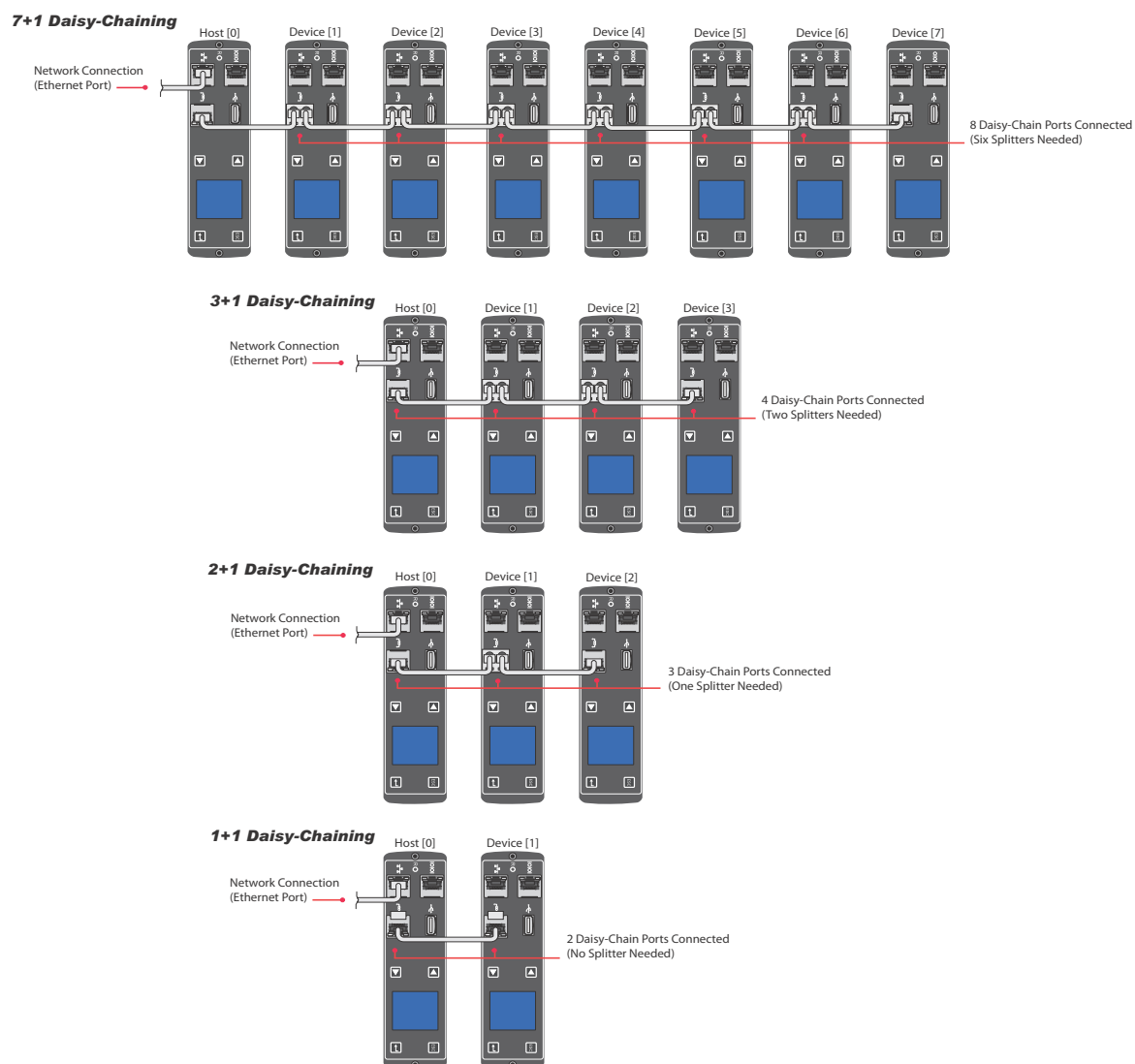


Figure 20. Locating the Daisy Chain Connector

5. Insert a Y splitter in the Daisy Chain connector for all PDUs between the Host and the last PDU in the chain, as shown in Figure 20 and Figure 21.
6. Go to Step 7 to configure the daisy-chained PDUs.

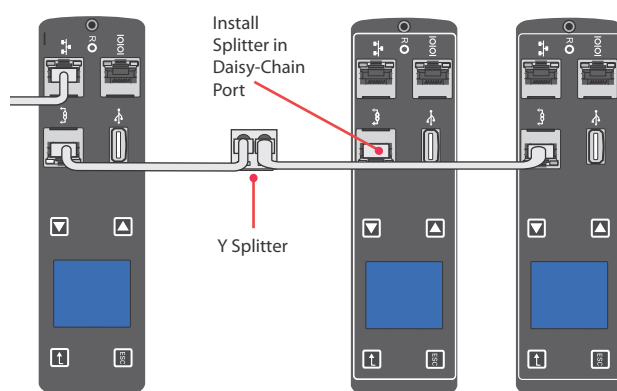


Figure 21. Y Splitter in Daisy-Chain Port (2+1 Daisy-chaining Shown)

7. Choose to configure the PDUs with either the LCD interface or the CLI interface:
 - To configure the PDUs using the LCD interface, go to “Daisy Chain Submenu” on page 69.
 - To configure the PDUs using the CLI interface, go to “Set Daisy Chain” on page 82.

NOTE You can monitor the PDUs with either the CLI interface or the Web interface.



- To monitor the PDUs using the Web interface, go to “Web Interface Operation” on page 84.
 - To monitor the PDUs using the CLI interface, go to “Get Daisy-chained PDU to Supervise or Retrieve Communication Status” on page 80 in the CLI Interface chapter.
-

Connecting Optional Environmental Monitoring Probe Equipment

You can purchase optional EMP equipment to monitor temperature and humidity around the PDU and to monitor the status of sensors.

You can install an optional EMP now or after completing the PDU installation and startup. Optional EMP equipment can be installed without turning off power to the PDU or the devices connected to it.



IMPORTANT

Follow all installation and operation safety information provided in the manufacturer’s instruction manual for the EMP equipment.

To install an optional EMP:

1. Locate the EMP and the Ethernet cable (supplied).
2. Refer to the manufacturer’s installation manual for instructions to connect the external contact inputs to the optional EMP for the external contact devices you plan to monitor.
3. Locate the Ethernet cable dedicated to the EMP. Connect one end of the cable to the RJ-45 connector on the EMP, then connect the other end of the cable to the serial connector on the PDU (see Figure 22).

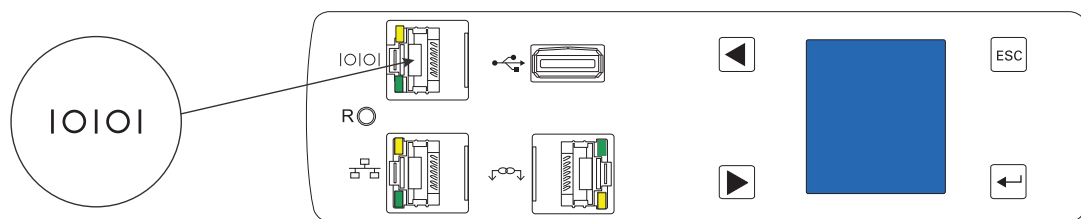


Figure 22. Connecting the EMP to the PDU RJ-45 Serial Port Connector



NOTE If you install an EMP, the PDU serial port must be dedicated to the EMP.

4. Use the mounting method appropriate to your installation to mount the EMP in a convenient location anywhere on the rack.
5. If desired, use cable ties to secure the Ethernet cable out of the way as needed.
6. On startup, the PDU automatically recognizes the EMP.

Connecting the Output Devices

The PDU outlets are available for connecting and monitoring devices such as workstations, servers, and switches. Connect a device you want to monitor to a power outlet on the PDU with the power cord that comes with the device.



NOTE You may find it useful to document the connections you make.

To connect your devices:

1. Verify that each circuit breaker is in the On position.
2. Route the PDU power cord toward a dedicated power source. If desired, use cable ties to secure the power cord as needed. If the power cord must exit the rack cabinet to connect to a power source, use the openings in the rack cabinet.



NOTE 1 Plug the PDU into an appropriately rated outlet for its type.

NOTE 2 Do not replace or rewire the power cord.

3. Connect the power cord to a properly wired and grounded dedicated power source. The PDU turns on and displays the Lenovo startup screen while starting. After five seconds, the sequence of LCD screensaver screens for this PDU model begin cycling.
4. Verify that no alarms display on the LCD. To resolve alarms, see “Maintenance and Alarms” on page 127.
5. If your model uses grip plug retention levers on the outlet plugs, make the lever in the “O” position before inserting the plug.

6. Connect your output devices to the outlet outlets on the PDU. Verify that each device is receiving power before connecting the next device.

**NOTE**

To avoid large surge currents, connect the protected equipment to the outlets individually rather than as a group. You may want to include a delay for Smart models when setting up groups of outlets to start at the same time to avoid a large in-rush current.

7. If your model uses grip plug retention levers, gently rotate the lever to the “+” position. You should hear a “click” sound as the mechanism engages.

**NOTE**

Only unplug the power cord when the grip plug retention mechanism is in the “+” position in an emergency. To remove the plug, gently rotate the lever to the “O” position and remove the plug.

8. Route all power cords neatly. If desired, use cable ties to secure the cords.

Operating the PDU

See “Operation Overview” on page 41 for instructions to operate the PDU, including starting and shutting down the equipment.

Chapter 4 Operation Overview

This chapter describes the Lenovo Power Distribution Unit (PDU) operation overview.

Operation Interfaces

You can configure and manage the Smart PDU through a local interface (onboard the PDU) or through remote interfaces (through the network):

- **Configure.** Basic configuration is available for some settings through the LCD menu onboard the PDU. Full configuration of all settings is available through the remote Web and Command Language Interpreter (CLI) interfaces.
- **Manage.** You can use the Web interface to monitor the PDU and manage outlets and groups of outlets. Outlets that are in the same user-defined group can be turned on, turned off, rebooted, and scheduled to perform actions in a synchronized manner.

Local Operation Interface

The LCD provides information about the PDU and connected devices using white text on a blue background. The LCD display flashes red when any alarm is active.

The LCD display orientation can be changed using an LCD or CLI setting. The display can be rotated 90°, 180°, or -90° (270°). See “Display Submenu” on page 68 or see Example 2 in “set command” on page 80 for more information.

LCD Display

The LCD display has three modes:

- **Screensaver Mode** (startup screen)
Screensaver mode cycles through a set sequence of screens that display current PDU values. Current values are refreshed every five seconds. The user cannot select a custom sequence of screens.
- **Energy Saving Mode**
This mode is activated manually. The backlight is turned off to conserve energy. The screen darkens. The screen reactivates when any button is pushed or when an active alarm occurs.
- **LCD Main Menu Mode**
The settings that display under each high level (main) menu depend on your PDU model.

Status Display

When the screensaver is activated, it displays a set of up-to-date values. However, this set of values is not user-configurable. To selectively view values, navigate through the LCD interface using the buttons on the front panel.

For example, selecting PDU from the Meter submenu and then selecting Total Input from the PDU Meter submenu displays total input values for the PDU. Figure 23 is an example of the display for a 1Ph PDU.

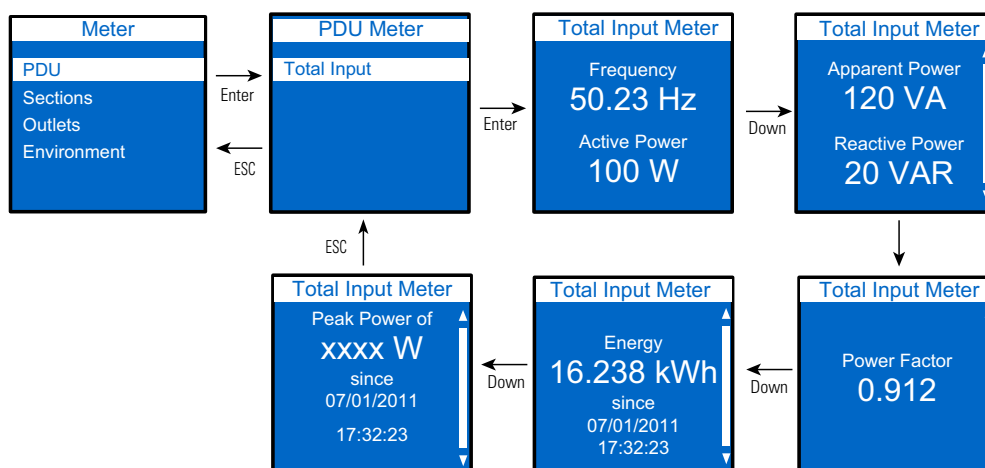


Figure 23. Example of Selected Value Display

Main Menu Display

The menu items are highlighted when they are selected. The resulting screens can include data displays, value setting options, or submenus. Figure 24 illustrates the highlighted Active Alarms LCD menu item selection.

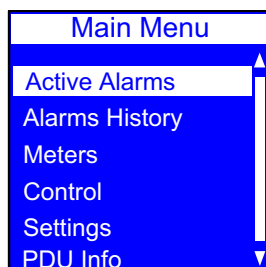


Figure 24. Menu Item Selection

See "LCD Interface Operation" on page 52 for detailed operation information.

Remote Operation Interfaces

You can communicate with the PDU using the remote interfaces listed in Table 3.

Table 3. Remote Interfaces

Interface	Description	PDU Connector	Cable (supplied)	Cabling Instructions
Web browser	PDU management interface through an Internet Web browser*	Ethernet connector	Ethernet cable	"Connecting to a LAN Ethernet Port" on page 36
SNMP	Standard Internet protocol for managing devices on networks**			
Telnet Command Line Interface (CLI)	Terminal emulation protocol for accessing the CLI via Ethernet to configure the eNMC module			
Console emulator CLI	Serial interface for accessing CLI directly from a computer	Serial connector ***	DB9-to-RJ-45 cable	"Connecting to a Computer Serial Port" on page 35

* Supports Microsoft® Internet Explorer® 8.0 and greater, Mozilla® Firefox®, Google Chrome™.

** Supports Simple Network Management Protocol (SNMP) v1, v2, and v3. Provides the ability to send traps, retrieve outlet specific data, set PDU and outlet values, and notify of events through SNMP trap or e-mail alert.

*** If you install an optional EMP, you must dedicate the serial connector to the EMP. (The EMP Ethernet cable is supplied in the EMP shipping carton.)

Outlets and Circuit Breakers

A variety of outlet types are available for the Lenovo PDUs. Each PDU model has a specific configuration of outlets. The configuration can be standard or customized to suit your needs.

The outlets are grouped in sets called sections. Sections are preset groups of individual outlets that you can identify and monitor through the interfaces that are available with your particular type of PDU.

The outlets are color-coded and labeled. The circuit breakers that are associated with the outlets have corresponding labels (see Figure 25). (The "circuit breaker tripped" status is not reported.)

Outlets and sections of outlets can be managed through the Web Interface (see "Outlets" on page 102, "Outlets" on page 102, and "System" on page 111). You can see measurement readings using the local LCD interface.

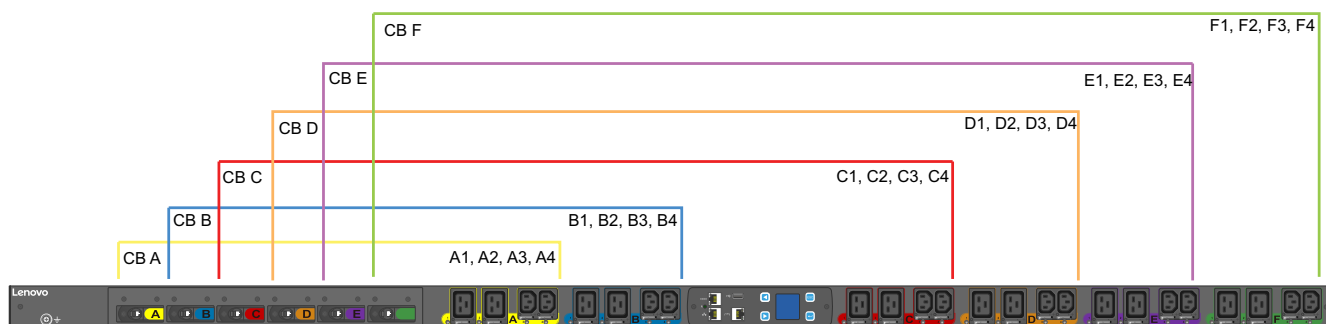


Figure 25. Outlet Groups and Circuit Breakers

Ports, Operation Buttons, and LED Status Indicators

The Lenovo PDUs include communication and serial ports (also used for environmental sensor monitoring), operation buttons, and status LEDs (see Figure 26). The PDU front panel includes communication and monitoring ports, LED status indicators, and operation buttons. The ports and the associated LED indicators are described in the following Table 4.



NOTE

At startup, check the LED status display colors on the communication and monitoring ports to ensure that they are operating correctly.

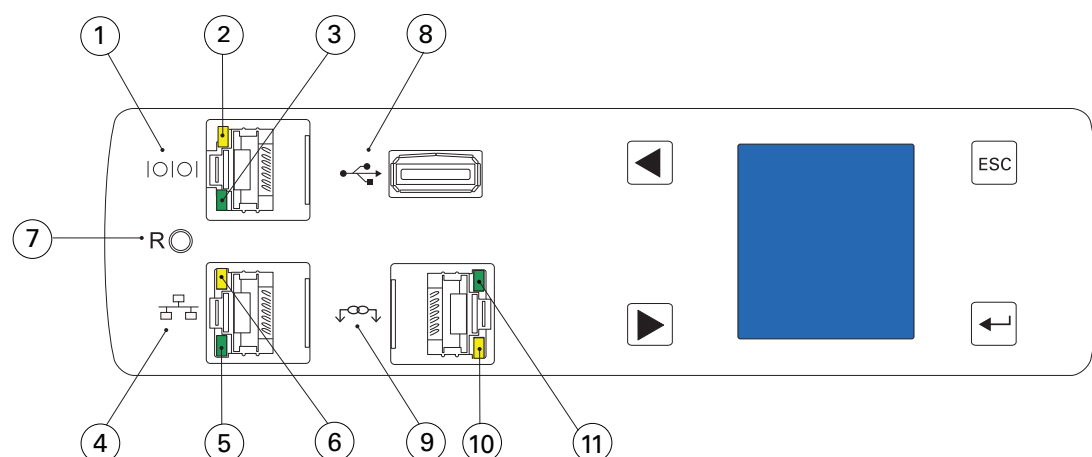


Figure 26. Communication and Serial Ports

Table 4. Communication and Environmental Sensor Monitoring Ports

Diagram Reference Number	Description
1	Serial or Environmental Sensor Monitoring (EMP) Port
2	Yellow Serial/EMP Port LED: RS-232 Operation and Activity Status OFF: No EMP connected FLASHING: EMP connected
3	Green Serial/EMP Port LED: PDU Communication Status OFF: PDU start-up in progress FLASHING: eNMC module operational
4	Ethernet 10/100 Base-T Port
5	Green Ethernet Port LED: Operation Transfer Rate Status OFF: Port operating at 10 Mbps/s ON: Port operating at 100 Mbps/s
6	Yellow Ethernet Port LED: Connection and Transmission Activity Status OFF: PDU not connected to the network ON: PDU connected to the network, but no activity FLASHING: Port is sending or receiving (transmission active)
7	Reset Button NOTE To restart the eNMC, insert a probe and press the button for 3 seconds (or until the LCD goes blank). This does not reset power to the outlets.
8	USB Port: Used for firmware upgrade and configuration file download/upload

Table 4. Communication and Environmental Sensor Monitoring Ports (Continued)

Diagram Reference Number	Description
9	Daisy-Chain Port
10	Yellow Daisy-Chain Port LED: Transmission Activity Status FLASHING: PDU is transmitting data
11	Green Daisy-Chain Port LED: Role Assignment in Communication Protocol ON: Device FLASHING: Host

Operation Concepts

This section provides information describing the following PDU operation concept:

- User login and access policy

For more information, see “Access Privileges” on page 90.

User Login and Access Policy

The web interface is protected by a login and a password. The PDU Network Management and Control (eNMC) module manages up to eight users and one Administrator.

A user is defined by:

- Name identifier (login)
- Password (minimum of five characters)
- Assigned access rights (Read Only, Read/Write, Read/Write/Control, No Access)
- List of groups of outlets to which the user has access



NOTE

At a minimum, users need Read-Only access rights to access the Web pages.

When a user accesses the Web interface, the system prompts for a login and password. The login and password for the administrator and for each user are hashed using a one-way hash algorithm. If the login and password match and the assigned user rights do not restrict access, the user can access the Web interface.



IMPORTANT

Users should always terminate sessions by clicking the logout link in the top right-hand corner of the Web interface page.

Common Operations

Starting the PDU

**NOTE**

The Lenovo PDUs have no power switch.

To start up the PDU, verify all circuit breakers are in the On position.

**IMPORTANT**

To power cycle the Lenovo PDU, remove the power cord from the power source and then plug it back in.

Shutting Down the PDU

To shut down the PDU:

1. Shut down the connected devices according to the manufacturer's recommended shutdown sequence.
2. Turn each circuit breaker to the Off position.
3. To remove power from the PDU completely, disconnect the PDU power cord from the power source.

Restarting the PDU Network Management and Control (eNMC) module

You can restart the communications module using either a hardware or software method.

**IMPORTANT**

Restarting the eNMC module will not affect the output power or the connected equipment.

A software restart is triggered from the Serial interface or Web interface upon user action (see Figure 27). This method is typically the better choice because all current settings in the communications module file system are saved before restarting.

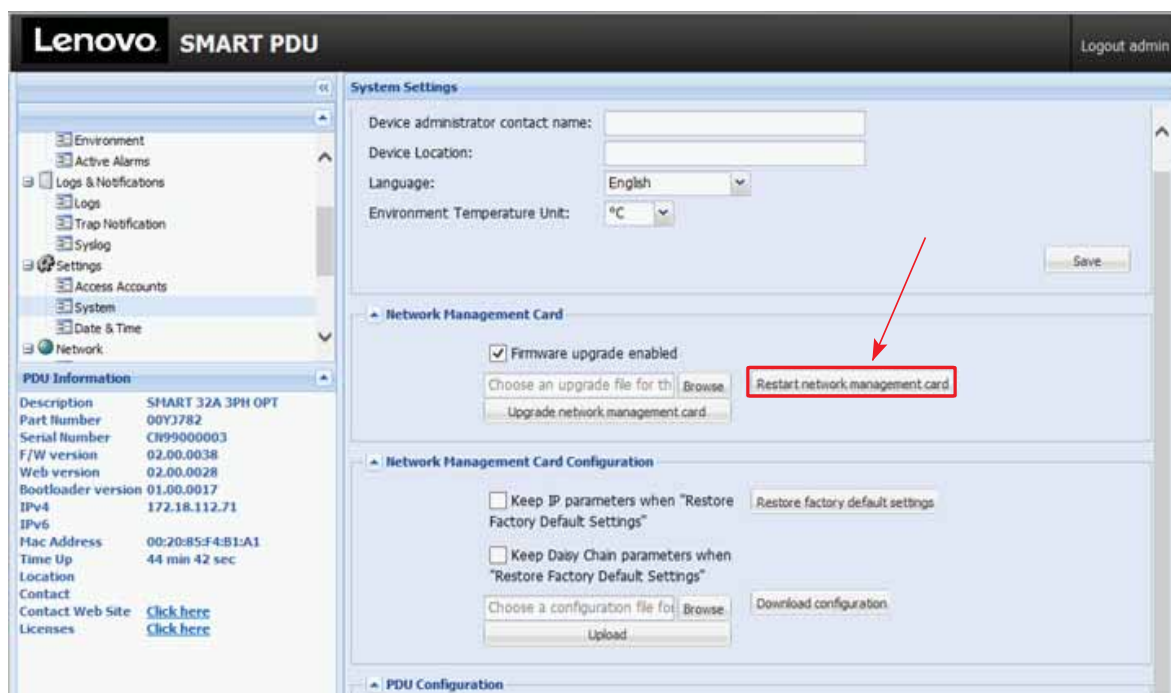


Figure 27. Reset the eNMC Module from the Web Interface

For a hardware restart, locate the Reset opening (labeled R) on the PDU (see Figure 28). Insert a probe, press the recessed button, and retract the probe. This method is not necessarily the best choice because the communications module does not force the system to save the parameters in the file system before restarting.

The H/W restart button does not affect PDU outlet status. The energy consumption is still recorded during the reboot of the eNMC module.



NOTE

When using a hardware restart to restart the eNMC module, there is no mandatory check to ensure that the file system parameters are saved before restarting.

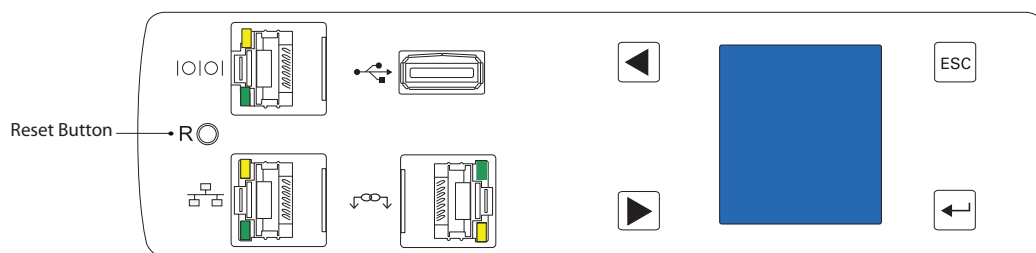


Figure 28. Reset Button

Chapter 5 Network Communication Configuration

The Lenovo Power Distribution Unit (PDU) automatically collects the network communication configuration settings (IP parameters) from the server by default. When the PDU is not connected to the network, it continuously attempts to connect. If DHCP is enabled on your network, the PDU automatically collects the network communication configuration settings.

In order to establish a network session, note the network configuration from the LCD. Users with PDU User and Admin privileges can review and change the network information using Command Line Interface (CLI), Telnet, and graphical user interface (GUI) once connected.



NOTE

In order to use Telnet, you must have a network connection already established.

The PDU defaults to using Dynamic Host Configuration Protocol (DHCP) when delivered. If you are unable to connect to the PDU through the network connection with this default address, change the IP address using the LCD or through the CLI using a terminal emulation program.

The network connection automatically receives an IP address through the DHCP if available on the network. If DHCP is enabled but a DHCP server is not available, the eNMC module will use the last-used IP address setting. Alternately, it is possible to set a static IP address by using either the LCD menu or a serial connection command line interface (CLI).

The default settings are:

- DHCP: Enabled
- IP Address: 192.168.123.123
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.123.1
- Username: USERID
- Password: passw0rd



NOTE

If you use the default IP address and are able to make a direct connection, you could use Telnet to change the settings to some other fixed values.

LCD — DHCP

1. The PDU defaults to DHCP enabled when delivered.
2. Connect to a network that has a DHCP server and wait 20 seconds before the eNMC module reboots with the new IP address.
3. After 20 seconds, obtain the IP address from the LCD home screen (see Figure 29).



Figure 29. LCD Home Screen

LCD— Static IP address

- 1. Disable DHCP (see Figure 30).

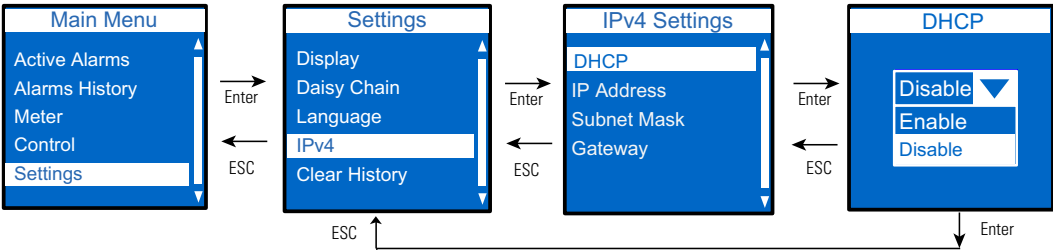


Figure 30. Disable DHCP

- 2. Set the static IP address (see Figure 31). Wait 10 seconds.

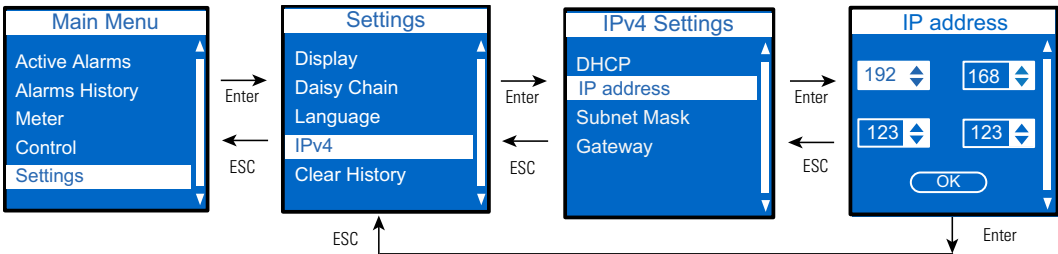


Figure 31. Set the Static IP Address

- 3. After 10 seconds, use the reset button to restart the eNMC module and apply the new settings (see Figure 32).

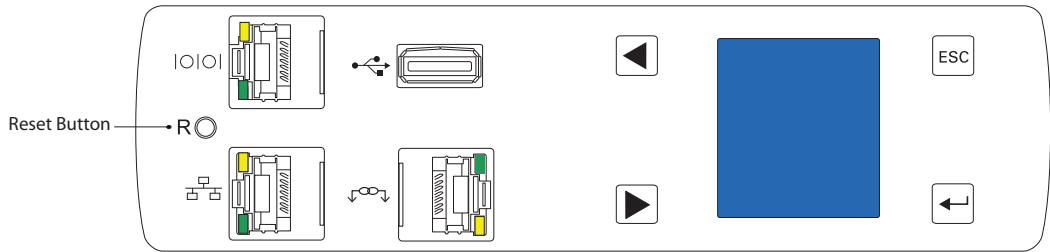


Figure 32. Reset Button

Serial connection — Static IP address

Use the RJ45-to-DB9 serial cable that is provided to connect the computer to the PDU. If your computer does not have a DB9 (RS-232) connector, a USB-to-RS-232 adapter can be purchased separately. Access the CLI using a terminal emulation program such as HyperTerminal, PuTTY, or TeraTerm.

To set up the serial port using your selected terminal emulation program, use the following settings:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: None

After establishing a serial connection, perform the following steps:

1. In the terminal emulator session window, enter the default user name (USERID) at the login prompt. For example:

```
Enter Login: USERID
```

```
Enter Password:
```

2. Type passw0rd (default) at the password prompt. Press Enter. The CLI uses a “get” command to return the value of a setting and a “set” command to change the value of a setting. For example:

```
PDU#0>set System.Network.DHCP 0
```

```
PDU#0>get System.Network.DHCP
```

```
0
```

3. Type set System.Network.DHCP 0 and press Enter to modify the value (0 = disabled and 1 = enabled). For example:

```
PDU#0>set System.Network.DHCP 0
```

```
0
```

4. Set the IP address to a value provided by your system administrator.

```
PDU#0>set System.Network.IPAddress xxx.xxx.xxx.xxx
```

```
xxx.xxx.xxx.xxx
```

5. If necessary, set the network Subnet Mask to the value required by your system administrator.

```
PDU#0>set System.Network.IPMask 255.255.yyy.yyy
```

```
255.255.yyy.yyy
```

6. Set the network Gateway to the value required by your system administrator.

```
PDU#0>set System.Network.IPGateway zzz.zzz.zzz.zzz
```

```
zzz.zzz.zzz.zzz
```

7. Wait 10 seconds. Use the reset button to restart the eNMC module and apply the new settings.

NOTE 1 You can also connect up to eight PDUs together using the Daisy-Chain port and an RJ-45 splitter (provided). This enables multiple PDUs to communicate over one Ethernet port.



NOTE 2 If you choose not to use the procedure to configure the communications module without the DHCP server installed, you can connect to the PDU using the default address: ***http://192.168.123.123***

Verify Web Operation After Configuration

To verify the communications module is operational and that you can access the Web interface:

1. Open a Web browser.
2. Enter the IPv4 or IPv6 address in the address bar in the following format:
http://<IPv4 address> or **http://<IPv6 address>**
3. When the user authentication pop-up dialog displays, type **USERID** in the User name field and **passw0rd** in the Password field.
4. The home page opens with the PDUOverview page.

Chapter 6 LCD Interface Operation

This chapter contains operation information for the Lenovo Power Distribution Unit (PDU), including:

- ▮ LCD display and control button functions
- ▮ Menu selections



NOTE

The LCD language is configurable. See language settings in “Language Submenu” on page 72.

LCD Display and Control Buttons

The PDU has a four-button, graphical LCD display (see Figure 33). Use the control buttons to change the screen display, retrieve specific performance data, or change configuration values. The display view can also change automatically. For example, the display changes to show active alarms as they occur, or particular displays update due to a change in operating state.

A backlight is used to light up the display with white and blue:

- ▮ The backlight turns off automatically when no button has been pressed for 15 minutes and there is no active alarm.
- ▮ Any active alarm will cause the backlight to turn on automatically.

A red blinking background indicates that an alarm is active.

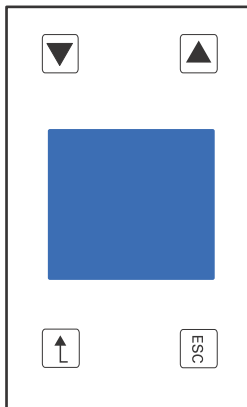


Figure 33. LCD Display

Table 5 summarizes how to use the control buttons.

Table 5. Control Buttons

Button	When on the Main Menu	When in Screensaver mode	When in Menu mode
	Returns to the Start-up screen.	Returns to the previous display screen before entering the screensaver mode.	Returns to the previous display screen.
	Opens the selected menu. NOTE: When menu items are highlighted, they are selected.	Returns to the previous display screen before entering the screensaver mode.	Signals that you want to set the values as displayed on the screen. NOTE: On information screens, this button has no action.
 	Scrolls up or down through the list of menu items.	Returns to the previous display screen before entering the screensaver mode.	Scrolls up or down to the next screen or value.

Operation Mode

Screensaver Cycling Sequence

The screensaver displays automatically after 30 seconds of inactivity from the start-up screen, a menu, or a submenu. Values are reset every five seconds. The screensaver displays data in a preset 1Ph cycle (Figure 34) or 3Ph cycle (Figure 35). These cycles are not user-configurable.

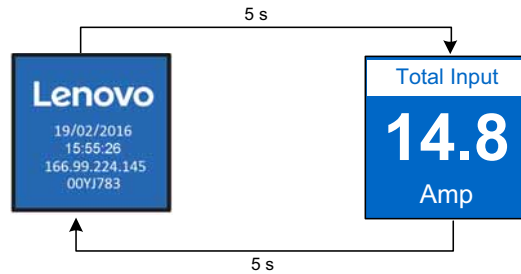


Figure 34. 1Ph Screensaver Cycle

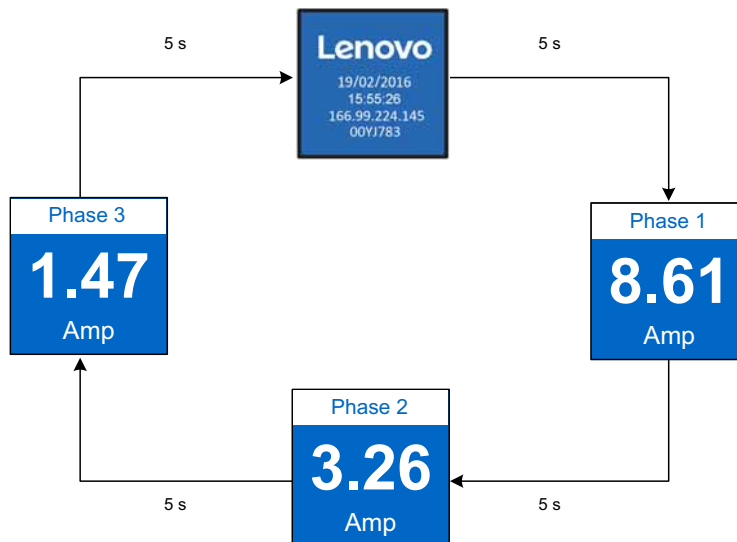


Figure 35. 3Ph Delta-configured Screensaver Cycle

Startup Screen

When the PDU powers up, the Startup screen displays (see Figure 36). Press **ENTER** to go to the Main Menu.



Figure 36. Startup Screen

Password Protected Menus

Both Control and the Settings menus can be password-protected. This locks out the menus to any user who does not know the password.

Password configuration can only be done through the Web interface and the CLI menu.

Figure 37 illustrates the sequence to enter a password for a locked menu.

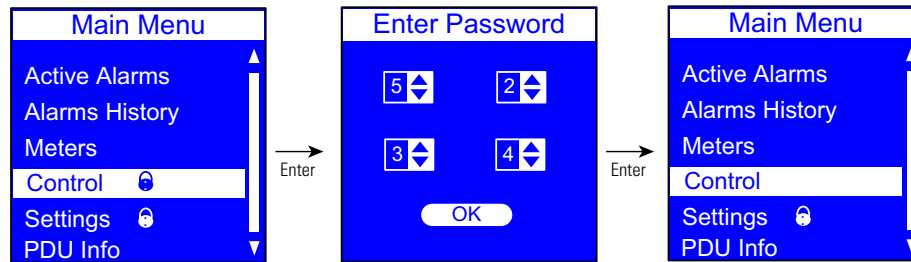


Figure 37. Password Protected Screens

Main Menu Selections

The PDU menu selection hierarchy provides useful performance information, alarms, PDU identification, and configuration settings (see Figure 38). The available menu items are illustrated in a menu hierarchy in Figure 39.

- Use the scroll buttons to select a menu item from the Main Menu.
- Selected menu items are highlighted and display as blue text on a white bar.
- Press **ENTER** to go the selected menu item.
- Press **ESC** from the Main Menu to return to the Startup Screen.

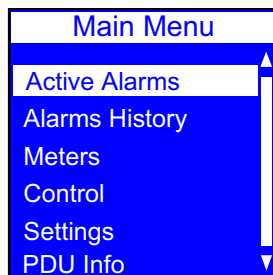
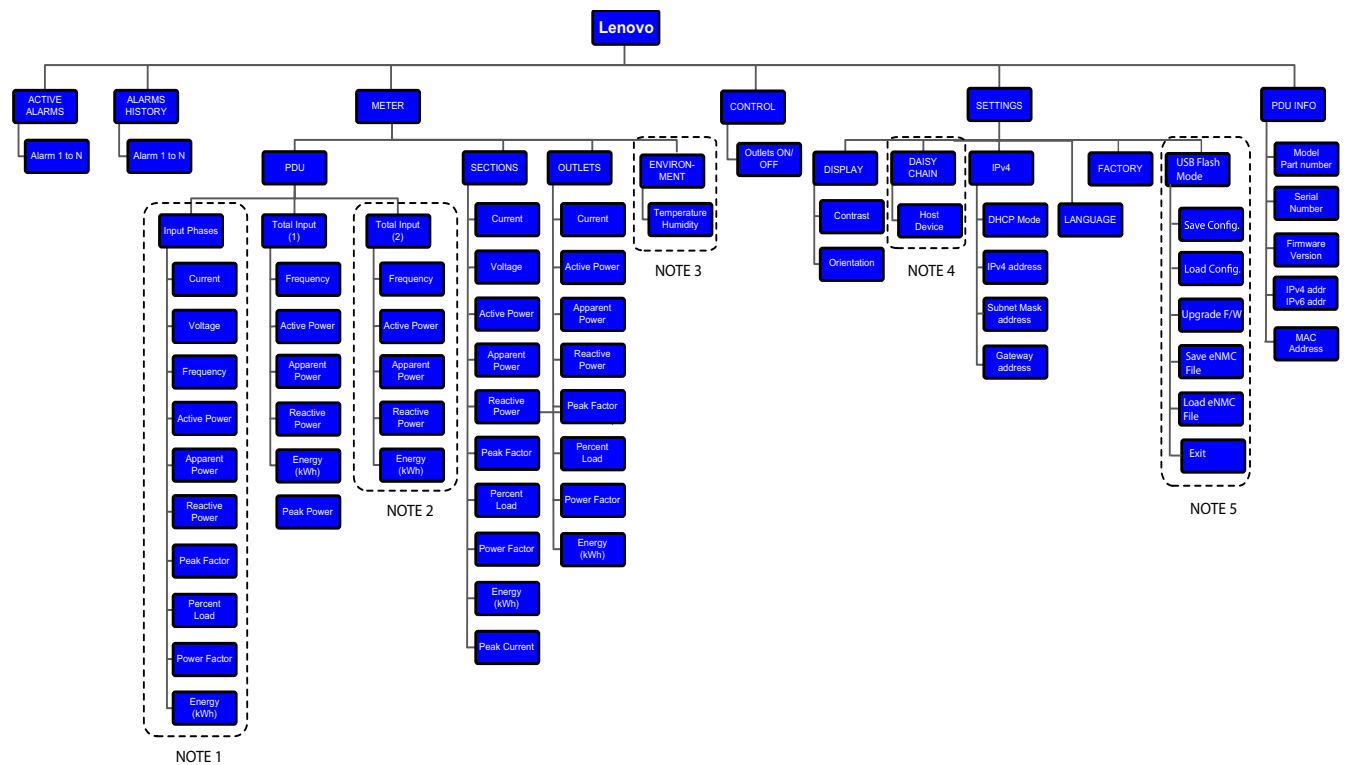


Figure 38. Main Menu Selections



NOTE 1 These submenus are only available for 3Ph input PDUs.

NOTE 2 These submenus are only available for dual input PDUs.



NOTE 3 This menu and submenu are only available if an EMP is connected.

NOTE 4 This submenu is only available for Host PDUs when a daisy-chained configuration is used.

NOTE 5 This submenu is only available if a USB drive is detected.

Figure 39. PDU Menu Hierarchy

Different sets of menus display depending on the type of topology you are managing or monitoring.

Table 6 shows LCD menus that are valid for PDU topologies.

Table 6. Menus Available for PDU Topologies

Models	Active Alarms	Alarm History	Meter ^{see NOTE 1}						Settings	PDU Info
			PDU			Sections	Outlets	Control		
			Input Phase	Total Input (1)	Total Input (2) ^{NOTE3}					
Basic	—	—	—	—	—	—	—	—	—	—
Smart	•	•	NOTE2	•	—	•	•	•	•	•

NOTE 1 The **Meter > Environment** menu is only available if an Environmental Monitoring Probe (EMP) is attached.

NOTE 2 The Input Phase menu is available if the PDU has multiple phases.

NOTE 3 The Total Input (2) menu is available if the PDU has multiple inputs

Active Alarms Menu

The Active Alarms menu filters and displays only active alarms for the PDU. Active alarm screens have priority over other screens. When an alarm occurs, the Active Alarms screen replaces the current screen and the backlight blinks in red and white (see Figure 40). Up to 100 active alarms can display.

On the Main Menu, scroll up or down to highlight **Active Alarms**. Press **ENTER** to display the first active alarm screen. Scroll up or down if needed to view active alarm data. When you finish your review, press **ESC** to return to the previous menu. If the backlight was blinking red to indicate an active alarm, the backlight returns to normal.

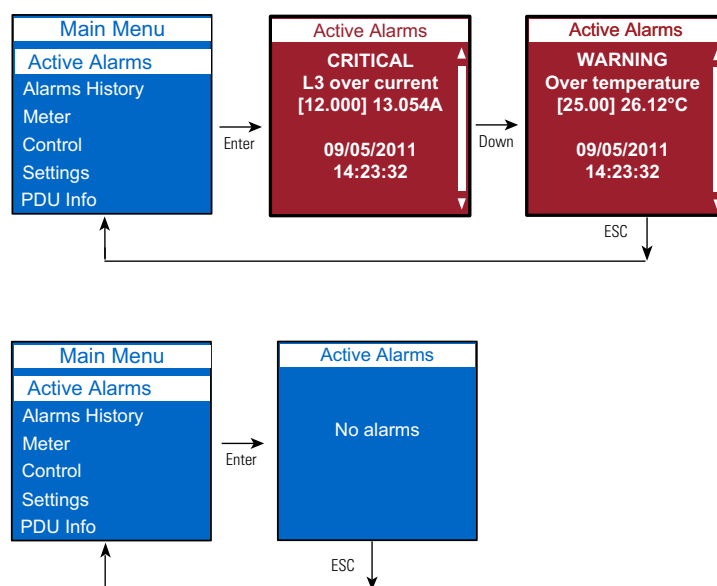


Figure 40. Example Active Alarm Displays

Alarms History Menu

The Alarms History menu allows you to scroll through the last 50 logged alarms, beginning with the most recent alarm. The Alarms History screens contain the type of alarm, the date (*MM/DD/YYYY*), and time (*hh:mm:ss*) when the alarm occurred (see Figure 41).

On the Main Menu, scroll up or down to highlight **Alarms History**. Press **ENTER** to display the most recent alarm in the history log. Scroll up or down to view the alarms. When you finish your review, press **ESC** to return to the previous menu.

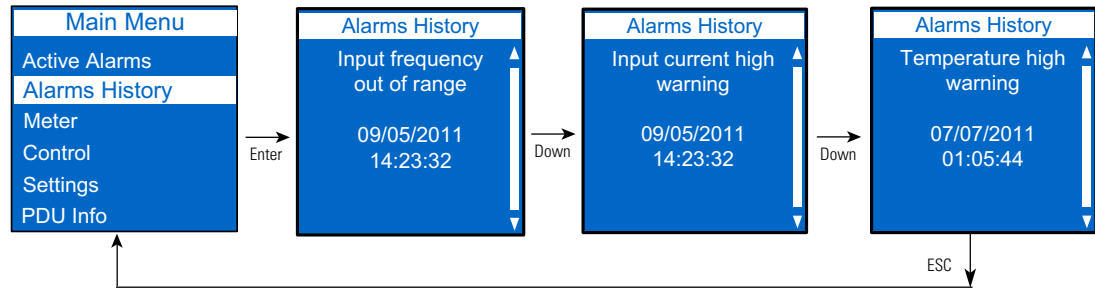


Figure 41. Example Alarm History Displays

Meter Menu

The Meter menu provides measurement data for the following submenus:

- ▮ PDU
- ▮ Sections
- ▮ Outlets
- ▮ Environment (only available if an EMP is installed)

On the Main Menu, scroll up or down to highlight **Meter**. Press **ENTER**. Scroll up or down to select a submenu and press **ENTER** to display the submenu options. Press **ESC** to return to the previous menu.

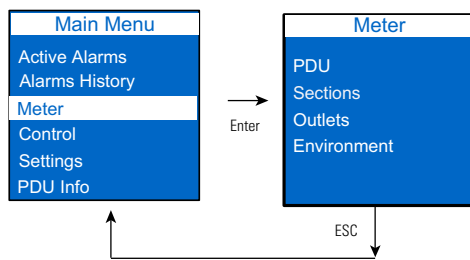


Figure 42. Example Meter Menu Display



NOTE

The measurement data for each screen is refreshed every two seconds.

PDU Submenu

These screens display Total Input data measurements for PDUs. In addition to Total Input measurements, you can view Phase Input data measurements for 3Ph, split-phase, and dual input PDUs. Depending on the PDU electrical topology, different PDU measures will display in the Total Input and the Input Phase meter screens.

Table 7 shows which measures will be present:

Table 7. Measures for Total Input and Phase Input Meter Screens

Measure	Total Input	Wye-wired Input Phase	Delta-wired Input Phase
Frequency	•	—	—
Voltage	—	•	•
Current	—	•	•
Percent Load	—	•	•
Active Power	•	•	—
Crest Factor	—	•	•
Apparent Power	•	—	—
Reactive Power	•	—	—
Power Factor	•	—	—
Energy	•	—	—
Peak Power	•	—	—

Total Input Meter Data

On the Meter menu, scroll up or down to highlight PDU. Press **ENTER** to display the Total Input submenu for your 1Ph, 3Ph, split-phase, or dual input PDU. Press **ENTER** again to see Total Input meter data measurements. Scroll up or down to review other Total Input meter data measurements. After you review the data, you can press **ESC** to return to the Input Meter menu and select L1, L2, or L3 to see Phase Input measurements. Press **ESC** to return to the previous menu.

For example, Figure 43 shows a total input display for 1Ph PDUs.

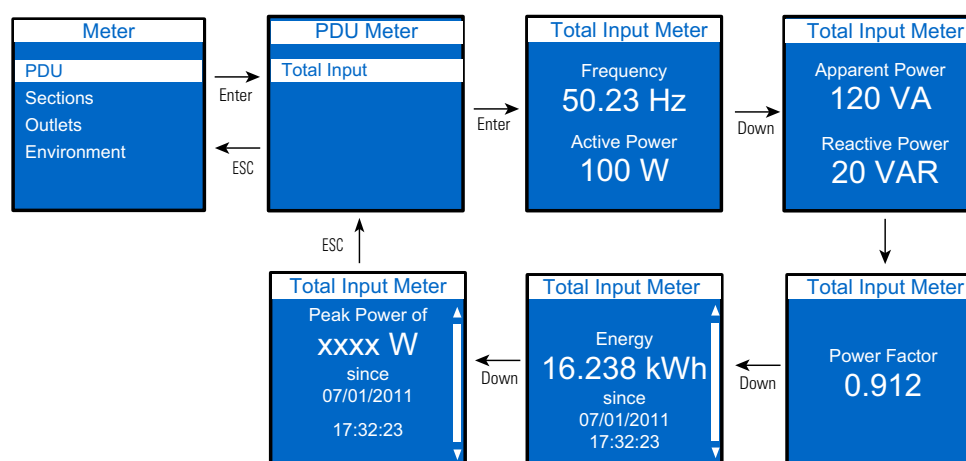


Figure 43. Example 1Ph Total Input Display



NOTE The **Total Input > Input Meter** selection screens will be different for 1Ph, 3Ph, dual input, and split-phase PDUs.

Figure 44 shows an input phase display for wye-wired 3Ph PDUs.

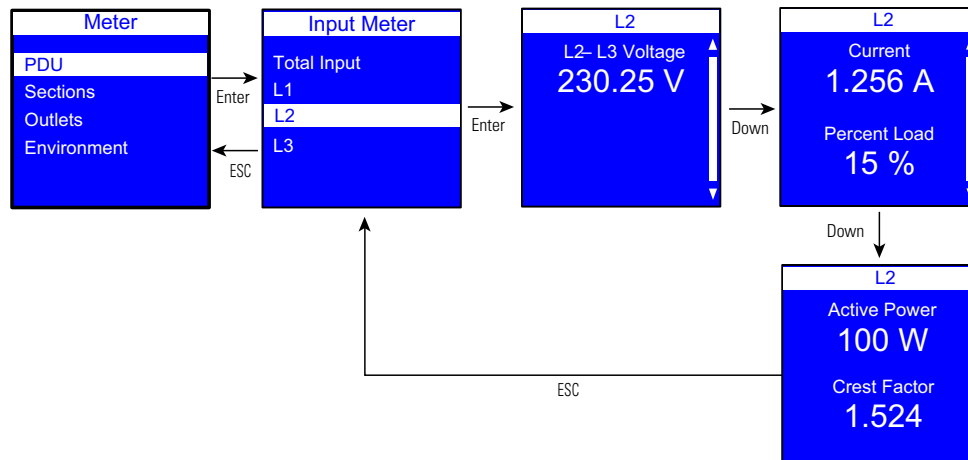


Figure 44. Example 3Ph Input Phase (wye-wired) Display

Sections Submenu

Section measurements include voltage data for all PDU sections. Other sections measurements are only available on PDUs that have current measurement capabilities (see Figure 45).

On the Meter menu, scroll up or down to highlight **Sections**. Press **ENTER** to display the Sections submenu. Scroll up or down to review the data for your selection. After you review the data, press **ESC** twice to return to the previous menu.

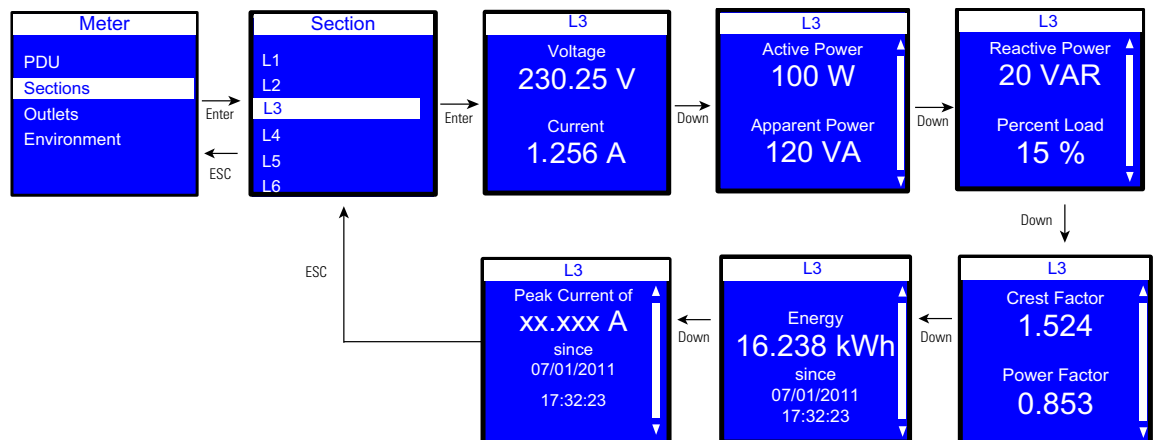


Figure 45. Example Section Submenu Display

Outlets Submenu

On the Meter menu, scroll up or down to highlight **Outlets**. Press **ENTER** to display the Outlets submenu. Scroll up or down to review the data for your selection. After you review the data, press **ESC** twice to return to the previous menu (see Figure 46).

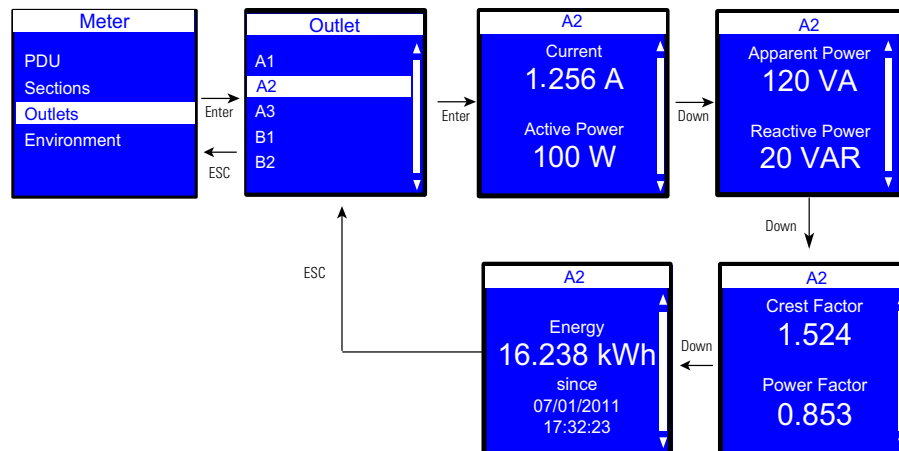


Figure 46. Example Outlets Submenu Display

Environment Submenu

The Environment submenu provides temperature and humidity data for the EMP. This menu is only available if an EMP is installed.

On the Meter menu, scroll up or down to highlight **Environment**. Press **ENTER** to display the Environment submenu. Press **ENTER** to review the data for your selection. After you review the data, press **ESC** to return to the previous menu. (Contact closures are not displayed on the LCD.)

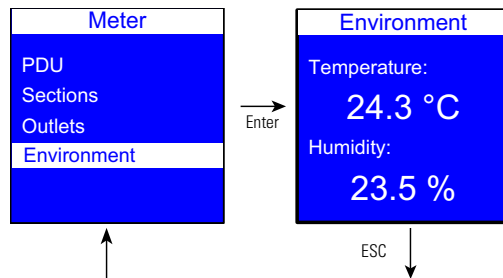


Figure 47. Example Environment Submenu Display

Control Menu

On the Main Menu, scroll up or down to highlight **Control**. Press **ENTER**. Scroll up or down to see a list of outlet group IDs. Select an outlet group. The On/Off drop down list displays. Select On or Off. The selected state of the outlet displays. Scroll up or down to see other lists of outlet group IDs (if available). Press **ESC** to return to the previous menu (see Figure 48).

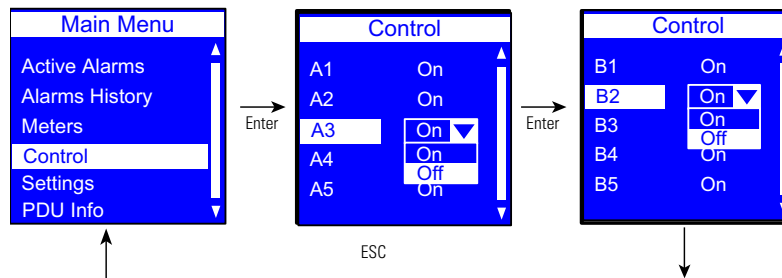


Figure 48. Example Control Submenu Display

Settings Menu

The Settings menu provides user configuration options. Only the available options display, depending on the assigned user privileges.

There are five standard Settings submenus and one optional submenu:

- USB Flash mode (only available if the USB device is detected)
- Display
- Daisy Chain
- Language
- IPv4
- Factory

On the Main Menu, scroll up or down to highlight **Settings**. Press **ENTER**. Scroll up or down to select a submenu and press **ENTER** to display the submenu options. Press **ESC** to return to the previous menu.

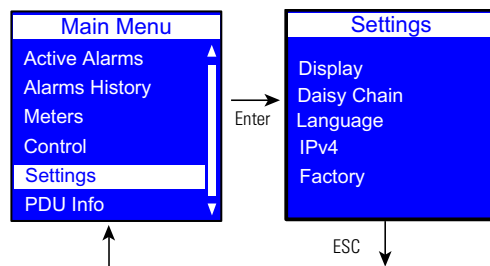


Figure 49. Example Settings Menu Display

USB Flash Mode Submenu

The “USB Flash Mode Submenu” displays in the Settings menu when a USB device is detected in the USB port. The menu selection does not display when the USB device is removed.

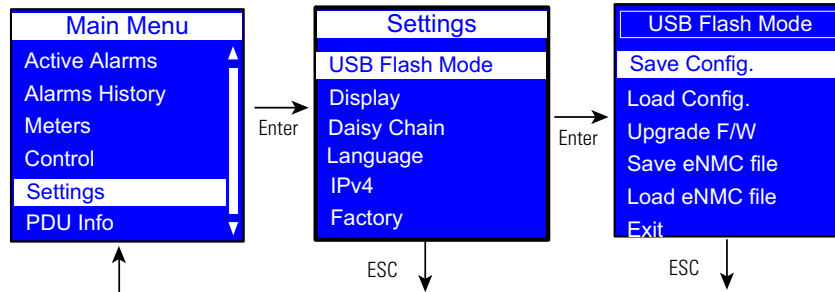


Figure 50. Example Settings USB Flash Mode Menu Display

Save User-Customized Settings Configuration Files to the USB

This LCD menu option allows you to save the user-customized configuration settings files to the USB drive. These files contain your custom settings, such as network parameters, outlet names, and threshold values. If you have several PDUs of the same model and hardware configuration, you can copy the customized setting files from one PDU and upload the files to the rest of the PDUs. This will help ensure consistency of the settings and save set-up time.

After this procedure is completed, the following files will exist on the USB device:

- eNMC/config/ConfigurationData.xml - Contains all network and communication-related settings. This can be saved from and loaded to any PDU when replicating configurations regardless of part number.
- eNMC/config/ConfigurationPdu.xml - Contains all the user-configurable settings related to the PDU itself such as voltage and current thresholds, customized naming, and outlet control parameters. The structure of this file depends on the part number so that it cannot be duplicated from part number x to part number y (PNx to PNY).

To save the user data configuration settings files to the USB drive:

1. Make sure eNMC module is power ON.
2. Insert a USB device in the USB port. Verify the USB drive contains the eNMC/config directory located at root of USB drive.
3. When the pop-up confirms that the USB is detected, click **OK**, and then press **Enter** to return to the Main Menu. (If not confirmed within 10 seconds, the pop-up goes away by itself.)
4. Under Settings, select USB Flash Mode.
5. The eNMC module restarts. (If there is no action within one minute, the eNMC module exits the USB Flash mode. Remove and reinsert the USB drive to access this menu again.)
6. Select Save Config (see Figure 51).

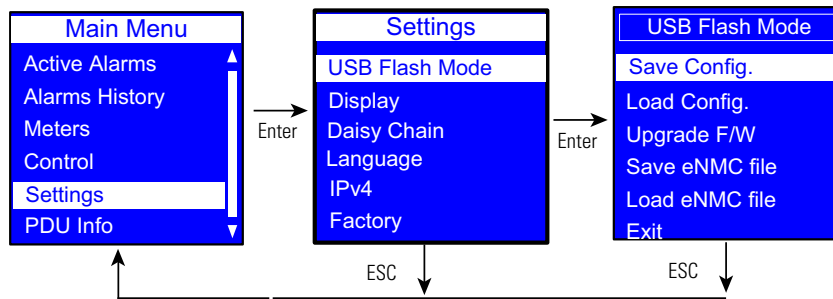


Figure 51. Example Save Config.

7. Click **OK** to continue when a successful pop-up message displays the following (see Figure 52):
 - The ConfigurationData.xml file is saved in the eNMC/ config directory on the USB drive.
 - The ConfigurationPdu.xml file is saved in the eNMC/ config directory on the USB drive.

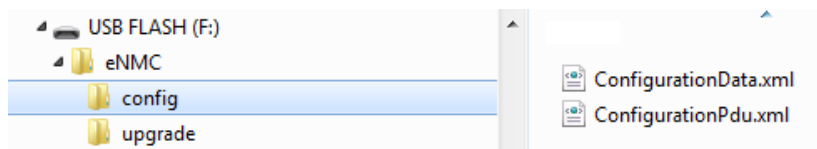


Figure 52. Example USB Root with eNMC Config Directory

8. Remove the USB drive and select **Exit**.

Load User-Customized Settings Configuration Files from the USB

This option loads the ConfigurationData.xml and ConfigurationPdu.xml files into the eNMC module from the USB device. The new parameters in these files will be applied when the eNMC module exits USB Flash Mode.

When this option is selected, the eNMC module will first attempt to load the eNMC/config/ ConfigurationData.xml file from the USB device. Next, the eNMC module will attempt to load the eNMC/config/ ConfigurationPdu.xml file from the USB device.

The ConfigurationPrivateData.xml file contains private data that is not recommended to be copied:

- Select the DHCP/static IP parameter
- Hostname parameter
- IP address parameter
- IPv6 address parameter
- Daisy Chain parameters

1. Verify that the USB drive contains the ConfigurationPdu.xml file and ConfigurationData.xml files in eNMC/config directory of USB drive (see Figure 53).

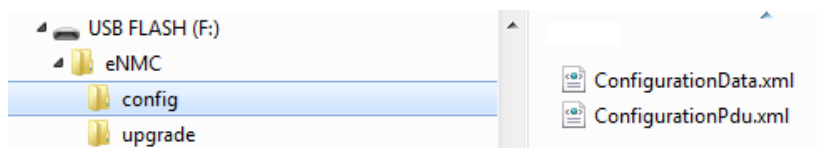


Figure 53. Verify Files at USB Root



NOTE 1 The eNMC/config directory contains only these two files.

NOTE 2 The ConfigurationPdu.xml file is compatible with a specific PDU part number.

2. Make sure eNMC module is powered ON.
3. Insert a USB drive.
4. When the pop-up confirms that the USB is detected, click **OK** then press **Enter** to go to the Main Menu. (If not confirmed within 10 seconds, the pop-up goes away by itself.)
5. Select USB Flash Mode from the Settings menu. The module restarts.
6. Select Load Config then click **OK** to start loading the ConfigurationData.xml file into the eNMC module (see Figure 54).

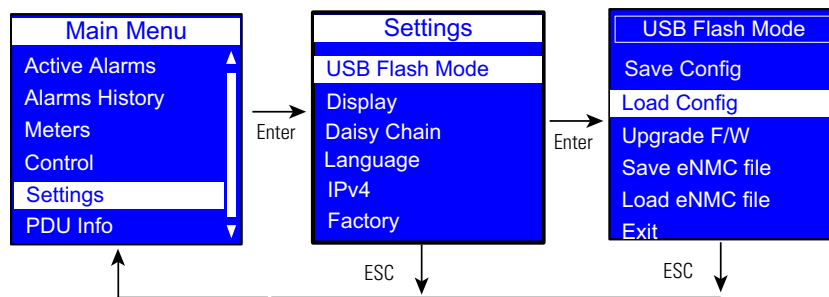


Figure 54. Example Load Config.

7. When the file is successfully loaded, click **OK** in response to the confirmation message.
8. Click **OK** to start loading the ConfigurationPdu.xml file into the eNMC module.
9. When the file is successfully loaded, click **OK** in response to the confirmation message.
10. Remove the USB drive and select **Exit** from the USB Flash Mode menu.

Save the PDU Hardware Configuration File to the USB

This procedure is used as part of the eNMC module replacement procedure. Each PDU model has a model-specific hardware configuration file for its eNMC module that can only be used on the specified model. This procedure allows you to copy the PDU hardware configuration file from a working PDU of the same model and store it on a USB flash drive so that it can be uploaded to a new eNMC module.

To save the PDU model-specific hardware configuration file to a USB drive:

1. Make sure the eNMC module is powered ON. Connect a USB flash drive to a working PDU.



IMPORTANT

This PDU must be of the same model type and configuration as the PDU that houses the eNMC you will replace.

2. When the LCD interface pop-up confirms that the USB flash drive is detected, click **OK**, and press **Enter** to return to the Main Menu. (If not confirmed within 10 seconds, the pop-up goes away by itself.)
3. From the LCD Settings menu, select USB Flash Mode. Press **Enter**, select **yes** to confirm, and then press **Enter** again. The module restarts. (If there is no action within one minute, the eNMC module exits USB Flash Mode. Remove and reinsert the flash drive to access this menu again.)

4. Select Save eNMC file to save the PDU hardware configuration file to the USB drive (see Figure 55). The file will save to the eNMC/config/hw path at the USB drive root directory (see Figure 56).).

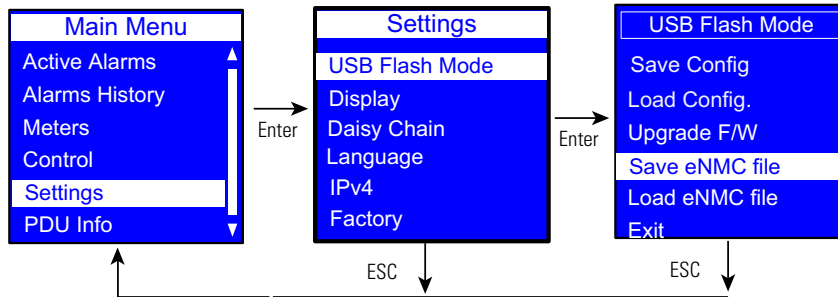


Figure 55. Example Save eNMC File

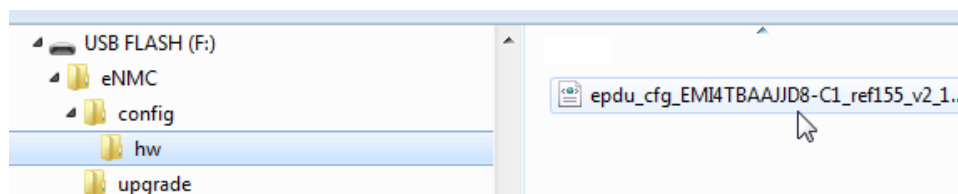


Figure 56. Verify HW File at USB Root

5. When the file is saved, click OK to confirm.

Load the PDU Hardware Configuration File from the USB to the eNMC Module

This procedure is used as part of the replacement procedure.

The PDU hardware configuration file provides the replacement eNMC module with the characteristics of the PDU model in which it resides, such as the type of input, the number of circuit breakers and outlets, and the way measurements should be displayed. Use this menu selection to upload the PDU model-specific hardware configuration file to the replacement eNMC module.



NOTE

This selection will only display in the menu if an PDU hardware configuration file is detected on the USB drive.

To load the PDU model-specific hardware configuration file to an eNMC module:

1. Make sure the eNMC module is powered ON. Connect the USB flash drive to the PDU with the new eNMC module.
2. When the LCD interface pop-up confirms that the USB flash drive is detected, click **OK**, then press **Enter** to return to the Main Menu. (If not confirmed within 10 seconds, the pop-up goes away by itself.)
3. From the LCD Settings menu, select USB Flash Mode. Press Enter, select yes to confirm, and then press Enter again. The module restarts. (If there is no action within one minute, the eNMC module exits USB Flash Mode. Remove and reinsert the USB flash drive to access this menu again.)
4. Select Load eNMC file, then click **OK** to upload the PDU hardware configuration file to the eNMC (see Figure 57).
5. When the file is successfully loaded, click **OK** to confirm.
6. Remove the USB flash drive and select **Exit**.

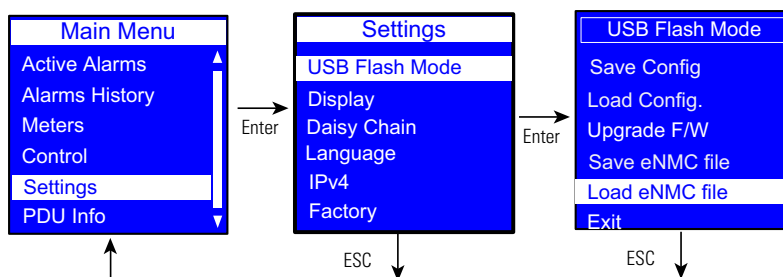


Figure 57. Example Load NMC File



NOTE 1 The eNMC/upgrade/hw directory contains only one file named epdu_cfg*.xml.

NOTE 2 The epdu_cfg*.xml file shall be compatible with the PDU part number.

Upgrade the eNMC Module Firmware using USB

To upgrade the eNMC module firmware:

1. Go to <http://shop.lenovo.com/us/en/systems/servers/options/systemx/rack-power-infrastructure/power/>.
2. Enter the PDU part number of your model in the PDU Part Number Search field and click **Search**. The product Web page displays.
 1. Select the **Options** tab and click either the PDU Firmware link or the free download link. The Download - PDU Software Tools and MIBs page displays.
 2. Click the link to the firmware upgrade file for your model in the column named PDU Firmware (Smart PDUs) and save the file to your computer.



NOTE The file is named Image*.bin.

3. Connect a USB drive to your computer and put the Image*.bin file in the eNMC/upgrade/ location on the USB drive root directory (see Figure 58).

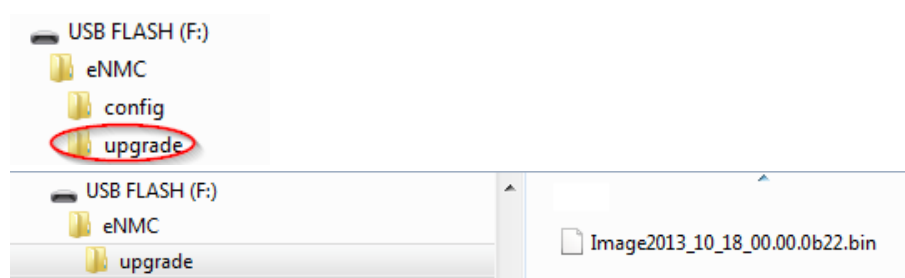


Figure 58. Root Directory of Flash Disk



NOTE There can only be one Image*.bin file in the eNMC/upgrade directory on your USB drive.

4. Make sure eNMC module is powered ON.
5. Insert the flash drive in the USB port of the eNMC front panel.

6. When the pop-up confirms that the USB is detected, click **OK**, and then press **Enter** to return to the Main Menu. (If not confirmed within 10 seconds, the pop-up goes away by itself.)
7. Select USB Flash Mode. Click **Yes** to confirm you want to enter the USB Flash mode. (If there is no action within one minute, the eNMC module exits the USB Flash mode. Remove and reinsert the USB drive to access this menu again.) The module restarts.
8. Select Upgrade FW and click **OK** to confirm the upgrade (see Figure 59). The eNMC module gets the file from the USB drive.

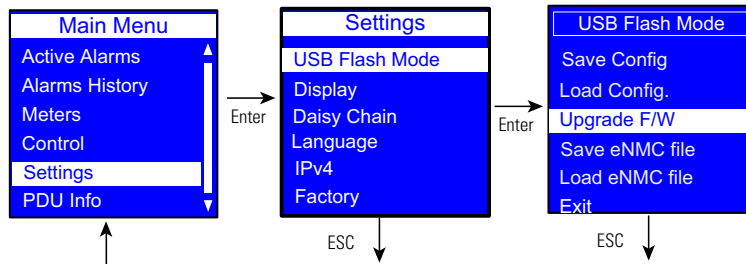


Figure 59. Example Select Upgrade Firmware

9. A few seconds after 100% is reached, the eNMC module restarts and then enters in Boot upgrade mode to continue upgrade. The upgrade is finished when eNMC module is restarted. This can take several minutes (see Figure 60).

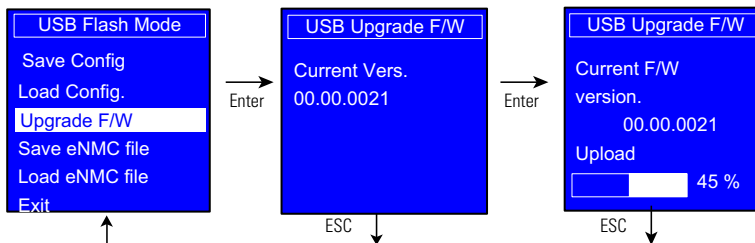


Figure 60. Example Upgrade in Progress

Exit

Select **Exit** to leave USB Flash Mode.

Display Submenu

The Display submenu allows you to customize settings for LCD contrast and orientation (see Figure 61).

On the Settings menu, scroll up or down to highlight **DISPLAY**. Press **ENTER** to display the screens to set the values for the submenu. After you select the values, press **ENTER** to set the values as displayed on the screen. Press **ESC** to return to the previous menu.

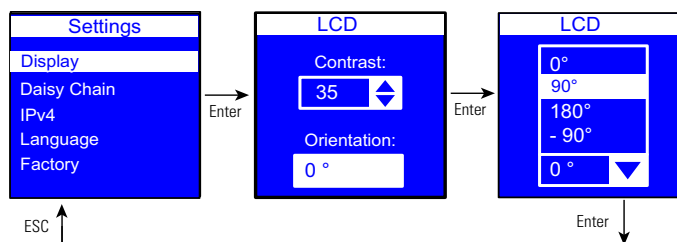


Figure 61. Example Display Submenu Displays

Daisy Chain Submenu

The Daisy Chain submenu allows you to configure two to eight PDUs to be monitored from a single Ethernet connection on the Host PDU. Use the Daisy Chain submenu options (Settings and Discovery) to configure the PDUs.

NOTE 1 The Host PDU must be connected to the network. There can only be one Host.



NOTE 2 To configure and monitor the PDUs, they must be connected together through the Daisy Chain connector on the front panel using an Ethernet network cable.

NOTE 3 All daisy-chained PDUs should have the same Configuration number. Daisy-chaining PDUs of different configuration numbers may lead to unpredictable results.

Use the Settings option for the first two configuration steps:

1. From the PDU (or PDUs) designated as a Device PDU, access the Daisy Chain Settings option and set the Device values.
2. From the PDU designated as the Host PDU, access the Daisy Chain Settings option and set the Host values.

Use the Discovery option for the final configuration step:

3. From the Host PDU, access the Daisy Chain Discovery option to start communication between the Host and the Device PDU (or PDUs).

Daisy Chain Settings Options

The Daisy Chain Settings option allows you to specify the PDU that will be the Host (the PDU that has the network connection) and the PDU (or PDUs) that will be a Device.

From the LCD of the **Device** PDU (or PDUs), set the values as follows (see Figure 62):

1. On the Settings menu, scroll up or down to highlight **Daisy Chain** and press **ENTER**.
2. Scroll up or down to highlight **Daisy Chain** and press **ENTER**.
3. Select **1 (Device)**, **2 (Device)**, **3 (Device)**, **4 (Device)**, **5 (Device)**, **6 (Device)**, or **7 (Device)** from the Id: selection drop-list. Press **ENTER**.
4. Select **End** or **Middle** from the Place: selection drop-list. Press **ENTER**.

NOTE 1 Select **End** when only two PDUs are daisy-chained together.



NOTE 2 Select **Middle** when the PDU (or PDUs) are connected between a host and another PDU.

NOTE 3 Select **End** when assigning the last device in the chain when daisy-chaining three or more PDUs.

5. Press **ESC** to return to the previous menu.

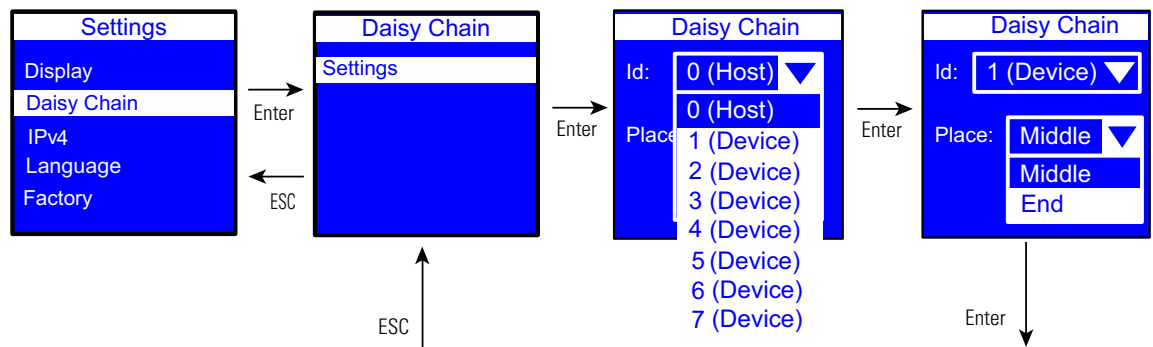


Figure 62. Example Daisy Chain Device PDU Setup (Device)

From the LCD of the **Host** PDU, set the values as follows (see Figure 63):

1. On the Settings menu, scroll up or down to highlight **Daisy Chain** and press **ENTER**.
2. Scroll up or down to highlight **Settings** and press **ENTER**.
3. Select **0 (Host)** from the Id: selection drop-list. Press **ENTER**.
4. Select **End** or **Middle** from the Place: selection drop-list. Press **ENTER**.
5. Press **ESC** to return to the previous menu.

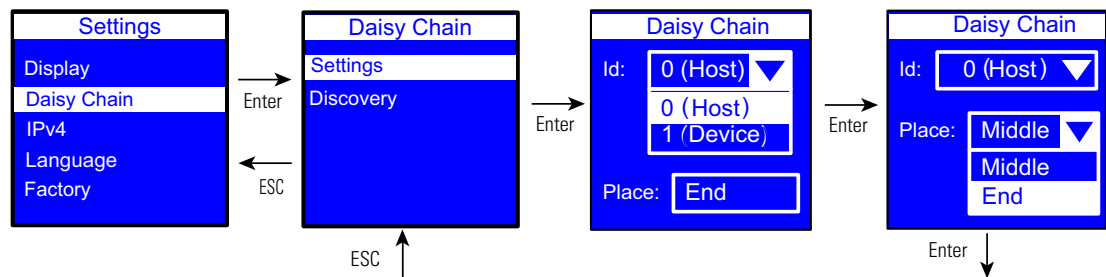


Figure 63. Example Daisy Chain Host PDU Setup (Host)

Daisy Chain Discovery Options

The Discovery option starts communication between the Host PDU and the Device PDU. This is only available for the Host PDU. The display you see varies depending on whether the PDU is communicating properly or not communicating (see Figure 64 and Figure 65).

From the Host PDU, perform a Discovery as follows:

1. On the Settings menu, scroll up or down to highlight **Daisy Chain** and press **ENTER**.
2. Scroll up or down to highlight **Discovery**.
3. Press **ENTER** to perform the discovery.
 - When the discovery completes successfully, the Media Access Control (MAC) address of the Device PDU displays (see Figure 46). Go to Step 4.
 - If there is no connection, the **No device chained** error message displays (see Figure 47). Go to the Daisy Chain Settings option screens and reset the values to correctly identify the Host. Once corrected, then select the Discovery option again.
 - If the Host and Device PDUs have been incorrectly identified, a **Host Conflict** error message displays. Go to the Daisy Chain Settings option screens and reset the values to correctly identify the Host and Device. Once corrected, select the Discovery option again.
4. Press **ENTER** to validate the Discovery.
5. Press **ESC** to return to the previous menu.

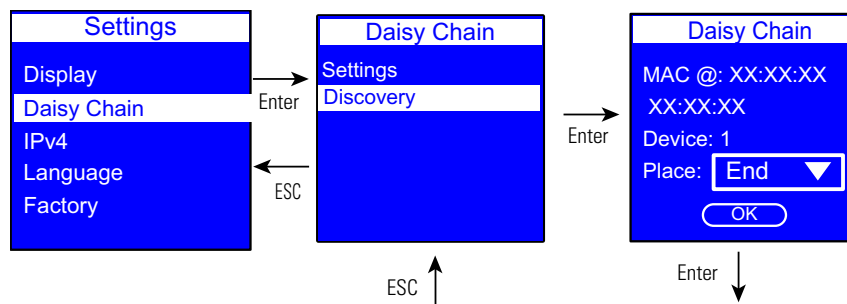


Figure 64. Example Daisy Chain PDU Discovery (Communicating)

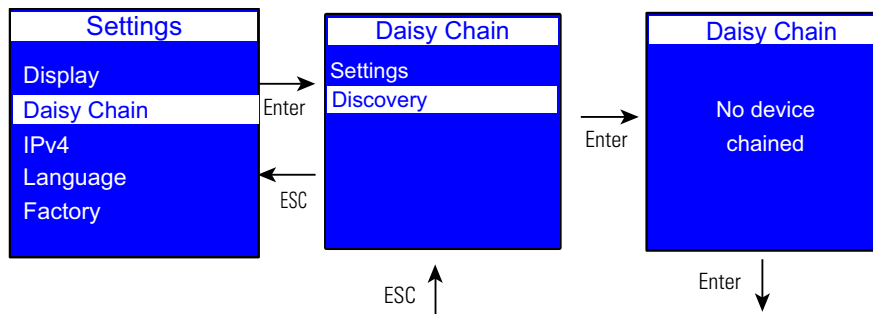


Figure 65. Example Daisy Chain PDU Discovery (Not Communicating)

IPv4 Submenu

The IPv4 submenu allows you to set options for:

- DHCP
- IP address
- Subnet Mask
- Gateway

Figure 66 shows the IP Address displays.

On the Settings menu, scroll up or down to highlight IPv4. Press **ENTER** to display the options screen. Scroll up or down to highlight the selected option from the menu. Press **ENTER** to display the screens to set the values for the selected option. After you select the values, press **ENTER** to set the values as displayed on the screen. Press **ESC** to return to the previous menu.

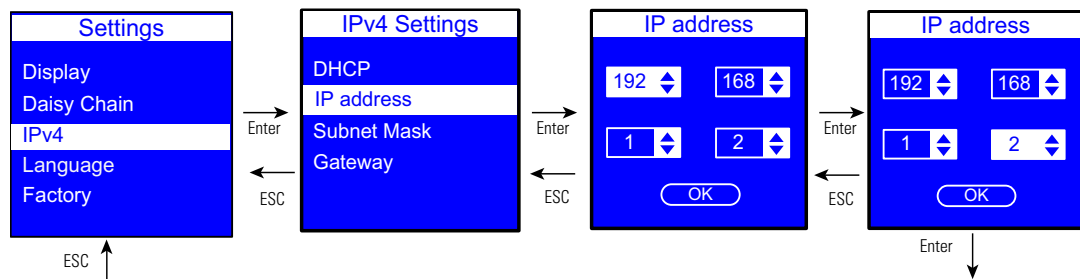


Figure 66. Example IPv4 Submenu Displays

Language Submenu

On the Settings menu, scroll up or down to highlight Language. Press **ENTER**. Scroll up or down to highlight the selected language option from the menu. Press **ENTER** to set the selected language. Press **ESC** to return to the previous menu (see Figure 67).

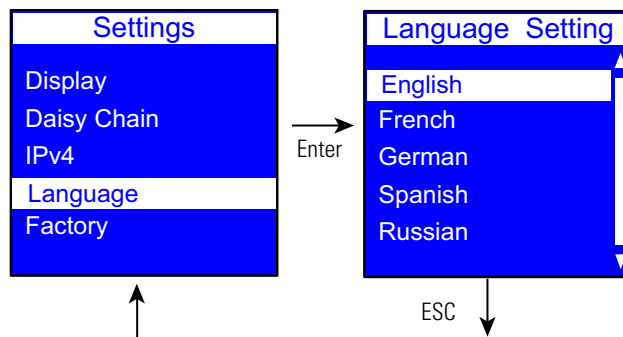


Figure 67. Example Language Setting

Factory Submenu

The Factory submenu allows you to reset the PDU to the factory settings (see Figure 68).

On the Settings menu, scroll down to highlight Factory. Press **ENTER** to display the screens to set and confirm the return to factory settings. After you make the selections, press **ENTER** to set the values as displayed on the screen. Press **ESC** to return to the previous menu.

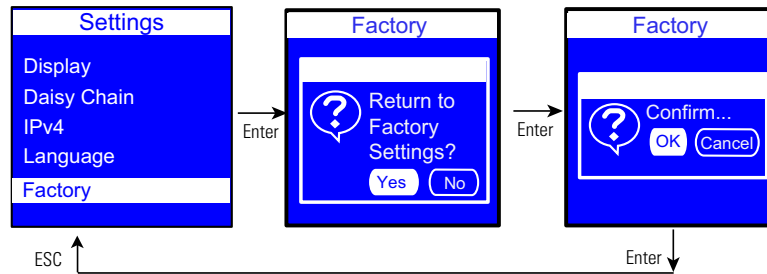


Figure 68. Example Factory Submenu Displays

PDU Info Menu

The PDU Info menu provides identification information for this PDU. The identification information includes the PDU model type and part number, serial number, PDU Network Management and Control (eNMC) module firmware version number, IP address, and PDU Network Management and Control (eNMC) module MAC (Media Access Control) address. These are information-only screens (see Figure 69).

On the Main Menu, scroll up or down to highlight PDU Info. Press **ENTER** to navigate to each screen. Scroll up or down on the screen if needed to view the PDU information displays. Press **ESC** to return to the previous menu.

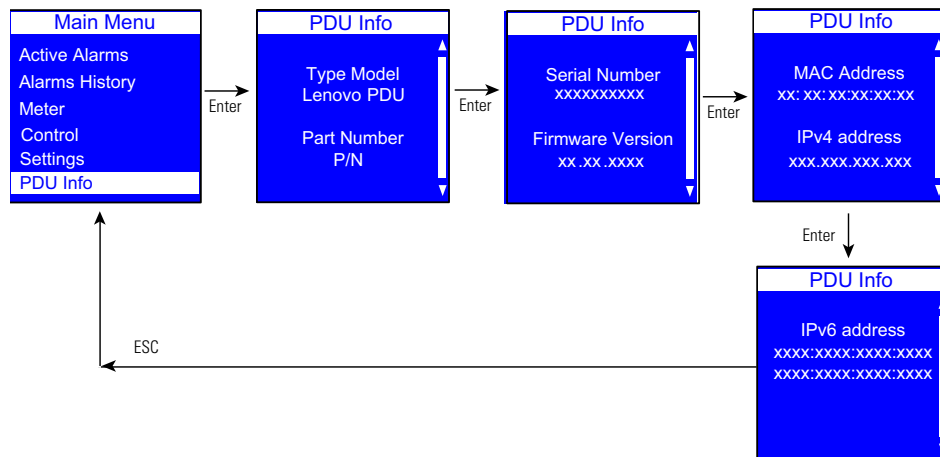


Figure 69. Example PDU Info Display

Chapter 7 Serial Interface Operation

This section describes the command line interface (CLI) commands used to remotely configure and monitor the Lenovo Power Distribution Unit (PDU) through the serial interface connection or network connection between the and a laptop or workstation.

Access to a CLI is provided through a terminal emulation program, such as HyperTerminal, Telnet, or SSH. A maximum of five concurrent sessions (Telnet or RS-232 port) are allowed.

Supported Commands

The PDU CLI command set for managing and monitoring the PDU includes the following commands:

- ?
- info
- quit
- get
- set
- pdu

NOTE Observe the following:



- Command variables are represented in command input syntax surrounded by angle braces (< >).
- Optional parameters are represented in command input syntax surrounded by straight brackets ([]).
- For data of type array, the 'x' character as index of array in command input syntax means all indexes.
- Commands are case sensitive, but object names are not case sensitive.



NOTE You must be logged into the PDU before commands can be sent.

? command

Use this command to list all available PDU CLI commands or receive detailed help on specified commands.

Usage

```
pdu#0>?  
pdu#0><command> ?
```

where:

<command> = info, get, set, pdu, quit

List all available PDU CLI commands

```
pdu#0>?
```

Example

```
pdu#0>?  
Usage: ? info get set pdu quit  
pdu#0>
```

List detailed help on a specific PDU CLI command

```
pdu#0><command> ?
```

Example 1

```
pdu#0>set ?  
Usage: change the device data defined by its' name followed by the new value set  
[name] [value]  
pdu#0>
```

Example 2

```
pdu#0>pdu ?  
Usage: select the strapping pdu unit to focus on pdu [number]  
PDU#0
```

info command

Use this command to display the device data defined by its name information (`info [name]`).

```
pdu#0>info ?
      info [System]
      info [Network]
      info [User]
      info [Access]
      info [Time]
      info [eMail]
      info [SNMP]
      info [NetworkManagement]
      info [EnergyWise]
      info [DaisyChain]
      info [UserDefinedGroup]
      info [PowerSchedule]
      info [Summary]
      info [Input1]
      info [Input2]NOTE 1
      info [Gang]
      info [Outlet]
      info [Environment]
pdu#0>
```

NOTE 1: On Dual Input PDU only.

Usage

```
pdu#0>info <object>
```

where:

<object> = name of a simple object, an object of type array or a family of objects

Example 1

```
pdu#0>info System.Network.DHCP
```

<u>Name</u>	<u>Unit</u>	<u>RO/Rw</u>	<u>Type</u>
System.Network.DHCP	RW		0: Disabled 1: Enabled

Example 2

```
pdu#0>info PDU.*
```

<u>Name</u>	<u>Unit</u>	<u>R0/RW</u>	<u>Type</u>
PDU.DaisyChain[x].ChangedStatus.Communication Lost	sec	R0	Integer:0..4294967295(136 years)
PDU.DaisyChain[x].iName	sec	R0	String[15]
.			
.			
.			
PDU.DaisyChain[x].PresentStatus.Communication Lost	sec	R0	0: Normal 1: Alarm

Example 3

```
pdu#0>info System.*
```

<u>Name</u>	<u>Unit</u>	<u>R0/RW</u>	<u>Type</u>
System.NetworkManagementSystem.Count		R0	Integer:0..65535
System.NetworkManagementSystem[x].HostName		RW	String[63]
System.NetworkManagementSystem[x].TrapCommunity		RW	String[24]
.			
.			
.			
System.NetworkManagementSystem[x].TrapSnmpVersion		RW	0: Disabled 1: SNMP V1 2: SNMP V3

Example 4

```
pdu#0>info Environment.*
```

<u>Name</u>	<u>Unit</u>	<u>R0/RW</u>	<u>Type</u>
Environment.ChangedStatus.CommunicationLost	sec	R0	Integer:0..4294967295(136 years)
Environment.ChangedStatus.OverHumidity	sec	R0	Integer:0..4294967295(136 years)
Environment.ChangedStatus.OverTemperature	sec	R0	Integer:0..4294967295(136 years)
Environment.Humidity		R0	Float:0..6553.5
Environment.Input[1].ChangedStatus.Alarm	sec	R0	Integer:0..4294967295(136 years)
Environment.Input[1].iName		RW	String[31]
.			
.			
.			
Environment.Input[1].PresentStatus.Alarm		R0	0: Normal 1: Alarm

quit command

Use this command to log out and exit the serial or network interface for the PDU.

Usage

```
pdu#0>quit
```

Log out of the CLI

```
pdu#0>quit
```

Example with serial interface

```
pdu#0>quit
Session closed
```

Example with network interface

```
pdu#0>quit
Connection to host lost.
```

get command

Use this command to view the value of an object or a family of objects that belong to the HID database or a card parameter.

Usage

```
pdu#0>get <object>
```

where:

<object> = a simple object, an object of type array or a family of objects

Get a single value

```
pdu#0>get <path>.<name>
```

Example

```
pdu#0>get System.Network.DHCP
1
pdu#0>
```

Get the size of an array

```
pdu#0>get <path>.Count
```

Example

```
pdu#0>get System.NetworkManagementSystem.Count
8
pdu#0>
```

Get a single value of an array

```
pdu#0>get <path[i]>.<name>
```

where:

[i] = the index in the array, from 1 to *n*. The value of *n* depends of the HID object and is obtained with a **get** command

Example

```
pdu#0>get System.NetworkManagementSystem[1].TrapCommunity
public
pdu#0>
```

Get all values of an array

```
pdu#0>get <path[x]>.<name>
```

**NOTE**

Values are separated by the pipe character (|).

Example

```
pdu#0>get System.User[x].SecurityRight
0|0|0|0|0|0|0|0
pdu#0>
```

Get all values of a family

```
pdu#0>get <short path>.*
```

where:

<short path> = incomplete path name. A node must be complete.

Example 1**Example 2**

```
pdu#0>get System.*
System.NetworkManagementSystem.Count
8
System.NetworkManagementSystem[x].HostName
../..
pdu#0>
```

Get Daisy-chained PDU to Supervise or Retrieve Communication Status

```
pdu#0> pdu [x]
pdu#0>get <short path>.*
```

where:

[x] = value 0 to 7 to indicate Host (0) or device (1, 2, 3, 4, 5, 6, or 7) to supervise; enter key to accept prompt PDU ID
 <short path> = incomplete path name. A node must be complete.

Example 1

```
pdu#0>get System.DaisyChain.*
System.DaisyChain.DeviceId
0
System.DaisyChain.Position
1
System.DaisyChain.Status
1
System.DaisyChain.Count
1
pdu#0>
```

NOTE 1 The communication status is returned for the selected Device or Host by **System.DaisyChain.Status**. The Status value is:

0: No Communication
 1: Communication OK
 2: Communication failed
 3: Host conflict
 4: Device conflict



NOTE 2 The Count command value is the number of PDUs connected in the daisy-chain configuration.

set command

Use this command to change the value of an object that belongs to the HID database or a card parameter.



NOTE Some data cannot be modified without appropriate user access rights.

Usage

```
pdu#0>set <object> <value>
```

where:

<object> = a simple object or an object of type array.

<value> = a value or a list of values separated with the pipe character (|). For a value of type string, the space character ' ' is taken into account.

Set a single value

```
pdu#0>set <path>.<name> <value>
```

Example 1

```
pdu#0>set System.Network.DHCP 1
1
pdu#0>
```

Example 2

```
pdu#0>set System.Display.LcdRotation 1
1
pdu#0>
```

where:

<0> = Rotation 0 Degrees (0U).
 <1> = Rotation 90 Degrees (IL).
 <2> = Rotation 180 Degrees (0U).
 <3> = Rotation 270 Degrees (IL).

Set value of an array

```
pdu#0>set <path[i]>.<name> <value>
```

where:

[i] = the index in the array, from 1 to *n*. The value of *n* depends of the HID object and is obtained with a **get** command

Example

```
pdu#0>set System.Network.SNMP.V3.User[1].Name User 1
User 1
pdu#0>
```

set all values of array

```
pdu#0>set <path[x]>.<name> <value 1>[|<value 2>]..../..[|<value n>]
```



NOTE Values are separated by the pipe character (|).

Example

```
pdu#0>set System.Network.SNMP.V3.User[x].Name User 1|User 2|User 3|User 4
User 1|User 2|User 3|User 4
pdu#0>
```

Set Daisy Chain**Device ID and Position**

```
pdu#0>set System.DaisyChain.DeviceID [x]
```

where:

[x] = value from 1 to 7 as a unique identifier for each device (zero is reserved for the Host)

```
pdu#0>set System.DaisyChain.Position [x]
```

where:

[x] = 0 for a device PDU connected between two other PDUs; 1 for a device PDU connected to just one PDU

Example

```
pdu#0>set System.DaisyChain.DeviceID
1
pdu#0>
```

```
pdu#0>set System.DaisyChain.Postion 1
1
pdu#0>
```

Host ID and Position

```
pdu#0>set System.DaisyChain.DeviceID [x]
```

where:

[x] = enter 0 as a unique identifier for the host only

```
pdu#0>set System.DaisyChain.Position [x]
```

where:

[x] = 0 if the host PDU is connected between two other PDUs; 1 if the host PDU is connected to just one PDU

Example

```
pdu#0>set System.DaisyChain.DeviceID 0
0
pdu#0>
```

```
pdu#0>set System.DaisyChain.Postion 1
1
pdu#0>
```

pdu command

Use this command to access different PDUs on the daisy chain, or to reset a daisy-chained PDU as the Host or Device.

Usage

pdu#0>pdu <value>

where:

<value> = 0 for the host; 1, 2, 3, 4, 5, 6, or 7 for the device

Example

```
pdu#0>pdu 1
pdu#1>
```

Error Messages

The following errors could display:

The command is unknown.

This error displays when an invalid command is entered. Valid commands are ?, info, get, set, pdu, and quit.

The parameter in the command is unknown.

This error displays when a parameter you entered in the command is not recognized.

The parameter in the command is out of limits.

This error displays in the following circumstances:

- ▮ The set command refers to a data name but does not have the second parameter.
- ▮ The set command refers to a value that does not match with the data.

The command is not valid for this object.

This error displays when the set command refers to an object that cannot be set after the system preforms a coherence check with other data.

The user has insufficient rights.

This error displays when:

- ▮ The set command contains read-only data.
- ▮ The user has insufficient rights to modify the data.

The PDU1 is not available.

This error displays when the indicated PDU is unreachable.

XML Object Tables

XML object tables are available online at <http://shop.lenovo.com/us/en/systems/servers/options/systemx/rack-power-infrastructure/power/>.

Chapter 8 Web Interface Operation

This chapter describes remotely configuring, managing, and monitoring an Lenovo Power Distribution Unit (PDU) remotely through the PDU Network Management and Control (eNMC) module Web interface. This chapter describes the following:

- Navigating the Web interface
- Accessing the Web interface
- Configuring settings and monitoring the PDU



NOTE

When the Web browser is set to 100% (full page), we recommend setting your screen resolution to a minimum of 1024 x 768 for the best display performance.

Navigating the Web Interface

The graphical Web interface is used to remotely monitor or configure the PDU (see Figure 70). The Web interface that corresponds to the PDU topology type displays. This section describes the functions provided by this interface.

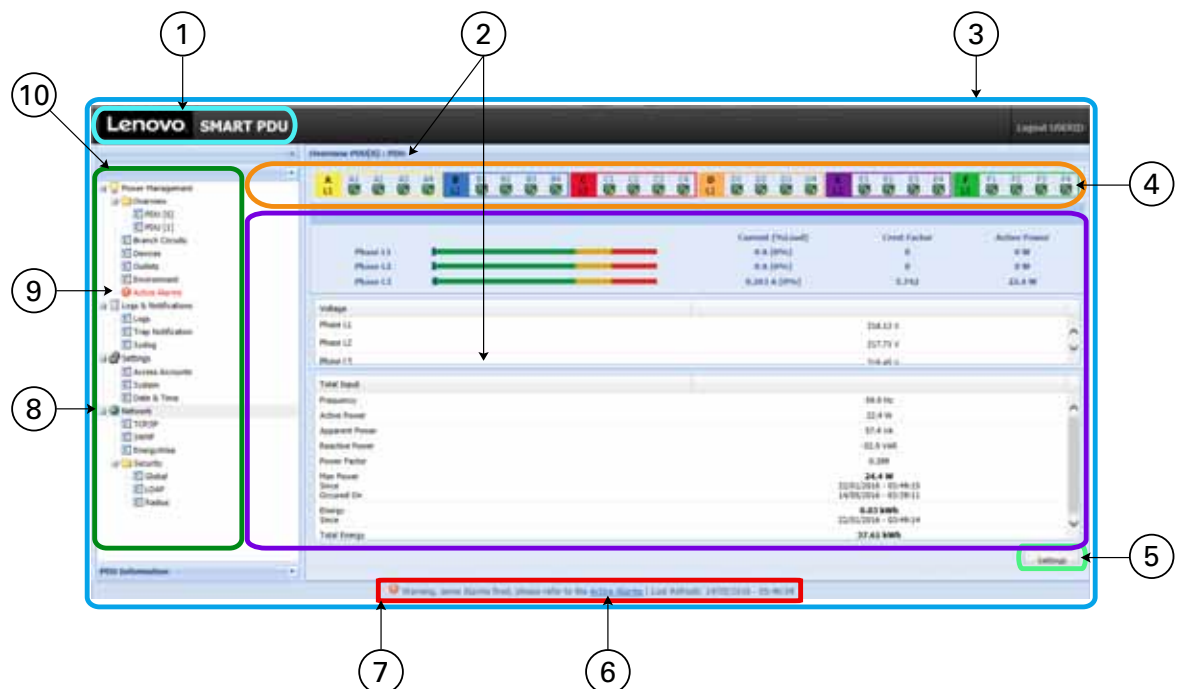


Figure 70. Navigating the Web Interface (Opening Page)

Table 8 provides descriptions of the Web interface components.

Table 8. Web Interface Region Descriptions

Area	Description
1 - Application Header Bar	The header bar identifies which Lenovo PDU Web application is within the host window.
2 - Menu Selection Page Display	As each menu link is selected, the corresponding information displays as the main page. The top of the page displays the menu selection title. NOTE You can expand your view of the contents vertically using the elevator scroll button on the side of the page. If you need more window viewing area, resize the Host Window to a wider or taller size. This enlarges the main page.
3 - Host Window	The host window is the page where the application resides. Both the height and the width of the host window can be resized. The application panels resize at the same time. An elevator scroll button displays on the side of the application panel if the panel cannot display the entire list within the resized panel. Drag the elevator scroll button up or down to view the entire list of data in the application panel.
4 - Outlet Icons	Roll over any outlet icon to see the type of outlet and whether there is an alarm. (A gray outlet status indicates that the outlet management feature could be damaged.) Outlet is Off  Outlet is on 
5 - Operation Buttons and Icons	Operation buttons and icons are provided to save data entries and updates. Enter data by typing or selecting entries and clicking the associated button. Some pages have buttons for specialized functions, such as clearing accumulated data logs. File operation icons are also provided to save or download files.
6 and 7- Current Alarms (when active)	An indicator appears as a notification in the refresh bar at the bottom of the page. For example, "Warning, some alarms fired, please refer to the Active Alarms Last Refresh: dd/mm/yyyy - hh:hh:ss" The words "Active Alarms" in the alarm notification sentence link to the Active Alarms page. The following symbols indicate the alarm level when an alarm threshold setting is exceeded: Active Alarms Present  High Critical Threshold Alarm  High Warning Threshold Alarm  Low Warning Threshold Alarm 

Table 8. Web Interface Region Descriptions (Continued)

Area	Description
8 - PDU Information	This panel displays identification information for the PDU that is providing data. The data fields include information about the PDU, including a model description, part number, serial number and the current PDU firmware version in use. NOTE For daisy-chained PDUs, you can select either PDU [0] for Host data and PDU [1], [2], [3], [4], [5], [6], or [7] for Device data.
9- Active Alarms Menu Selection	This indicator alerts you to the presence of currently active system alarms. It is in the menu hierarchy. When alarms are active, the text for Active Alarms is red. Selecting Active Alarms opens the Active Alarms page and displays the current active alarms.
10 - Menu Bar	The menu bar on the left panel contains links to pages for configuring the system or managing and monitoring the PDU. The menu hierarchy is expandable and collapsible. You can move the menu bar out of view using the horizontal scrolling tab at the bottom of the page. Click any selection in the menu bar to retrieve PDU performance data, review operation log information, or retrieve system or network configuration settings. The data on the selected page is presented in table format.

NOTE 1 The data that displays on the Web interface depends on the PDU model you are using. For example, a dual reporting window displays data for Input 1 and for Input 2 when the PDU has two inputs. In this chapter, the examples shown represent typical data displays reported from a single-input model.



NOTE 2 The Web interface supports Microsoft® Internet Explorer® 8.0 and greater, Firefox® (installed on Linux® or Windows®), and Google® Chrome®.

NOTE 3 On most pages, you can display relevant tooltips as you roll over images and fields.

Languages

The Web interface language is configurable. The following languages are available for your selection:

- ┆ English
- ┆ French
- ┆ Spanish
- ┆ German
- ┆ Italian
- ┆ Chinese Simplified
- ┆ Japanese
- ┆ Korean
- ┆ Chinese Traditional
- ┆ Polish
- ┆ Portuguese
- ┆ Czech

Accessing the Web Interface

The Web interface can be accessed using a standard Web browser.

**NOTE**

The PDU defaults to using DHCP when delivered. If you are unable to connect to the PDU through the network connection with this default address, see “Network Communication Configuration” on page 48 for more information.

To access the Web interface:

1. Open the Web browser.
 2. Enter a new PDU IP address or select the previously entered PDU IP address from the URL address drop list. The Authentication dialog displays.
 3. Enter a valid user name and password in the Authentication dialog box (see Figure 71). Click **Login** to continue or **Cancel** to exit.
-

**NOTE**

The default user name is “USERID” and the default password is “passw0rd.”

The image shows a web-based authentication dialog box. The title bar is labeled 'Authentication'. The dialog contains two text input fields, one for 'Login:' and one for 'Password:'. At the bottom of the dialog, there are two buttons: 'Login' and 'Cancel'.

Figure 71. Login Authentication

4. The PDU Overview page displays.
5. To access another page to observe and control the PDU, click any selection in the menu bar. The page that corresponds to your menu selection opens and displays in the main selection page window.

Menu Selections

Depending on the permission level of the user, the Menu Bar provides up to four groups of selections:

- ┆ Power Management
 - Overview
 - PDU [0] See NOTE 1
 - PDU [1]
 - PDU [2]
 - PDU [3]
 - PDU [4]
 - PDU [5]
 - PDU [6]
 - PDU [7] See NOTE 1
 - Branch Circuits
 - Devices
 - Outlets
 - Environment
 - Active Alarms
- ┆ Logs and Notifications
 - Logs
 - Trap Notification
 - Syslog
- ┆ Settings See NOTE 2
 - Access Accounts
 - System
 - Date & Time
- ┆ Network
 - TCP/IP
 - SNMP
 - EnergyWise
 - Security
 - ┆ Global
 - ┆ LDAP
 - ┆ RADIUS

NOTE 1 Menu selections for PDU [0], [1], [2], [3], [4], [5], [6], or [7] only display if the PDUs are configured in a daisy-chained configuration. If provided, selecting either PDU [0] or PDU [1], [2], [3], [4], [5], [6], or [7] displays the Overview page for the specified PDU only.



NOTE 2 The Settings menu is different from the Settings button. Selecting the **Settings** button on any power management page displays a separate window that allows you to change settings, such as alarm thresholds.

NOTE 3 See “Access Privileges” on page 90 for more information about levels of access privileges.

Power Management

Use the Power Management menu selections to see up-to-date operating measurements on the PDU Overview page. This page provides the present readings for the PDU that is reporting data. (If PDUs are daisy-chained, you can select to see Host or Device PDU Information.) The readings are reported per phase and, for 3Ph PDU models, all phases. This page includes data such as current, voltage, and crest factor. The outlet icons are green if the outlet is on and red if the outlet is off. Roll over the icon to see the outlet type and status.

The Outlets page provides present measurements or readings such as current or active power. You can set measurement thresholds for alarm or warning notifications as well. You can also set power schedules for outlets.

On the Outlet Settings dialog, the Power Schedule section allows you to schedule automatic power On, power Off, or Reboot actions for selected outlets. These schedules can be set for a single instance, daily or weekly activity at specified time intervals.

The Environment menu selection provides humidity and temperature data if you have an EMP installed. You can set measurement thresholds for alarm or warning notifications as well. It also provides open or closed status for two dry contacts.

You can check current alarms on the Active Alarms page to see a list of alarms by date, time, and description. See “Maintenance and Alarms” on page 127 for a list of alarms.

Logs & Notifications

Use the Logs & Notifications menu selections to see a list of the most recent events (Logs page). You can set trap receivers (Trap Notification page) and you can also view Syslog information.

Settings

The Settings menu selections that display depend on the type of privilege you have. These selections allow you to configure administrative settings, system attributes, and network access and control. Depending on privilege, this menu can include the following:

- **Access Accounts:** The Access Accounts page allows you to set up the SuperUser, local or remote administrators, local PDU-users and Outlet-users, and remote PDU-users and Outlet-users as individuals or groups. Access Accounts also allows the SuperUser to set up the LCD password.
- **System:** Use the System selection for identifying the administrator contact information, uploading an PDU or PDU Network Management and Control (eNMC) module configuration file, upgrading, restarting, or restoring factory default configuration to the PDU eNMC module. You can also reset the language and configure reporting for the EMP.
- **Date & Time:** The Date & Time page allows you to select the date format and set the date and time, either manually or by synchronizing with the Network Time Protocol (NTP) server. You can set the time zone and have the option of allowing Daylight Savings Time (DST).

Network

This selection allows you configure TCP/IP, SNMP, and Security settings for this PDU.

- ▮ **TCP/IP:** Use this page to configure Ethernet, IPv4, IPv6, DNS, and SMTP.
- ▮ **SNMP:** Use this page to configure general SNMP settings, SNMPv1 settings, and SNMPv3 settings. You can also access the Lenovo PDU Management Information Base (MIB) from this page.
- ▮ **Energy/Wise:** Use this page to enable or disable the Energy Wise feature.
- ▮ **Security:** Use this page to set port settings and Lightweight Directory Access Protocol (LDAP) settings.
 - **Global:** Set the port settings and the authentication mode on this page.
 - **LDAP:** Set the LDAP search configuration and global LDAP server global parameters for the specified LDAP servers on this page.
 - **RADIUS:** Add or edit the parameters for a primary or secondary RADIUS server on this page.

Access Privileges

The level of access privilege determines what the user will see and what actions the user can perform. For example, the level of access privilege determines which menu items the user can access or which fields display on individual setting and configuration dialogs. Any menu or dialog functions that are not included in the access privilege set for a user do not display, or are they are grayed-out.

These accounts can be configured not only for individuals, but also for groups. All remote users and administrators belong to a remote group and their access privileges are defined from this group. Remote accounts also provide a way to attach LDAP users (see “Configure Remote Group Access” on page 111).

Three user roles can be assigned these access privilege levels:

- ▮ Administrator
- ▮ Local or Remote PDU-User
- ▮ Local or Remote PDU-User/Outlet User

Administrator

There can be one SuperUser and up to eight standard local or remote administrators.

Only one user can be the SuperUser Administrator. This defaults to the local user, but a SuperUser should be assigned at first connection. This account is not accessible or editable by the standard administrators or PDU-Users/Outlet Users. The SuperUser always has read-write privileges to view and edit all data, plus the following privileges restricted only to the SuperUser:

- ▮ Exclusive access to modify the SuperUser account settings
- ▮ Can upload the communication module configuration file or upgrade the firmware
- ▮ Can access both the Serial interface and the Web interface
- ▮ Exclusive access to the Network and Date and Time Settings menu



NOTE

The default Administrator login is “USERID” and the default password is “passw0rd”. The login and password should be changed at the first connection. If the administrator loses the password or login, contact your service representative to recover it.

Local or Remote Administrator

Up to eight standard administrators (local or remote) can be assigned. Only accessible menu items display for the user according to the assigned permissions.



NOTE

This menu indicates the two PDU are daisy-chained, one host (PDU [0]) and one device PDU (PDU [1]).

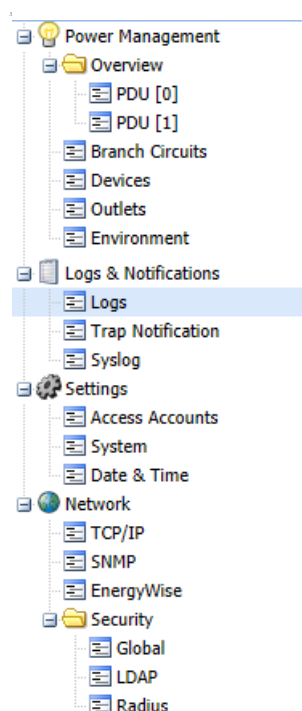


Figure 72. Administrator Menu View

Read-Write Access

A local or remote administrator who is assigned read-write access can perform the following:

- ▮ Access to up-to-date PDU data and measurements
- ▮ Create, modify, or disable an administrator or user account except for the SuperUser
- ▮ Create, modify, or disable User-Defined Groups
- ▮ Configure e-mail recipient addresses for e-mail notification to users
- ▮ Restart the communications module
- ▮ Cannot access the Serial interface; must use the Web interface only
- ▮ Access all menus on the Web interface
- ▮ Access to retrieved PDU up-to-date data and measurements
- ▮ Clear logs
- ▮ **Local Administrator Only.** Can switch on bootloader mode and upgrade firmware

Read-Only Access

A local or remote administrator with read-only access has limited privileges, including:

- ▮ Access to up-to-date PDU data and measurements
- ▮ Has the authority to change the password, but not the login (Remote PDU-Users cannot change the login or password)
- ▮ Cannot access the Serial interface; must use the Web interface only
- ▮ Can access the log and notifications submenu, but cannot clear the logs data
- ▮ Cannot configure the TCP/IP, SNMP Global Security, and LDAP settings

No Access

An administrator with no access is not authorized to access to the Web page.

PDU-User**Read-Write Access**

A local or remote PDU-User with read-write access privileges has access to the same functions as the administrator, except this user cannot change the account configuration for another user, such as e-mail addresses for notifications.

Only accessible menu items display for the user according to the assigned permissions.

**NOTE**

This menu indicates the two PDU are daisy-chained, one host (PDU [0]) and one device PDU (PDU [1]).

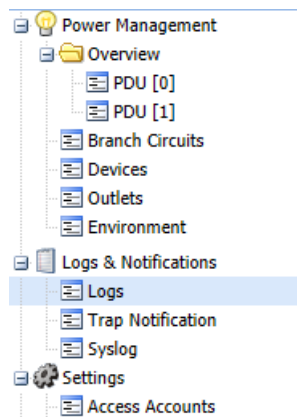


Figure 73. PDU-User Menu View

Read-Only Access

An PDU-User with read-only access has limited privileges, including:

- Access to up-to-date PDU data and measurements
- Has the authority to change the password and e-mail address, but not the login (Remote PDU-Users cannot change the login or password, but can change their own e-mail address.)
- Cannot access the Serial interface; must use the Web interface only
- Can access the log and notifications submenu, but cannot clear the logs data
- Cannot configure the TCP/IP, SNMP Global Security, and LDAP settings
- Cannot upload the communication module configuration file or upgrade the firmware
- Cannot change his profile or another user's account

No Access

An PDU-User with no access privileges is not authorized to access to the Web page.

Outlet-User

The Outlet-Users have only one read-write privilege. The Outlet-User has the authority to change his own password and e-mail address, but not the login. (Remote Outlet-Users cannot change the login or password, but can change their own e-mail address.) All other privileges are restricted to viewing PDU and assigned outlets data. Only accessible menu items display for the user according to the assigned permissions.

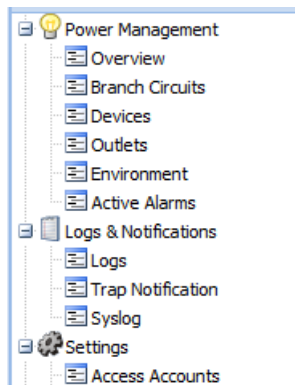


Figure 74. Outlet-User Menu View

Read-Only Access

Outlet-Users with read-only access have limited privileges, including:

- Access to retrieved PDU up-to-date data and measurements, but cannot change settings for the PDU
- Access to retrieved data for the outlets in user-defined groups assigned by the administrator
- Cannot access the Serial interface; must use the Web interface only
- Can access the log and notifications submenu, but cannot clear the logs data
- Cannot configure the TCP/IP, SNMP Global Security, and LDAP or other global settings
- Cannot upload the communication module configuration file or upgrade the firmware
- Cannot change his profile or another user's account

No Access

An Outlet-User (local or remote) with no access privileges is not authorized to access to the Web page.

Session Management

The following session management restrictions apply:

- ▮ There can only be one SuperUser with read-write access rights and up to eight multi-users with configurable access rights.
- ▮ Only one PDU-User or Outlet User with read-write access and at least one common outlet can be logged-in at a time.
- ▮ When the administrator connects, any existing read-write sessions are closed. The other user (or users) will be asked to authenticate and open a new read-only session.
- ▮ If a user with read-write access is logged in and another user with read-write access wants to log in, the following message displays: "Another user is logged in with R/W access. Continue as R/O?"
- ▮ PDU sessions are also limited in the following ways:
 - Only five standard sessions without Secure Sockets Layer (SSL) or Secure Shell (SSH) sockets are allowed.
 - Only two secure sessions can be running at the same time.
 - Only an administrator can have two simultaneous sessions open in Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure (HTTP/HTTPS), Telnet/SSH.



NOTE

During an HTTP/HTTPS or Telnet/SSH session, the session times out if there is no activity for five minutes. After a session times out, you must login again.

Overview

Review/Modify PDU Data



NOTE

Menu selections for PDU [0], [1], [2], [3], [4], [5], [6], or [7] only display if the PDUs are configured in a daisy-chained configuration. If provided, selecting either PDU [0] or PDU [1], [2], [3], [4], [5], [6], or [7] displays the Overview page for the specified PDU only.

1. Access the Web interface and log in.
2. The PDU: Overview page displays.
3. In the PDU Information panel, review PDU identification information.
4. In the main page, review PDU monitoring data.



NOTE 1

The phase information that displays reflects the PDU model. For example, the number of phases that display depends on whether the PDU is a single-phase, split-phase, or three-phase model. The phase labels also change depending on whether the model is a delta-wired or a wye-wired model.

NOTE 2

Roll the cursor over an outlet icon to see the type of outlet and the status (On or Off).

5. To modify PDU voltage and current threshold values, click the **Settings** button. The Settings dialog displays.

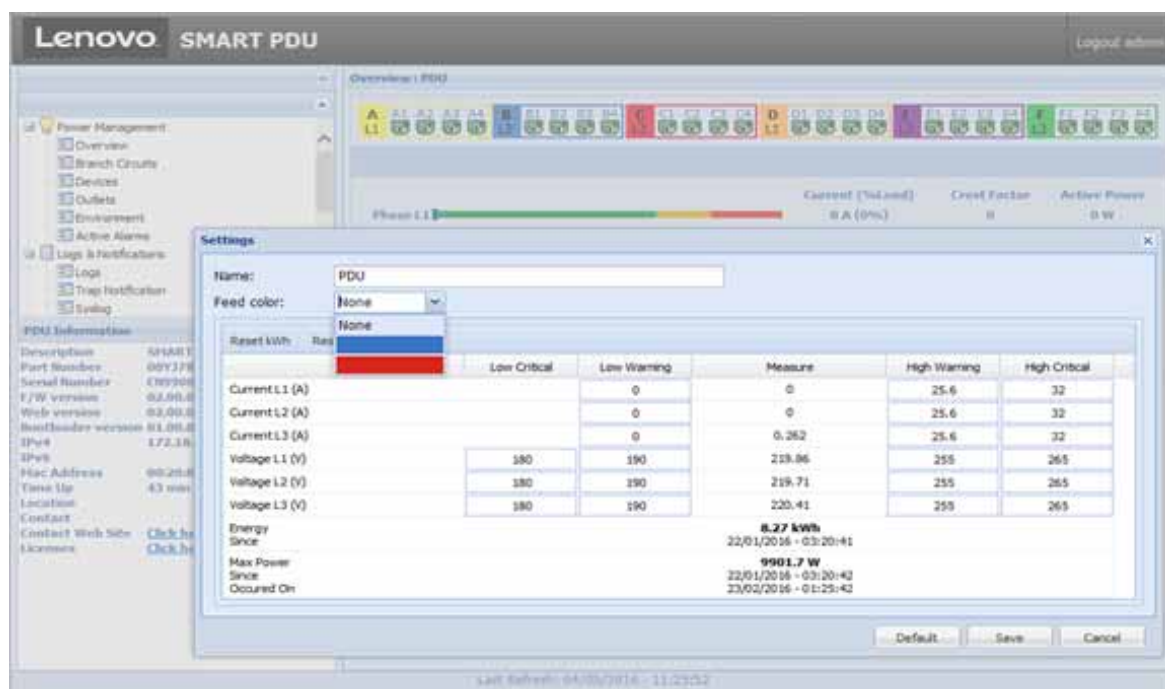


Figure 75. PDU Voltage and Current Threshold Values Settings

**NOTE**

Select a color for the input feed of an PDU by selecting the drop-down menu of the Feed color field. This color is displayed for the tag on the left of the section.

6. To enter new threshold values, type new values in any of the text boxes that follow, then click **Save**:
 - Low warning current threshold
 - High warning current threshold
 - High critical current threshold
 - Low critical voltage threshold
 - Low warning voltage threshold
 - High warning voltage threshold
 - High critical voltage threshold
7. To reset the threshold values to the default values, click **Default**, then click **Save**.
8. To reset a kWh (kilowatt hour) counter to zero, click **Reset kWh**, then click **Save**.

**NOTE**

If you do not save the action, the kWh counter remains unchanged.

9. To reset the maximum power counter to zero, click **Reset Max Power**, then click **Save**.
10. To cancel this action and return to the Overview page, click **Cancel**.

Branch Circuits



NOTE All sections, with or without breakers, are displayed.

Review Branch Circuits

1. Access the Web interface and log in.
2. Under Power Management, select **Branch Circuits**. The Branch Circuits main page displays.
3. In the main page, review the status of the sections:
 - You can see additional section details by clicking the red arrow next to the current percentage value in the Current (%Load) column, or double-clicking the row.
 - Specific outlet details are available when you roll over the outlet icons. Green icons mean that the outlet is ON.
 - Red icons mean one of the following conditions exists for the outlet:
 - At least one outlet is off
 - At least one outlet status is unknown
 - Communication is lost.
 - At least one outlet status is unknown and communication is lost.
4. To change settings for all sections associated with the PDU, check the checkbox next to the PDU name. Otherwise, check the checkbox beside the section name to change individual section settings. This selects the section or sections to which you will apply changes.

Change Groups Measurements Settings

1. Access the Web interface and log in.
2. Under Power Management, select **Branch Circuits**. The Branch Circuits main page displays.
3. To change measurement settings, select a section or sections and click **Groups measurement settings** in the top row of the page. The Groups measurement settings dialog displays.
4. To enter new threshold values, type new values in any of the text boxes that follow, click **Apply** and then click **Save**:
 - Low warning current threshold
 - High warning current threshold
 - High critical current alarm threshold
 - Low critical voltage threshold
 - Low warning voltage threshold
 - High warning voltage threshold
 - High critical voltage threshold
5. You can reset the total energy and the peak current of the selected sections. Click **Reset kWh** or **Reset max currents** to issue these commands:
 - **Reset kWh:** Resets the total cumulative energy of the sections and updates the date.
 - **Reset max currents:** Resets the peak current and updates the date for the PDUs that belong to this section.
6. Click **Save** to save the settings that were reset.

Turn Sections On or Off

1. Access the Web interface and log in.
2. Under Power Management, select **Branch Circuits**. The Branch Circuits main page displays.
3. To turn sections off or on with the selected expediency, check a checkbox a section or sections and select a setting from the **Turn On/Off sections** drop-down list in the top row of the page:
 - **On:** Immediately switch on the outlets of the selected groups.
 - **Immediate Off:** Immediately switch off the outlets of the selected groups.
 - **Delayed Off:** Switch off the outlets of the selected groups after a delay (set in the Outlet settings menu).
 - **Delayed Reboot:** Switch off the outlets of the selected groups after the switch-off delay, and then switch on after the reboot period. The switch-off delay and the reboot period are set in the Outlet settings menu.
4. A pop-up message asks if you are sure you want to switch the selected section on or off. Click **Yes** or **No**.
5. If Yes, a message pops up indicating that your changes were saved.

Change Individual Section Settings

1. Access the Web interface and log in.
2. Under Power Management, select **Branch Circuits**. The Branch Circuits main page displays.
3. To change individual section settings, click the section name. The Branch Circuit Settings dialog displays.
4. To enter new threshold values, type new values in any of the text boxes that follow, then click **Save**:
 - Low warning current threshold
 - High warning current threshold
 - High critical current alarm threshold
 - Low critical voltage threshold
 - Low warning voltage threshold
 - High warning voltage threshold
 - High critical voltage threshold
5. To reset the threshold values to the default, click **Default** and then **Save**.
6. You can reset the total energy and the peak current of the selected sections. Click **Reset kWh** or **Reset max currents** to issue these commands:
 - **Reset kWh:** Resets the total cumulative energy of the sections and updates the date.
 - **Reset max currents:** Resets the peak current and updates the date for the PDUs that belong to this section.
7. Click **Save** to save the settings that were reset.

Devices

Rules for Devices

The following rules for Devices apply:

- ▮ A maximum of 32 Device Groups can be defined.
- ▮ A device can be connected to a maximum of two PDUs.
- ▮ A device can be connected to a maximum of six outlets per PDU, unless two PDUs are daisy-chained. In this case, outlets can belong to a maximum of two daisy-chained PDUs
- ▮ At the top of the outlets settings grid, a warning advises about this limit. If the limit is reached, all unchecked outlets in the PDU column are disabled.
- ▮ An outlet can only be connected to one device at the same time. Already connected outlets are disabled in the grid.
- ▮ Some measures and some actions are available on each Device Group and others are specifically available on each PDU that belongs to the Device Group.
- ▮ Users cannot select the same PDU in the two columns of the Outlets settings grid. If users select the same PDU in the first column that was selected in the second column, then the previous PDU that was defined in the first column will be set in the second column.
- ▮ Saving a device with outlets from an unknown PDU will display outlet numbers in red to show a connection failure.
- ▮ If a PDU is not daisy-chained, outlet settings grid will display only one PDU column when adding a new device.
- ▮ If a PDU is not daisy-chained, but users display settings of a device connected to two PDUs, the outlet settings grid will display the two PDU columns.
- ▮ Clicking **Apply** does not save data; only clicking **Save** will save your changes.

Review Devices

1. Access the Web interface and log in.
2. Under Power Management, select **Devices**. The Devices main page displays.
3. In the Devices panel, review the status of the devices. Note that the green circle with a check indicates that all outlets are on. The red circle with an exclamation mark indicates one of the following:
 - ▮ At least one outlet is off
 - ▮ At least one outlet status is unknown
 - ▮ Communication is lost.
 - ▮ At least one outlet status is unknown and communication is lost.
4. To see which condition applies, roll over the red circle with an exclamation mark.

NOTE 1 On the main Device page, the measurements that display are the sum of instantaneous measurements obtained on each outlet.



NOTE 2 For energy, the reference date is either the date when the group was created or the date when the user reset its' energy.

5. Click the checkbox next to the device name or double-click the row to see load-balancing details about this device, including the outlet status, the gauge of the instantaneous current, and the peak current (see Figure 76).

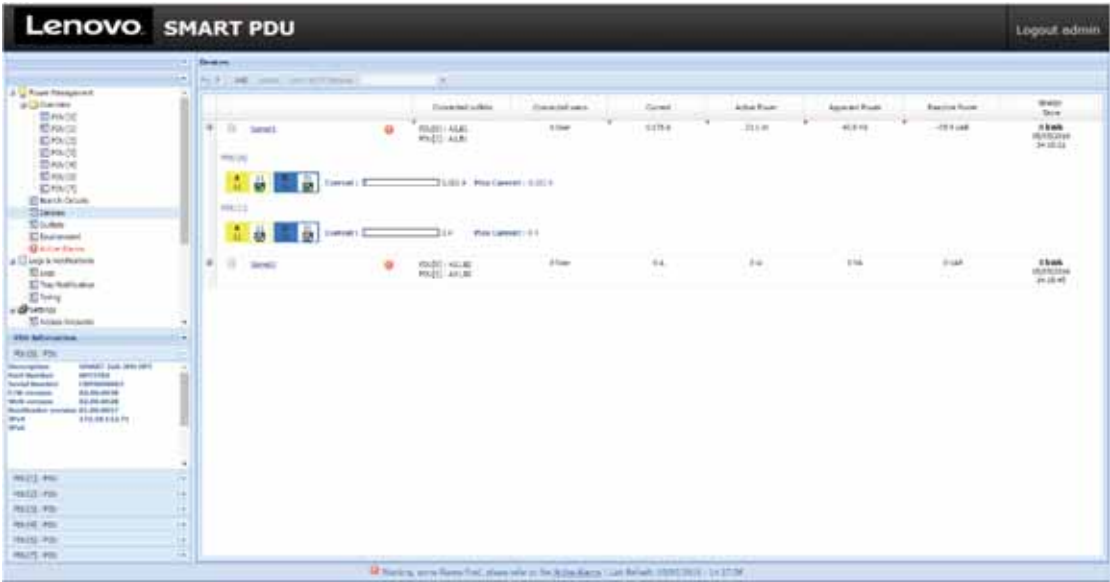


Figure 76. Expand Load-Balancing Details on Row for Device

NOTE 1 Use the cursor to roll over outlet data in the row load-balancing details display to see additional information. For example, in the load balancing panel, a tooltip containing complementary information concerning outlets is displayed when you roll over the outlet images.

NOTE 2 The display may be highlighted with a red color if:



- If there is a connection failure on a PDU, problems are highlighted in red numbers above the outlet image to locate their position in the unknown PDU.
- Some load balancing value can be wrong if related PDU has out-of-date firmware. These values are highlighted in red and display a tooltip.

NOTE 3 Note that only 32 devices are allowed, so the **Add** button is grayed-out (unavailable) when the maximum number of devices are listed.

NOTE 4 Perform an action on several devices at the same time by selecting the applicable device checkboxes and clicking the action button in the bar above the window.

Add Devices

Connected outlets are outlets that power the given device. To identify those outlets, initially select the PDU to which they are connected. (In a Daisy chain, you can chose from up to eight PDUs. In a setup with no daisy-chained PDUs, but just a single unit, only one selection value is provided.)

For example, when you have at least two daisy-chained PDUs, two columns display, allowing you to select two supporting PDUs and the two corresponding check boxes lists. Then, you check the boxes corresponding to the outlets powering the device your are defining.

To add devices:

1. Access the Web interface and log in.
2. Under Power Management, select **Devices**. The Devices page displays.
3. Click **Add** in the top bar of the page. The Device Settings dialog displays.

4. Type the name in the **Name** field (31 characters maximum).
5. In the Connected outlets panel, select the PDU that the device is plugged into.
6. Select the outlets in each PDU (unavailable outlets are grayed-out).
7. Select the power schedule of the device in the Power Schedule area.
8. Click **Save**. A message displays to alert you that if a Power Schedule was previously defined on outlets in the Outlets settings menu, that Power Schedule will be overwritten. The new device name displays after a refresh.

Delete Devices



NOTE

It is recommended that you delete device groups when they are no longer used.

1. Access the Web interface and log in.
2. Under Power Management, select **Devices**. The Devices page displays.
3. In the Devices panel, select the checkbox associated with one or more device groups.
4. Click **Delete**.
5. Click **Save**.

Turn Devices On or Off

1. Access the Web interface and log in.
2. Under Power Management, select **Devices**. The Devices page displays.
3. In the Devices panel, check the checkbox associated with one or more device groups.
4. Select one of the following actions from the drop-down list beside **Turn on/off devices**:
 - **Turn on**: Immediately switch on the devices of the selected groups.
 - **Turn Immediate Off**: Immediately switch off the devices of the selected groups.
 - **Turn Delayed Off**: Switch off the devices of the selected groups after a delay (set in the Outlet settings menu).
 - **Turn Delayed Reboot**: Switch off the devices of the selected groups after the switch-off delay, and then switch on after the reboot period. The switch-off delay and the reboot period are set in the Outlet settings menu.
5. A pop-up message asks if you are sure you want to switch the selected section on or off. Click **Yes** or **No**. If Yes, a message pops up indicating that your changes were saved.

Change Device Settings

1. Access the Web interface and log in.
2. Under Power Management, select **Devices**. The Devices page displays.
3. In the Devices panel, click the name of a device or devices. The Device Settings dialog displays.
4. To enable the Power schedule to apply it to this device, check the checkbox for Power Schedule. This indicates that the power schedule is enabled for this device or devices. Unless None is selected for the Action value, you can make changes in the Power schedule fields.

5. In the Action field, select either **On**, **Off**, or **Reboot** from the drop-down list.
 - **None:** The actions in this schedule are not executed. This is the default upon opening this dialog. (You can use this setting to hold the settings for future activation.)
 - **Off:** Select this value to switch off the outlets of the current device according to the corresponding schedule you specify.
 - **On:** Select this value to switch on the outlets of the current device according to the corresponding schedule you specify.
 - **Reboot:** Select this value to switch off and then switch back on the outlets of the current device according to the corresponding schedule setting. The delay between the Off and the On can be set on the Outlet Settings dialog using the **Power Reboot Period** field (see Step 9 on page 103). With this setting, additional actions scheduled by the Further Actions selections are disabled.
6. Set the time schedule for this action by selecting a time from the "at:" drop-down list.
7. Set the days or date of the action using one of the following:
 - If you want to set up a schedule of days for this action, check the **Recurrent**. Check the checkbox next to the name of the days from the "Active Days" drop-down list. (You can exclude some days using this setting.) When settings are saved, the "Date of Action" value is automatically set to the date of the first occurrence of the action.
 - If you want to set a single date to execute an action or further action, uncheck the **Recurrent** checkbox. The Date of Action field and calendar drop-down list displays. Select the date from the calendar.

**NOTE**

"Date of Action" fields are only available when the "Recurrent" checkbox is unchecked. This field specifies the date when the action will be executed, but only once.

8. Click **Save**.
9. **Optional.** You can add additional scheduled actions. For example, suppose your first action is On. You can pair it with a subsequent Off action. The schedule for this second action is set by selecting **Off** from the Further Action drop-down list and setting values in the date and time fields. By default, this second action is set to "None," meaning nothing more will happen.
 - **None:** The actions in this schedule are not executed at the specified time. This is the default if the Action is set to Off or On.
 - **Off:** Select this value to switch off the outlets of the current device according to the corresponding schedule setting.
10. Set the schedule for this action by selecting a date and time from the drop lists for the "at:" and Date of Action" field.

**NOTE**

This date and time must occur after the date and time set for the first action.

11. Click **Save**.
12. If the PDUs do not have a connection failure, you can reset the total energy of the Device Group and the peak current of each PDU Device group. Click **Reset kWh** or **Reset max currents** to issue these commands:
 - **Reset kWh:** Resets the total cumulative energy of the Device Group and updates the date.
 - **Reset max currents:** Resets the peak current and updates the date for the two PDUs that belong to this Device group.

13. Click **Save** to save the settings that were reset.

**NOTE**

If there is a connection failure on a PDU, you cannot reset the device energy value or the maximum currents. The current measurements display in red to indicate that there is a problem with that PDU.

Outlets

**NOTE**

The display varies depending on the profile assigned to the user.

Review/Modify PDU Outlets

**NOTE**

The On/Off/reboot/last-known state is associated with the “Control” feature for PDUs.

1. Access the Web interface and log in.
2. Under Power Management, select Outlets. The Outlets page displays.
3. Review basic monitoring information for individual outlets.
4. Click the outlet name to display a dialog for renaming the outlet.
5. To apply an operative action for a selected outlet, select the corresponding checkbox and then select one of the following values from the Turn On/Off drop-down list in the top bar, then click **Save**.
 - ▮ **On**: Immediately turn on the selected outlets.
 - ▮ **Immediate Off**: Immediately turn off the selected outlets.
 - ▮ **Delayed Off**: Turn off the selected outlets after a delay (set on the Outlet settings dialog).
 - ▮ **Delayed Reboot**: Turn off the selected outlets after the turn-off delay, and then turn on the selected outlets after the reboot period (the turn-off delay and reboot period are set on the Outlet Settings dialog).
6. To modify PDU threshold values for a specified outlet, click the link on the group friendly name. The Outlet Settings dialog displays.
7. To set whether an outlet state (On, Off, or Reboot) can be changed, check or uncheck the Enable Switching check box, then click **Save**.
 - ▮ **Disabled**: Uncheck the check box to disable the setting, which indicates that the outlet state cannot be changed.
 - ▮ **Enabled**: Check the check box to enable the setting, which indicates that the outlet state can be changed.
8. To set the state of the outlet with the PDU is powered on, select one of the following values from the State on Device Startup drop-down list, then click **Save**:
 - ▮ **On**: The outlet is powered after a duration of time set in the Outlet Switch On After field.
 - ▮ **Off**: The outlet is not powered.
 - ▮ **Last Known State**: The outlet is powered on if it was On when the PDU was powered Off. Otherwise, the outlet is not powered.

9. **Administrator or User with Read/Write/Control only.** To specify the duration an outlet will be Off before switching On during a reboot, type the number of seconds the outlet should be Off in the Power Reboot Period(s) text box. Click **Save**.

**NOTE**

This setting can be overwritten by the Power Reboot Period defined for groups of outlets on the Group Settings dialog.

10. To enter new threshold values, type new values in any of the text boxes that follow, then click **Save**:
 - Low warning current threshold
 - High warning current threshold
 - High critical current threshold
11. To reset the threshold values to the default values, click **Default**, then click **Save**.
12. To reset a kilowatt hour (kWh) counter to zero, click **Reset kWh**, then click **Save**.

Environment

Configure Environment Sensor Settings

1. Access the Web interface and log in.
2. Under Power Management, select Environment. The Environment page displays.
3. In the Environment panel, review the present PDU environment monitoring temperature and humidity data. Also review the status of installed dry contacts, open or closed.

NOTE 1

The environmental monitoring data panel only displays data under these circumstances:

- if the EMP is installed and configured in the system
- if the user read-write access rights

**NOTE 2**

The environmental monitoring data panel displays the value of the last EMP value read as follows:

- When the EMP is disconnected, the startup value will be 0 (zero).
 - When the EMP is first connected, the startup value will be 0 (zero) because the last known reading was taken before a sensor was connected.
 - When the EMP remains connected, the startup value is the last known EMP reading.
-

4. To modify environment threshold values, or to receive alarms when dry contacts change state, click the **Settings** button located in the lower, right-hand corner of the Web interface screen. The Environment Settings dialog displays.

**NOTE**

In the Environment Settings dialog, the measure column displays the present status or state of the dry contacts. This is a read-only column.

5. To select default values for thresholds or dry contacts, click **Default**.

6. To enter new threshold values, type new values in any of the text boxes that follow, then click **Save**:
 - ▮ Low critical humidity alarm threshold
 - ▮ Low warning humidity threshold
 - ▮ High warning humidity threshold
 - ▮ High critical humidity alarm threshold
 - ▮ Low critical temperature alarm threshold
 - ▮ Low warning temperature threshold
 - ▮ High warning temperature threshold
 - ▮ High critical temperature alarm threshold
7. To choose if you are notified when a dry contact state changes (Open or Closed), select one of the settings from the drop-down list under Open or Closed for the specified contact, then click **Save**:
 - ▮ **Informational**: No alarm is generated.
 - ▮ **Alarm**: An alarm is generated when the specified dry contact is Open or Closed.
8. To reset the threshold values to the default values, click **Default**, then click **Save**.
9. To cancel this action and return to the Environment page, click **Cancel**.

**NOTE**

To change the temperature scale to Celsius or Fahrenheit unit of measurement (°C or °F), see "Set General System Settings" on page 112.

Power Schedule

**NOTE**

Power schedules can be set by an Administrator with Read/Write/Control only.

Define a Power Schedule

1. Access the Web interface and log in.
2. Under Power Management, select Outlets. The Outlets page displays.
3. Select an outlet and click the outlet name. The Outlet Settings dialog displays.
4. Check the Power Schedule checkbox.
5. Add an action in the first action block by selecting either **On**, **Off**, or **Reboot** from the drop-down list.
 - ▮ **None**: The actions in this schedule are not executed. This is the default upon opening this dialog. (You can use this setting to hold the settings for future activation.)
 - ▮ **Off**: Select this value to switch off the current outlet according to the corresponding schedule you specify.
 - ▮ **On**: Select this value to switch on the current outlet according to the corresponding schedule you specify.
 - ▮ **Reboot**: Select this value to switch off and then switch back on the current outlet according to the corresponding schedule setting. The delay between the Off and the On can be set on the Outlet Settings dialog using the **Power Reboot Period** field (see Step 9 on page 103). With this setting, additional actions scheduled by the Further Actions selections are disabled.
6. Set the time schedule for this action by selecting a time from the "at:" drop-down list.

7. Set the date schedule for this action by selecting a date from the "Date of Action" selection calendar.

**NOTE**

"Date of Action" fields are only available when the "Recurrent" checkbox is unchecked. This field specifies the date when the action will be executed, but only once. If you want the action to be scheduled to repeat, see Step 11.

8. **Optional.** You can add additional scheduled actions. For example, suppose your first action is On. You can pair it with a subsequent Off action. The schedule for this second action is set by selecting **Off** from the Further Action drop-down list and setting values in the date and time fields. By default, this second action is set to "None," meaning nothing more will happen.
 - ▮ **None:** The actions in this schedule are not executed at the specified time. This is the default if the Action is set to Off or On.
 - ▮ **Off:** Select this value to switch off the current outlet according to the corresponding schedule setting.
 9. Set the schedule for this action by selecting a date and time from the drop lists for the "at:" and Date of Action" field.
-

**NOTE**

This date and time must occur after the date and time set for the first action.

10. Click **Save**.
 11. Do you want to make the Power Schedule recurrent, so that specified schedules are executed multiple times?
 - If yes, go to Step 12.
 - If no, this procedure is completed.
-

**NOTE**

When a power schedule is recurrent, you set the schedule to repeat on specified days. To set any schedule, including recurrence, the Action or Further action cannot be set to "None."

12. Check the Recurrent checkbox.
13. In the active days field, select which day or days to be affected by this action. When settings are saved, the "Date of Action" value is automatically set to the date of the first occurrence of the action.
14. Click **Save**.

Active Alarms

**NOTE**

When the Active Alarms menu item in the menu bar list is red and displays an exclamation mark icon, an alarm is active.

Review Active Alarms

1. Access the Web interface and log in.
2. Under Power Management, select Active Alarms. The Active Alarms page displays.
3. Ensure the PDU operation button in the upper left corner is not collapsed. If so, expand it to see the list of alarms.
4. Review the alarm detection date/time, description, the threshold setting, and the value reading that triggered the alarm.

-
- NOTE 1** The term “active alarms” indicates that the alarm is currently set. When an alarm is no longer active, it is removed from this page.
-  **NOTE 2** The format of the date is set on the System Date & Time submenu (see “Date & Time” on page 114).
-

Logs

Clear the Event Log

1. Access the Web interface and log in.
2. Under Logs & Notifications, select Logs. The Logs page displays.
3. Click **Clear**.

-
-  **NOTE** Only a user with read-write access can clear the log. Click the arrow beside Type to sort the order of the columns, to apply filters to see the logs for a specific data type, or to sort all data in ascending or descending order.
-

Download the Event Log as a Comma Separated Value File

1. Access the Web interface and log in.
2. Under Logs & Notifications, select Logs. The Logs page displays.
3. Click **Save to File**. The File Download dialog displays.
4. Click **Save**. The Save As window displays.
5. From the **Save in** drop-down list, specify where the file should be downloaded.
6. Either accept the default file name (logevent.csv) or enter a new file name.
7. Click **Save**.

-
-  **NOTE** To import a CSV file in Excel, select the UTF-8 format.
-

NOTE For daisy-chained PDUs:

- PDU type 00 indicates the Host PDU [0] logs.
 - PDU type 01 indicates the Device PDU [1] logs.
 - PDU type 02 indicates the Device PDU [2] logs.
 -  ▸ PDU type 03 indicates the Device PDU [3] logs.
 - PDU type 04 indicates the Device PDU [4] logs.
 - PDU type 05 indicates the Device PDU [5] logs.
 - PDU type 06 indicates the Device PDU [6] logs.
 - PDU type 07 indicates the Device PDU [7] logs.
-

Trap Notification

Define the Trap Receivers

1. Access the Web interface and log in.
2. Under Logs & Notifications, select Trap Notification. The Trap Notification page displays.
3. Click a linked Trap Receiver in the Name column to select the trap receiver to define.
4. Type the name to identify the trap receiver. This value is not used to send traps.
5. Choose one of the following protocols:
 - **Disable:** The trap receiver is disabled. (No trap is sent to this user and the **Test** button is deactivated.)
 - **SNMP v1:** Traps are sent over SNMPv1 protocol. (It must be compliant with the SNMP version defined in "Enable/Disable the SNMP Agent" on page 118.)
 - **SNMP v3:** Traps are sent over SNMPv3 protocol. (It must be compliant with the SNMP version defined in "Enable/Disable the SNMP Agent" on page 118.)
6. Type the trap receiver IPv4 / IPv6 address or its host name.
7. Type the trap community (public or private).
8. From the On Event drop down list, select one of the following trap sources:
 - **Disable:** The trap receiver is disabled and the **Test** button is deactivated.
 - **All Alarms:** The trap receiver is enabled.
9. Click **Save**. If desired, test the configuration (see "Test Trap").
10. Click **Test**. (See the "Test Trap" section that follows for more information).

Test Trap**NOTE**

To receive the test trap #53, the trap receiver must be configured with a protocol compliant with the one defined as the trap source (see “Enable/Disable the SNMP Agent” on page 118).

This action consists of sending a test trap (#53) to all configured and enabled trap receivers. To achieve this action, the following requirements must be met:

- The PDU Network Management and Control (eNMC) module is running in Normal Operation mode.
- The PDU Network Management and Control (eNMC) module is connected to the Local Area Network (LAN).
- The PDU Network Management and Control (eNMC) module owns a valid IP address.
- The SNMP must be enabled: SNMPv1, SNMPv3, or SNMPv1&v3.

The target trap receiver configuration requires a valid IP address and the trap receiver protocol must match the configured SNMP version.

**NOTE**

See “Enable/Disable the SNMP Agent” on page 118.

Syslog**Retrieve or Modify Syslog Data**

1. Access the Web interface and log in.
2. Under Logs & Notifications, select Syslog. The Syslog Server page displays.
3. Review to the Syslog status, the port number, and the protocol for the specified Syslog server.
4. To enable or disable a server, click the check box beside the Syslog server name and click the **Enable** or **Disable** button.
5. To modify the settings for a server, click the Syslog name. The Syslog Server Settings dialog displays.
6. In the Syslog Server Settings dialog, enable or disable the selected server from the Enable Server drop-down list. You can also change the following:
 - port number and the protocol selection to either UDP or TCP from the Protocol drop-down list
 - message transfer method according to:
 - 5424: Syslog Protocol IETF
 - 5425: TLS
 - 5426: Transfer over UDP
 - 6587: Transfer over TCP
 - 3167: Syslog protocol IETF (obsolete)
 - facility code used for all messages from 1 to 23
 - use of unicode byte order mask (BOM) according to RFC 5424
7. When you finish modifying Syslog server settings, click **Save** or **Cancel**.
8. (Optional). Click **Test** to test the configuration.

Access Accounts

Configure the SuperUser

1. Access the Web interface and log in.
2. Under Settings, select Access Accounts. The Access Accounts page displays.
3. In the Admin Access panel, perform the following:
 - ▮ Type the SuperUser login.
 - ▮ Type the SuperUser password.
 - ▮ Type the SuperUser password again.
4. Click **Save**.

Configure the E-mail Notification Settings



NOTE 1 By default, an e-mail address is attached to each account.

NOTE 2 Any user can change his own e-mail address.

1. Access the Web interface and log in.
2. Under Settings, select Access Accounts. The Access Accounts page displays.
3. In the Admin Access panel, click the e-mail address link.
4. The e-mail recipient address displays. If needed, change the address.
5. If needed, type the descriptive text to identify the e-mail receiver.
6. Enable or disable the e-mail receiver in the status drop-down list.
7. Check the Attached Files check box to attach the event log file to the e-mail sent to this receiver, or uncheck the box to send the e-mail without the event log file.
8. Select the date of the next report using the date picker or manually enter the date in mm/dd/yyyy format.
9. Set the frequency of the report if this recipient should receive regular reports.
10. Set the time of delivery using the drop-down list.
11. From the On Event drop down list, select one of the following:
 - ▮ **Disable**: E-mail delivery is disabled and the **Test** button is deactivated.
 - ▮ **All Alarms**: E-mail is enabled and the **Test** button is activated.
12. Click **Test** to send a test e-mail.
13. Otherwise, click **Save** or **Cancel**.

Configure the LCD Password



NOTE 1 Only an administrator can activate, deactivate, or modify the LCD password.

NOTE 2 There can only be one LCD password on the PDU.

1. Access the Web interface and log in.
2. Under Settings, select Access Accounts. The Access Accounts page displays.

3. In the LCD Access panel, perform the following:

- Activate the feature to change the password.
- Type the LCD password.
- Type the LCD password again.

4. Click **Save**.

Configure Local User Access

NOTE 1 Only an administrator can create or modify a user account.



NOTE 2 Local users can use this user name and password for authentication if the authentication mode selected in the Network Security Global submenu is Local (see "Set Authentication Mode" on page 122).

NOTE 3 The User name is used for authentication. It must be unique. If there is a name conflict when you are creating a new account, a warning message displays.

1. Access the Web interface and log in.
2. Under Settings, select Access Accounts. The Access Accounts page displays.
3. In the Multi-User Access panel, select **Add a local user** from the Add drop down list. The Users Settings dialog displays.
4. Perform the following:
 - Type the user's login user name to replace the default name.
 - Type the user's password (minimum of five characters).
 - Type the user's password again.
5. Choose one of the following profile characteristics:
 - **Admin:** This user has administrator privileges and controls the access of other users to the Web interface. The Administrator can restart the communications module, but cannot perform a firmware upgrade.
 - **PDU User:** This user has access to the PDU and either read only or restricted read-write privileges.
6. Choose one of the following security levels:
 - **No Access:** The user is not allowed to access the Web interface.
 - **Read-Only:** The user can access the Web interface, view the measures, and view the thresholds of the outlets and groups. This user is not allowed to change any settings or perform actions.
 - **Read/Write:** The user can access the Web interface, view the measures, and is allowed to change settings.
7. To configure an e-mail address for this account, click the link of the e-mail address corresponding to this user. See "Configure the E-mail Notification Settings" for more information.
8. Click **Save**.
9. To enable an e-mail address for this account, click the link on the e-mail address under the e-mail Address column.

Configure Remote Group Access



NOTE 1 A remote account is an account that will be created on the communications module in order to be attached to LDAP users so they can use the PDU. The account should already exist on the LDAP database.

NOTE 2 These LDAP users will use their LDAP login/password for authentication on the module.

1. Under Settings, select Access Accounts. The Access Accounts page displays.
2. In the Multi-User Access panel, select **Add a remote group** from the Add drop down list. The Remote Group Settings dialog displays.
3. Type the remote group login user name to replace the default name.



IMPORTANT

This login user name must match the group name that the user has in the LDAP database.

4. Choose one of the following profile characteristics:
 - **Admin:** This remote group has administrator privileges and controls the access of other users to the Web interface.
 - **PDU User:** The administrator assigns this remote group either read only or read-write privileges to this user.
5. Choose one of the following security levels:
 - **No Access:** The user is not allowed to access the Web interface.
 - **Read-Only:** The remote group can access the Web interface, view the measures, and view the thresholds of the outlets and groups. This user is not allowed to change any settings or perform actions.
 - **Read/Write:** The remote group can access the Web interface, view the measures, and is allowed to change settings.
6. To configure an e-mail address for this account, click the link of the e-mail address corresponding to this user. See "Configure the E-mail Notification Settings" for more information.
7. Click **Save**.
8. To enable an e-mail address for this account, click the link on the e-mail address under the e-mail Address column.

System

NOTE The Web interface will not be available as follows:



- during firmware upgrades using the **Upgrade network management card** button
- during a communications module restart using the **Restart network management card** button
- during restoration to factory defaults using the **Restore factory to default settings** button

Set General System Settings



NOTE

Refresh the Web pages (press F5) to see changes to the general system settings.

1. Access the Web interface and log in.
2. Under Settings, select System. The System Settings page displays.
3. In the General panel, type the Device Administrator Contact Name and the Device location in the text boxes.
4. To change the language, select a language from the drop down list (see Figure 77).

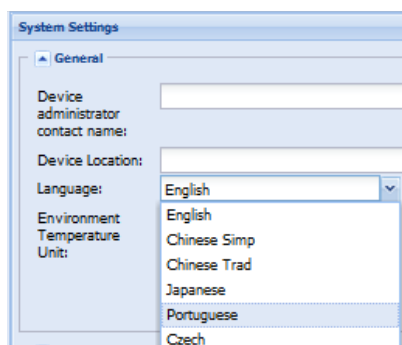


Figure 77. Change Language on System Settings Page

5. Select °C or °F in the Temperature drop-down list to change the temperature scale (Celsius or Fahrenheit unit of measurement).
6. Click **Save**.

Enable/Disable Firmware Upgrade

1. Access the Web interface and log in.
2. Under Settings, select System. The System Settings page displays.
3. In the Network Management Card panel, choose whether the firmware upgrade functionality can be used:
 - **Enabled:** Check the check box to use the firmware upgrade functionality (default).
 - **Disabled:** Uncheck the check box to disable the firmware upgrade functionality.
4. To save your changes, click **Yes** in response to the message prompt.

Configure PDU Network Management and Control Module

1. Access the Web interface and log in.
2. Under Settings, select System. The System Settings page displays.
3. In the Network Management Card Configuration panel, choose whether the IP setting and/or Daisy Chain settings should remain unchanged after a default factory reset of the eNMC module.
 - ▮ **Enabled:** Check the check box beside the Keep IP parameters when “Restore Factory Default Settings” to retain IP settings at their current values after restoration. Check the check box beside the Keep Daisy Chain parameters when “Restore Factory Default Settings” to retain IP settings at their current values after restoration.
 - ▮ **Disabled:** Uncheck the check box to reset IP settings (or Daisy Chain settings) to default values (default).
4. To select and store an eNMC module configuration file to be used during an upgrade, use **Browse** to review and select the configuration file.



NOTE

When uploading a file, you cannot write the file path in the text field. You must select the file from the file explorer window that displays when you click **Browse**.

5. Click either **Upload** or **Download Configuration** and a message is provided to tell you if the file uploaded successfully or failed to upload:
 - ▮ **Upload:** Gets the list of the PDU XML parameters from a file selected by the browser and sends it to the PDU. When the upload completes, a pop-up confirmation message displays:
The file has been successfully uploaded.
You must reboot your Network Management Card for changes to take effect.
Note: This will NOT restart the PDU or change the power status of the outlets.



NOTE

Changes to network parameters require a restart, but all other setting changes will take effect immediately.

- ▮ **Download Configuration:** Stores a list of the PDU XML parameters in a file selected by the browser.
6. To restore the eNMC module to factory defaults, click **Restore Factory to default settings**. A pop-up confirmation message displays:
Are you sure you want to restore the factory default settings of the Network Management Card?
Note: This will NOT restart the PDU or change the power status of the outlets.

Perform Firmware Upgrade



NOTE

A firmware upgrade can only be performed by a SuperUser. This upgrades the firmware and the Web page. The Web interface will not be available during the upgrade.

1. Access the Web interface and log in.
2. Under Settings, select System. The System Settings page displays.
3. In the Network Management Card panel, ensure the firmware upgrade functionality is enabled and that the upgrade file has been downloaded.

4. To upgrade the communications module, click **Upgrade network management card**. The upgrade is launched immediately.
5. Click **Restart network management card**.
6. When the upload of the image file completes, the following message displays:
 Your file was correctly uploaded.
 Please wait about three minutes while the image writes to your flash device,
 then click the browser refresh button.
 Click OK to restart the card and begin the upgrade of the firmware.

PDU Configuration

1. Access the Web interface and log in.
2. Under Settings, select System. The System Settings page displays.
3. Ensure that the Device Administrator Contact Name and the Device location have been typed in the text boxes.
4. To select and store an eNMC module configuration file to be used during an upgrade, use **Browse** to review and select the configuration file.



NOTE

When uploading a file, you cannot write the file path in the text field. You must select the file from the file explorer window that displays when you click **Browse**.

5. Click either **Upload** or **Download Configuration** and a message is provided to tell you if the file uploaded successfully or failed to upload:
 - **Upload:** Gets the list of the PDU XML parameters from a file selected by the browser and sends it to the PDU.
 - **Download Configuration:** Stores a list of the PDU XML parameters in a file selected by the browser.



NOTE 1

The file to upload must be a file compatible with the hardware of the PDU. If not, the upload does not process due to an incompatibility error.

NOTE 2

You do not need to restart the card after a successful upload.

Date & Time

Manually Configure the Date and Time

1. Access the Web interface and log in.
2. Under Settings, select Date & Time. The Date & Time page displays.
3. In the Global Settings panel, choose the date format from the drop-down list.
4. Click **Save**.
5. Click the **Set manually** radio button.
6. Type the date according to the format defined by Date Format, or select the date using the date picker.
7. Type the time or select a time from the drop-down list. The time format is *hh:mm:ss*, where *hh* = hours, *mm* = minutes, *ss* = second.
8. Click **Save**.

**NOTE**

Changing the date to a future date and then reverting the date to the current date may affect the order of the display in the logs.

Automatically Configure the Date and Time

1. Access the Web interface and log in.
2. Under Settings, select Date & Time. The Date & Time page displays.
3. In the Global Settings panel, choose the date format.
4. Click **Save**.
5. In the Global Settings panel, click the **Synchronize with NTP Server** radio button
6. Type the Time Server IPv4 / IPv6 address or host name.
7. Choose the time zone from the drop-down list.
8. Choose one of the following DTS (Daylight Saving Time) options:
 - **No Daylight Saving**
 - **European DST**
 - **American DST**
9. Click **Save**.

**NOTE**

The PDU Network Management and Control (eNMC) module retrieves the date and time from the configured NTP server every hour.

TCP/IP**NOTE**

The Web interface will not be available during a communications module restart using the **Restart network management card** button.

Configure the Ethernet Link Speed and Duplex Mode**NOTE**

By default, the Ethernet link speed and duplex mode is configured on “auto-negotiation” which means the eNMC module adapts its Ethernet speed and duplex mode to the network on which it is connected. However, it is possible to force the following modes:



- Auto-negotiation
- 100 Mbps Full Duplex
- 100 Mbps Half Duplex
- 10 Mbps Full Duplex
- 10 Mbps Half Duplex

1. Access the Web interface and log in.
2. Under Network, select TCP/IP. The TCP/IP page displays.

3. In the Ethernet panel, choose one of the following link speed and duplex modes from the drop-down list:
 - Auto-negotiation
 - 100 Mbps Full Duplex
 - 10 Mbps Half Duplex
 - 10 Mbps Full Duplex
 - 10 Mbps Half Duplex
4. Click **Save**.
5. Open the System page. In the Network Management Card panel, click **Restart network management card** to restart the PDU Network Management and Control (eNMC) module. A pop-up confirmation message displays:
 Are you sure you want to restart the Network Management Card?
 Note: This will NOT restart the PDU or change the power status of the outlets.

Configure the IPv4 Settings

1. Access the Web interface and log in.
2. Under Network, select TCP/IP. The TCP/IP page displays.
3. In the IPv4 panel, select the manner by which IPv4 settings are configured from the BootP/DHCP drop-down list:
 - **Enabled.** The IPv4 settings are configured by the DHCP server. If DHCP is enabled, go to Step 5.
 - **Disabled.** The IPv4 settings are manually configured by the user. If DHCP is disabled, perform the following:
 - Type the IPv4 address.
 - Type the IPv4 subnet mask.
 - Type the IPv4 address of the gateway (if any).
 - Type the PDU host name (used for DNS resolution).
 - Type the PDU domain name (used for DNS resolution)
4. Click **Save**.
5. Open the System page. In the Network Management Card panel, click **Restart network management card** to restart the PDU Network Management and Control (eNMC) module. A pop-up confirmation message displays:
 Are you sure you want to restart the Network Management Card?
 Note: This will NOT restart the PDU or change the power status of the outlets.

Configure the IPv6 Settings



NOTE

By default, the IPv6 interface is disabled. You can enable it from the Web interface or the Serial interface.

1. Access the Web interface and log in.
2. Under Network, select TCP/IP. The TCP/IP page displays.
3. In the IPv6 panel, enable the IPv6 interface by checking the **IPv6 Enabled** check box.

4. Select one of the following configuration methods for IPv6 settings
 - For manual configuration, uncheck the **IPv6 Address Auto Configuration Enabled** check box. Continue to Step 5.
 - For auto configuration, check the **IPv6 Address Auto Configuration Enabled** check box. Continue to Step 10.

NOTE 1 For manual configuration, provide the IPv6 global address with its prefix length and the IPv6 address of the gateway (if any).



NOTE 2 For auto-configuration, the global IPv6 addresses and prefix lengths are automatically configured by the network (an IPv6 router is required). The gateway IPv6 address is defined by the user.

NOTE 3 Regardless of the configuration you choose, the local IPv6 address is auto-generated by the eNMC module.

5. Type the local IPv6 address.
6. Type the prefix length for the global IPv6 address.
7. Type the IPv6 gateway address (if any).
8. Type the second IPv6 address and prefix.
9. Click **Save**.
10. Open the System page. In the Network Management Card panel, click **Restart network management card** to restart the eNMC module. A pop-up confirmation message displays:
Are you sure you want to restart the Network Management Card?
Note: This will NOT restart the PDU or change the power status of the outlets.

Configure the DNS

When the IPv4 address is automatically obtained by DHCP, the DNS server addresses (primary and secondary) are provided by the DHCP server.

You can define DNS IPv4/IPv6 addresses from the Web and Serial interfaces. However, this configuration is overwritten when the PDU Network Management and Control (eNMC) module restarts and the IPv4 address is obtained from a DHCP server that provides DNS addresses.

1. Access the Web interface and log in.
2. Under Network, select TCP/IP. The TCP/IP page displays.
3. In the DNS panel, type the primary DNS server's IPv4 or IPv6 address.
4. Type the secondary DNS server's IPv4 or IPv6 address (if any).
5. Click **Save**.

Configure the SMTP

1. Access the Web interface and log in.
2. Under Network, select TCP/IP. The TCP/IP page displays.
3. In the SMTP panel, type the SMTP server IPv4 / IPv6 address or host name.
4. If not already provided, type the SMTP port.

5. If your SMTP server requires authentication, perform the following:
 - Check the SMTP Server Authentication check box.
 - Type the login.
 - Type the password.
 - If not already provided, type the sender address.
6. Click **Save**.

SNMP

Enable/Disable the SNMP Agent

1. Access the Web interface and log in.
2. Under Network, select SNMP. The SNMP Settings page displays.
3. Choose one of the following SNMP versions:
 - **Disabled:** the agent is disabled; the MIB cannot be read and no traps are sent.
 - **SNMPv1:** only SNMPv1 users and SNMPv1 traps are supported.
 - **SNMPv3:** only SNMPv3 users and SNMPv3 traps are supported.
 - **SNMPv1 & v3:** both SNMPv1 and SNMPv3 users and traps are supported.
4. Type the SNMP Port number and the SNMP Trap Port number in the entry boxes.
5. Click **Save**.

Define SNMPv1 Users

1. Access the Web interface and log in.
2. Under Network, select SNMP. The SNMP Settings page displays.
3. Ensure that SNMPv1 is selected in the SNMP Version field.
4. In the SNMP V1 panel, in the Community column, select the SNMPv1 user to configure. The Community Settings dialog displays.
5. Choose one of the following access rights for the selected SNMPv1 user:
 - **No Access:** The user is not allowed to access the Web interface.
 - **Read-Only:** the SNMPv1 user can only get the MIB objects.
 - **Read-Write:** the SNMPv1 user can get and set the MIB objects.
6. Click **Save**. Otherwise, click **Cancel** to return to the SNMP Settings page.

Define SNMPv3 User-based Security Model Users

1. Access the Web interface and log in.
2. Under Network, select SNMP. The SNMP Settings page displays.
3. Ensure that SNMPv1 is selected in In the SNMP Version field.
4. In the SNMP V3 panel, in the Users column, select the SNMPv3 user to configure. The SNMP User Settings dialog displays.

5. Choose one of the following access rights for the SNMPv3 user:
 - **No Access:** the SNMPv3 user is disabled with no access to the MIB objects.
 - **Read-Only:** the SNMPv3 user can only get the MIB objects.
 - **Read-Write:** the SNMPv3 user can get and set the MIB objects.
6. Choose one of the following security levels to be applied to the SNMPv3 user:
 - **Not Set:** the SNMPv3 user is not configured and therefore disabled.
 - **Auth Priv:** an authentication password and a privacy key are required to access the MIB objects.
 - **Auth No Priv:** an authentication password but no privacy key are required to access the MIB objects.
 - **No Auth No Priv:** no authentication password or privacy key are required to access the MIB objects.
7. Type the authentication password (if required by security level), with 8 to 24 characters allowed.
8. Type the privacy key (if required by security level), with 8 to 24 characters allowed.
9. Click **Save**. Otherwise, click **Cancel** to return to the SNMP Settings page.

Access Lenovo PDU MIB Objects (Privileged Access Only)

1. Access the Web interface and log in.
2. Under Network, select SNMP. The SNMP Settings page displays.
3. Click **Link to the PDU MIB**.

Energy Wise

Enable Energy Wise

1. Access the Web interface and log in.
2. Under Network, select **Energy Wise**. The Energy Wise page displays.
3. In the Configuration panel, ensure that the **Enable** check box is checked and that the associated SDK Version number displays. (The SDK version is not editable.)
4. Type the Domain name (maximum 63 characters).
5. For Security, select **Enabled or Disabled**.
6. For Secret, type the secret key (maximum 63 characters).
7. For Threshold Level, type a threshold number (minimum value 0, maximum value 10).
8. For the Remote Port and Listen Port value, type a port number (minimum value 1, maximum value 65535).
9. Click **Save**.

Disable Energy Wise

1. Access the Web interface and log in.
2. Under Network, select **Energy Wise**. The Energy Wise page displays.
3. In the Configuration panel, ensure that the **Disabled** check box is checked. (When **Disable** is selected, all other fields in the Configuration panel are also disabled.)
4. Click **Save**.

Start/Stop Energy Wise Commands

1. Access the Web interface and log in.
2. Under Network, select **Energy Wise**. The Energy Wise page displays.
3. The current Energy Wise state value displays in the Status field. Valid states are:
 - ▮ Unknown
 - ▮ Not Initialized
 - ▮ Stopped
 - ▮ Stopping
 - ▮ Starting
 - ▮ Started
 - ▮ Down
 - ▮ Initializing
 - ▮ Up
 - ▮ Active
 - ▮ Requested Shutdown
4. For Command, select one of the following from the drop-down list:
 - ▮ Start
 - ▮ Graceful Stop
 - ▮ Off-State Cache Stop
 - ▮ Restart
5. Click **Save**.

Security

Enable/Disable SSL Encryption



CAUTION

Up to four PDUs may be daisy-chained when using the SSL with 2048 byte encryption key size.

1. Access the Web interface and log in.
2. Under Network and Security, select Global. The Security page displays.
3. In the Ports Settings panel, ensure that the **HTTP Enable** check box is checked and that the associated HTTP Port number displays.
4. Check the **Force SSL** check box to enable SSL encryption, or uncheck the box to disable it. If enabled, the HTTPS Port entry box is active. Type the port number.
5. Click **Save**.
6. Open the System submenu in the Settings menu. In the Network Management Card panel, click **Restart network management card** to restart the PDU Network Management and Control (eNMC) module.

NOTE 1 With SSL encryption, the Web interface is accessible from **https://<IPv4 address>** and the **https://[IPv6 address]**, or both, according to the IP configuration.



NOTE 2 When **Force SSL** is selected, the Web page is only available through HTTPS. If you enter the IP address through HTTP, it will be automatically redirected to HTTPS and you will receive the following message and a new URL link:
The Network Management Card is protected by SSL encryption.
Please use the following address(es) to connect to the Network Management Card. **https://166.99.224.82**

Enable/Disable the Telnet Interface

NOTE 1 Selecting a console type on the Security page makes the corresponding port entry box active.



NOTE 2 Not selecting a console type makes the corresponding port entry box inactive and grayed-out.

-
1. Access the Web interface and log in.
 2. Under Network and Security, select Global. The Security page displays.
 3. In the Ports Settings panel, select **Telnet** from the Console drop-down list to enable the Telnet interface, or select **Disabled** to disable it.
 4. If enabled, the Telnet Port entry box is active. Type the port number.
 5. Click **Save**.
 6. Open the System submenu in the Settings menu. In the Network Management Card panel, click **Restart network management card** to restart the PDU Network Management and Control (eNMC) module.

Enable/Disable the SSH Interface

1. Access the Web interface and log in.
2. Under Network and Security, select Global. The Security page displays.
3. In the Ports Settings panel, select **SSH** from the Console drop-down list to enable the SSH interface, or select **Disabled** to disable it.
4. If enabled, the SSH Port entry box is active. Type the port number.
5. Click **Save**.
6. Open the System submenu in the Settings menu. In the Network Management Card panel, click **Restart network management card** to restart the PDU Network Management and Control (eNMC) module.

Enable/Disable FTP

1. Access the Web interface and log in.
2. Under Network and Security, select **Global**. The Security page displays.
3. In the Ports Settings panel, select one of the following from the drop-down list:
 - FTP enable
 - Force FTPS ("Explicit FTPS" is used by default)
4. Check the **FTP Enable** check box to enable FTP, or uncheck the box to disable it.
5. Click **Save**.
6. Open the System submenu in the Settings menu. In the Network Management Card panel, click **Restart network management card** to restart the eNMC module.

Set Authentication Mode

1. Access the Web interface and log in.
2. Under Network and Security, select Global. The Security page displays.
3. In the Authentication Mode panel, select a value from the External Authentication drop-down list:
 - **None:** This disables external authentication. The Preference Order field is automatically checked to the **Local First, then External** value.
 - **Radius:** This enables RADIUS. If LDAP or RADIUS are enabled, you must set a preference order in the Preference Order drop-down list:
 - **External First, then Local**
 - **Local First, then External**
 - **External only**
 - **LDAP:** This enables LDAP. If enabled, you must set a preference order in the Preference Order drop-down list:
 - **External First, then Local**
 - **Local First, then External**
 - **External only**
4. Click **Save**.
5. Open the System submenu in the Settings menu. In the Network Management Card panel, click **Restart network management card** to restart the eNMC module.

Set LDAP Search Configuration

NOTE Each selection combination requires a different set of entries. Only applicable fields are active. Fields that do not apply to your selection are inactive.



- Active fields are white and the inactive fields are blue shaded.
 - When you click your cursor in inactive fields, nothing happens.
 - You can type in active fields.
-

1. Access the Web interface and log in.
2. Under Network and Security, select LDAP. The LDAP page displays.

3. Select the LDAP Server Type, User Search Bind, and Authorization Mode values from the drop-down list:
 - **LDAP Server Type:** Allows you to select a configuration.
 - **Active Directory:** Allows to configure a typical AD configuration. Some fields are read-only (User Object and User Attribute are disabled).
 - **Other:** All fields are editable.
 - **User Search Bind:** Defines if a special user for the LDAP searches must be used.
 - **Anonymous Search:** Search bind uses an anonymous way (Search User and Password are disabled)
 - **User bind Search:** Uses an LDAP user.
 - **Search User:** DN (if Bind Type = simple) or the username (if Bind Type = MD5) of the LDAP user allowed to search in the LDAP dictionary.
 - **Password:** Password of the Search User.
 - **User Base DN:** Entry of the LDAP dictionary where to start the user search.
 - **User Object:** Object class of the LDAP users.
 - **User Attribute:** Login identifier.
 - **Authorization Mode:** Choose authorization by user attribute or by group.
 - **By User attribute:** Stores the group name in the user attribute (Group Name Attribute).
 - **By Group:** Stores the group name in the group LDAP object (UPS Group Base DN).
 - **PDU Group Base DN:** LDAP dictionary entry from which the group search starts.
 - **Group Name Attribute:** LDAP attribute that stores the group name.
 - **User Name Attribute:** LDAP attribute that stores the users names linked to this group.
4. The resulting required field entries are active and highlighted. Type the associated values in the active entry boxes.
5. Click **Save**.

Authenticate LDAP Remote User

To test the login and password and authenticate an LDAP remote user:

1. Access the Web interface and log in.
2. Under Network and Security, select LDAP. The LDAP page displays.
3. In the LDAP Authentication Test panel, select the following:
 - **Login:** The login of the remote user.
 - **Password:** The password of the remote user.
4. Click **Test**. An authentication test is launched and a message displays on the LDAP Authentication Test panel to indicate if the authentication was successful or unsuccessful.

Table 9 provides authentication error messages and descriptions of possible causes.

Table 9. Authentication Error Messages and Possible Causes

Error Message	Description
User Not Found	- Bad value in the User Object field. The usual value for AD is user. - Bad value in the User Attribute field. The usual value for AD is sAMAccountName. - Although the DN set in the User Base DN field exists in the LDAP Server, the login input is not found under the LDAP tree of this object. - The login input does not exist in the LDAP Server.
Search Bind Failed	- The User Search Bind field is set to Anonymous, but this mode is not supported by the LDAP Server. - The User Search Bind field is set to User Bind Search, but the Password is empty while it is required by the LDAP server.
Search User Invalid Credential	- Bad value in the Password field of the Search User. - Bad value in the Search User field: - In SASL MD5 mode: A DN is used in the Search User field instead of a name. The DNS does not provide the reverse resolution of the LDAP server IP. - In simple mode: Usually, a DN must be used in the Search User field. - Regardless of the mode: The Search User input did not match any existing object in the LDAP database.
Root for User Base DN is incorrect	The root part of the User Base DN field is incorrect.
Relative Distinguished Name for User Base DN is incorrect	The root part of the User Base DN field is correct, but the remaining part does not exist in the LDAP server.
User Invalid Credential	The login password is incorrect.
LDAP Search Group Not Found	- No remote group has been set in the Access Accounts page. - No relationship has been found between the PDU remote groups and the LDAP groups. - Although the DN set in the PDU Group Base DN field exists in the LDAP Server, no PDU remote groups have been found under the LDAP tree of this object. - Bad value in the Group Name Attribute field (configuration Other). - Bad value in the User Name Attribute field (configuration Other).
Root for Group Base DN is incorrect	The root part of the PDU Group Base DN field is incorrect.
Relative Distinguished Name for Group Base DN is incorrect	The root part of the PDU Group Base DN field is correct, but the remaining part does not exist in the LDAP server.
LDAP Server Unavailable	- Bad LDAP server IP address. - Bad LDAP server port. - Bad LDAP server name. - In case of LDAPS/Start TLS Encryption method: The LDAP server is not configured to use SSL. The PDU Authority Certificate is required by the LDAP server but it has not been added in the certificate store of the LDAP server as Trusted Certification Authority. If the Activate AC Certificate field of the LDAP Server Global Parameters panel is checked, the LDAP Server Authority Certificate uploaded in the PDU is not the correct.

Set LDAP Server Global Parameters

1. Access the Web interface and log in.
2. Under Network and Security, select LDAP. The LDAP page displays.
3. In the LDAP Server Global Parameters panel, select the following:
 - **Encryption Method:** The Encryption method defines if an SSL connection is used between the PDU and the LDAP server when the LDAP requests are sent during the PDU user authentication process. From the drop-down list, select one of the following:
 - **None:** (No SSL connection) The data is sent without encryption. The standard port number is 389 (the port for no encryption). It can be set or modified from the LDAP Server Settings dialog.
 - **LDAPS:** (With SSL Connection) This selection uses an LDAP-over-SSL connection. The standard port number is 636. It can be set or modified from the LDAP Server Settings dialog
 - **Start TLS:** (With SSL Connection) Use the "start TLS" extension (RFC 2830). The standard port number is 389 (the same port that for no encryption). It can be set or modify from the LDAP Server Settings dialog.
 - **Bind Type:** The bind operation uses the LDAP user credentials to identify the LDAP authentication connection between the PDU and the LDAP server. From the drop-down list, select one of the following:
 - **Simple:** The user credentials are sent without encryption. However, if an SSL connection is used, the credentials are encapsulated in an SSL-encrypted connection.
 - **SASL Digest MD5:** Using MD5, a hash algorithm is used to encrypt the user credentials.
4. To upload your AC Certificate, select **Browse**. Highlight the selected file and click **Open**.



IMPORTANT

The AC Certificate is the AC Certificate of the LDAP server, not the AC Certificate of the PDU. The certificate format is a Base64 encoded DER certificate, enclosed between the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" tag. In order to configure your LDAP server for SSL, you need the AC certificate of the PDU certificate.



NOTE

When uploading a file, you cannot write the file path in the text field. You must select the file from the file explorer window that displays when you click **Browse**.

5. Click **Upload**.
6. Click **Save**.

Modify LDAP Server Settings

1. Access the Web interface and log in.
2. Under Network and Security, select LDAP. The LDAP page displays.
3. In the LDAP Server panel, click a linked host name. The LDAP Server Settings dialog displays.
4. In the Enable Server drop-down list, select **Enable** or **Disable** to enable or disable the selected LDAP server or servers.
5. If enabled, you can choose to change the server name, the port number, and the number of seconds to time out in the Server, Port, and Time Out (sec) entry boxes.
6. Click **Save**. Otherwise, click **Cancel** to return to the LDAP page.

Add RADIUS Server

Authorization configuration must be done in the radius server to add the PDU remote group defined in the Remote Group Access PDU setting.

The authorization is based on the information sent by the server through the following RADIUS attribute:

- Vendor Specific ID: 534
- Vendor Specific Attribute ID: 29, format string

The authorization strings sent by the server from the vendor-specific attributes (VSA) are compared with the remote groups configured in the PDU. If a remote group is found, the profile user linked to the remote group is set to the remote user (in case of authentication success). If no group is found, the access is rejected by the PDU.

This attribute must be added in the RADIUS server configuration and must be sent for each remote user allowed to access to the PDU.

To add a RADIUS server:

1. Access the Web interface and log in.
2. Under Network and Security, select RADIUS. The RADIUS page displays.
3. In the RADIUS Server panel, select the following:
 - **Authentication Protocol:** Select an authentication method from the drop down list, either Password Authentication Protocol (PAP) or Challenge-Handshake Authentication Protocol (CHAP).
4. Check the **Add** check box.
5. In the RADIUS Settings panel, select the following:
 - **Primary or Secondary Server:** Identify the server by selecting Primary Server or Secondary Server.
 - **Enable Server:** From the drop-down list, select **Enable** to enable the server or **Disable** to disable the server.
 - **RADIUS Server:** Enter the IPv4 address, IPv6 address, or the host name of the RADIUS server.
 - **Secret:** Shared secret (case sensitive).
 - **NAS IP Address:** The NAS field allows you to select an IP address from the IP addresses of the card.
 - **UDP Port:** The User Datagram Port (UDP) number (standard: 1812).
 - **Time Out (sec):** Type the number of seconds to wait for a response from the authentication server before trying to reconnect.
 - **Retry Number:** Type the number of times to try to reconnect to the authentication server before reporting that the connection failed for one authentication attempt.
6. When you finish selecting parameters for the RADIUS server, click **Save** or **Cancel**.

Edit Parameters for a RADIUS Server

1. Access the Web interface and log in.
2. Under Network and Security, select RADIUS. The Security - RADIUS page displays.
3. In the RADIUS Server panel Name column, click the name of the RADIUS server you want to edit.
4. The RADIUS Settings dialog displays. Change the parameters as needed.
5. When you finish modifying parameters for the RADIUS server, click **Save** or **Cancel**.

Chapter 9 Maintenance and Alarms

This section explains maintenance functions for the Lenovo Power Distribution Unit (PDU), including:

- Preventive maintenance
- Equipment disposal
- Updating Firmware
- Alarms

Preventive Maintenance

For the best preventive maintenance, keep the area around the PDU clean and dust-free. If the atmosphere is very dusty, clean the outside of the system with a vacuum cleaner. Do not to exceed 60°C (140°F) for best performance.

Equipment Disposal

Contact your local recycling or hazardous waste center for information on proper disposal of the used PDU.



CAUTION

Do not discard waste electrical or electronic equipment (WEEE) in the trash. For proper disposal, contact your local recycling/reuse or hazardous waste center.

Firmware Upgrade

The firmware upgrade process allows you to maintain the most current firmware by updating the PDU Network Management and Control (eNMC) module with new or enhanced features and applying periodic bug fixes.

The upgrade file is named **Image<xxx>.bin**. (The <xxx> values will vary for each upgrade.) During the upgrade, the firmware and the Web page are both upgraded to avoid incompatibility between the firmware version and the Web site. Additional validation checks are performed as well.

The new firmware files can be uploaded using either Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), or USB. With all methods, the basic steps are the same:

1. **Upload the Binary File.** This file will be stored in a temporary location in the communications module.
2. **Implement the Firmware.** After the file is loaded, the bootloader will implement the firmware in the eNMC module to upgrade the firmware and refresh the Web pages.



NOTE

Groups of Lenovo PDU models can be configured or updated with new firmware at the same time using UPS Power Manager (UPM). The UPM software is available separately at no cost for up to 10 devices. Refer to the *Eaton Intelligent Power Manager (IPM) User's Guide* for more information.



IMPORTANT

We strongly recommend that you leave only one UPM activated when mass upgrade or mass configuration operations are performed to upgrade eNMC from UPM. You should shut off all paralleled UPM (up to 9) during these operations.

Upgrading Firmware with Hypertext Transfer Protocol

The HTTP upgrade using the Web occurs in two stages:

- ▮ Upload the binary file
- ▮ Implement the firmware

Uploading the Binary File

To access the Web interface:

1. Ensure that an Ethernet cable is correctly connected between a Windows PC and the Ethernet port on the PDU. Verify communication.
2. Start up the PDU and note the IP address displayed on the LCD.
3. Open the Web browser and type the IP address you obtained from the PDU.
4. When the connection is made, the Authentication dialog displays.
5. Enter a valid user name and password in the authentication dialog box (see Figure 78). Click **Login** to continue or **Cancel** to exit.

**NOTE**

The default user name is "USERID" and the default password is "passw0rd."

The image shows a web-based authentication dialog box. It has a light blue background and a title bar that says 'Authentication'. Inside the dialog, there are two text input fields. The first is labeled 'Login:' and the second is labeled 'Password:'. Below these fields are two buttons: 'Login' and 'Cancel'.

Figure 78. Login Authentication

6. The PDU Overview page displays.
7. From the menu bar, click Settings and then System. The System Settings page displays in the Main Application window (see Figure 79).
8. In the Network Management Card panel, check **Firmware upgrade enabled** and click **Browse** to find the upgrade file.

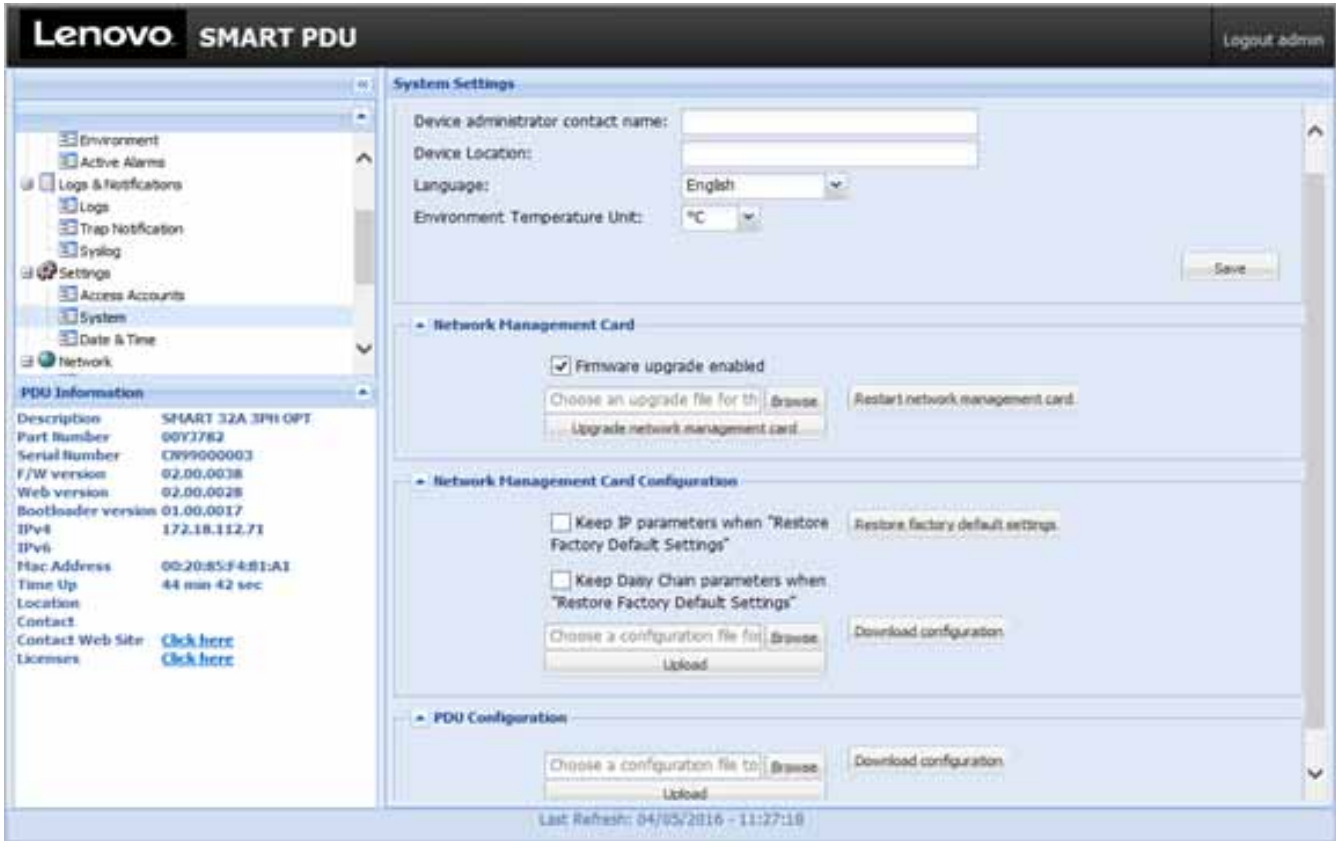


Figure 79. System Settings Page

- 9. From the Open window, select the **Image<xxx>.bin** file, and click **Open**.
- 10. In the Network Management Card panel, click **Upgrade Network Management Card** to launch the upload. A progress bar shows the progress of the update.

 CAUTION

Do not disturb the upgrade until the progress bar shows complete.

- 11. When finished, a message displays and the communications module restarts automatically. The upgrade takes four to five minutes. When the upgrade completes, refresh the Web pages.

Upgrade the Firmware and Refresh Web Pages

After the binary file is uploaded to the communications module, the final step is an automatic process that upgrades the firmware and refreshes the Web pages.

The communications module reboots and, in Bootloader mode, detects a new available image, checks validity of this image, and launches the upgrade of the firmware and refresh the Web pages. As the upgrade processes, a message box displays with percent completed.

When completed, an upgrade message displays **F/W: 100%**, and the communications module reboots with the new firmware and refreshed Web pages.

Upgrading the Firmware with FTP Protocol



NOTE

By default, FTPS protocol is set. Use a dedicated software to upgrade the firmware via FTPS. Select FTP protocol via Web pages and use the FTP command via an MS-DOS console to upgrade the firmware.

The FTP upgrade occurs in two stages:

- Upload the binary file
- Implement the firmware



NOTE

The FTP server must be enabled for this procedure. This is an option on the Global Security page of the Web interface.

Uploading the Binary File

To access the Web interface:

1. Ensure that an Ethernet cable is correctly connected between a Windows PC and the Ethernet port on the PDU. Verify communication.
2. Start up the PDU and note the IP address displayed on the LCD.
3. Open an MS-DOS command line window and connect to the communications module in FTP mode (see Figure 80):
 - Type **FTP @IP**, where @IP is the previous IP address.
 - Type the user name and password of the SuperUser.
 - Type the **hash** command. This allows you to follow the upload as it progresses.
4. At the **ftp>** command line, use the **put** command with the **Image<xxx>.bin** file to launch the upgrade (see Figure 80).

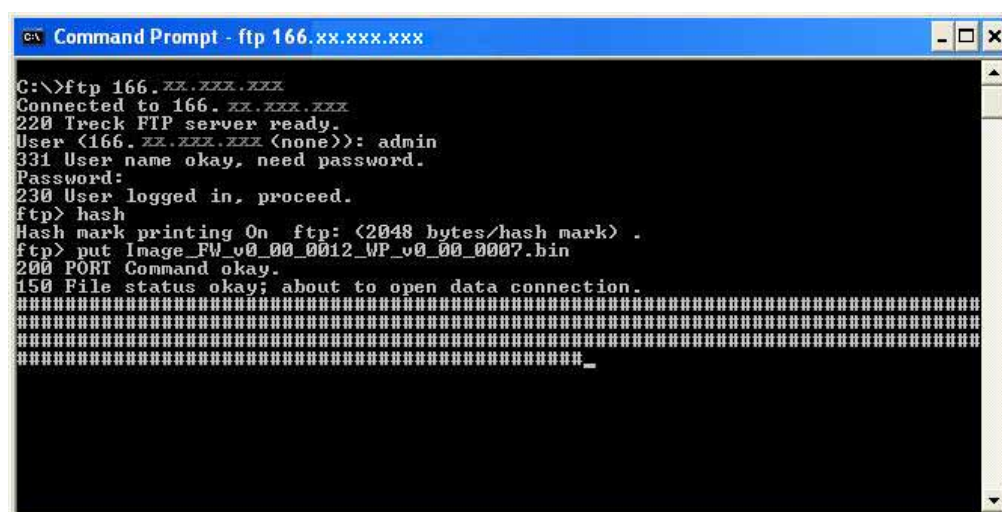


Figure 80. Launching the Upgrade

- When the upgrade finishes, the closing message displays (see Figure 81).

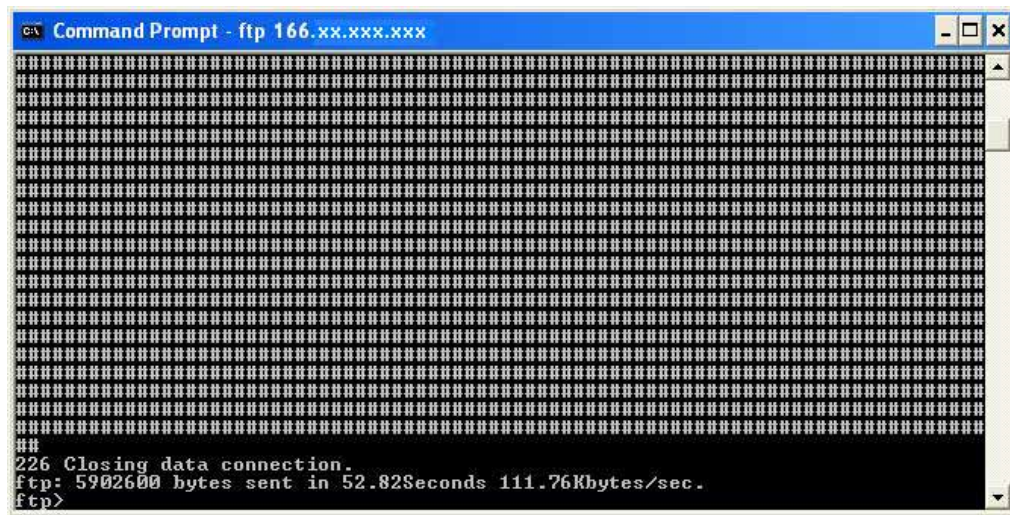


Figure 81. Closing Message

Upgrade the Firmware and Refresh Web Pages

After the binary file is uploaded to the communications module, the final step is an automatic process that upgrades the firmware and refreshes Web pages.

The communications module reboots and, in Bootloader mode, detects a new available image, checks validity of this image, and launches the upgrade of the firmware and refresh the Web pages. As the upgrade processes, the LCD display shows the completion status.

When completed, an upgrade message on the LCD displays **F/W: 100%**, and the communications module reboots with the new firmware and refreshed Web pages.

Upgrading the Firmware with the USB Port

See “Settings Menu” and “USB Flash Mode Submenu” on page 63 for more information of upgrading with the USB.

Active Alarms

The Lenovo PDUs have a rich set of alarms and events to notify you of up-to-date activity and operation status. Both the local PDU LCD interface and the remote Web interface provide active alarm notifications when alarms become active.

- On the LCD interface, the existing LCD display is replaced by the Active Alarms screen and the backlight is blinking red when an alarm is generated.
- On the Web interface, two active alarm notifications are provided:
 - In the menu hierarchy, the text for Active Alarms is red when alarms are active.
 - In the bottom of the window (the refresh bar), a message displays, “Warning, some alarms fired, please refer to the Active Alarms | Last Refresh: dd/mm/yyyy - hh:hh:ss.” The words “Active Alarms” in the message are a link to the Active Alarms page.



NOTE

The alarm and event list is subject to change.

**NOTE**

For LCD interface information, see “Active Alarms Menu” on page 57. For Web interface information, see “Active Alarms” on page 105.

- To clear flashing LCDs and the LED:
 - Press any button on the PDU or clear the alarm using the Web interface.
- To correct a condition:
 - Define the alarm condition and resolve the condition.
- Self-correcting conditions:
 - Sometimes, the alarm automatically clears when the condition resolves. For example, if a load over current alarm is generated, the alarm is cleared when the current drops 0.1A below the level (alarm hysteresis).

Defining the Alarm or Event Condition

You can derive defining information about the alarm or event from the associated number code. Figure 82 shows the location of the associated number code in the Code column on the Logs page of the Web interface.

Date and Time	Description	Type	Code
14/05/2016-07:58:35	Environment temperature normal	PDU [0]	207000
14/05/2016-07:54:26	User logged in HTTP (USERID)	User	301600
14/05/2016-05:42:40	User logged in HTTP (USERID)	User	301600
14/05/2016-05:41:45	Environment temperature high critical [26.0]	PDU [0]	207400
14/05/2016-05:41:44	Environment probe connected	PDU [0]	208100
14/05/2016-05:41:34	Daisy Chain Connected	PDU [0]	251001
14/05/2016-05:41:32	Network cable connected	User	300200
14/05/2016-05:41:31	Network Management Card restarted	User	300105
14/05/2016-05:41:23	Network cable connected	User	300200
14/05/2016-05:41:18	Network cable not connected	User	300300
14/05/2016-05:39:00	Environment probe connected	PDU [0]	208100
14/05/2016-05:39:00	Environment temperature high critical [26.0]	PDU [0]	207400
14/05/2016-05:38:48	Network cable connected	User	300200
14/05/2016-05:38:47	Network Management Card restarted	User	300103
14/05/2016-05:38:28	Network cable connected	User	300200
14/05/2016-05:38:18	Network cable not connected	User	300300
14/05/2016-05:36:20	Environment temperature high critical [26.0]	PDU [0]	207400
14/05/2016-05:35:59	User logged in HTTP (USERID)	User	301600
14/05/2016-05:34:45	Environment probe connected	PDU [0]	208100
14/05/2016-05:34:33	Network cable connected	User	300200
14/05/2016-05:34:32	Network Management Card restarted	User	300103
14/05/2016-05:34:02	Environment temperature normal	PDU [0]	207000

Figure 82. Location of Alarm Code on Web Interface

This number code is a six-digit number. The first digit in the number conveys the source of the alarm or event. The remaining five digits in the number code further identify and define the type of alarm (see Figure 83).

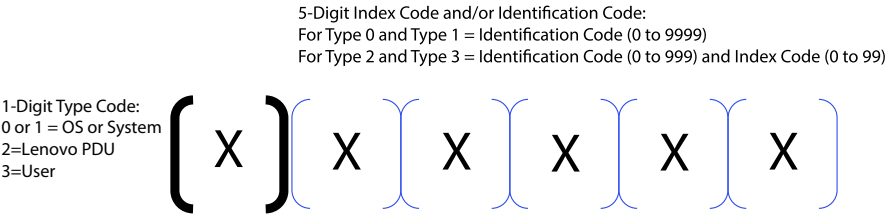


Figure 83. Alarm Code Format

Type Code 0 or 1 (OS or System)

IMPORTANT

For Type Code 0 and Type Code 1, always contact customer support for assistance. These errors are not user-correctable.

The Type Code 0 and Type Code 1 alarms and events are triggered from the OS or the system. Figure 84 provides an example of a Type Code 1 system alarm number code. It only contains an 5-digit identification code (no index code).

Alarm number code 102820: No answer from a CAN device

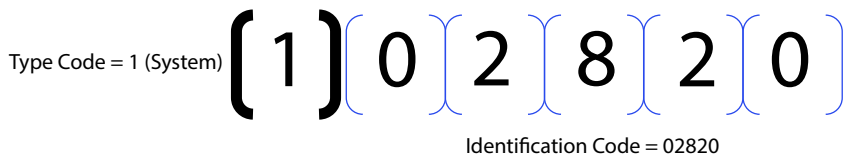


Figure 84. Example Type 1 Code

Table 10 lists OS or System alarms and events.

Table 10. OS or System Alarms and Events

Type Code	Identification Code	Alarm or Event
1	03073	Code unreachable
1	03074	Heap overflow
1	03075	Not enough memory in Heap
1	02817	A command is sent to an unavailable device CAN
1	02818	*Not used
1	02819	Impossible to open a session with a CAN device
1	02820	No answer from a CAN device
1	02821	*Not used
1	02822	The number of CAN devices discovered on CAN bus is too great
1	02823	Command unknown
1	02824	Device CAN Id out of range
1	02825	Time duration of a command is too long
1	02826	Report acquired from CAN device is wrong
1	02827	Report descriptor acquired from CAN device is wrong
1	01281	Mutex not available

Table 10. OS or System Alarms and Events (Continued)

Type Code	Identification Code	Alarm or Event
1	01282	HID object Id out of range
1	01283	Report empty or not valid
1	01284	Report Id out of range
1	01285	Not enough memory in HEAP
1	01286	Duration of the acquisition of Teridian is too long
1	01282	HID object Id not in list of data saved in EEPROM
1	02561	*Not used
1	02562	*Not used
1	02563	*Not used
1	02564	Wrong data type
1	02565	String too long
1	02566	*Not used
1	02567	*Not used
1	01025	*Not used
1	01026	Semantic error
1	01027	Impossible to open log file
1	01028	Impossible to write data in log file
1	01029	Impossible to seek data in log file
1	01030	Impossible to read data in log file
1	01031	Mutex not available
1	01032	*Not used
1	01033	Impossible to clear LOG file
1	03585	Initialization of SSH task failed
1	03076	Error writing in flash memory during an upload
1	03077	End signature of the uploaded file does not match
1	03078	Checksum of the uploaded file does not match
1	03586	Reading of the host key file (or table) failed
1	03587	Listening of SSH socket failed
1	03588	Acceptance of SSH socket failed
1	03589	Break received
1	03590	Max number of SSH connection reached
1	03591	Certificate error
1	03592	*Not used
1	04865	Error reading from the 12C Eeprom
1	04866	Error writing to the 12C Eeprom
1	03841	SNMP bad trap number

Type Code 2 or 3 (PDU or User)

Type 2 alarms and events are triggered from the PDU. These alarms and events are primarily threshold crossings when the operation measurement is beyond the threshold value range setting. Type 2 alarms and events also provide the state of optional connected equipment.

Type 3 alarms and events are triggered from user actions.

Figure 85 provides an example of a Type Code 2 PDU alarm number code.

Number code 211402: Lenovo PDU Critical Overcurrent L2 Phase

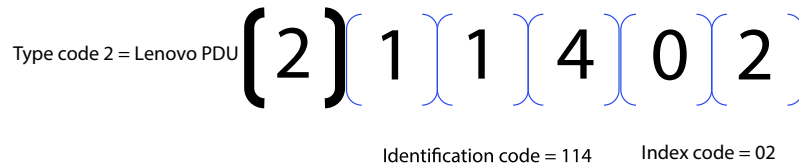


Figure 85. Example Type 2 Code

Table 11 lists PDU and User alarms and events.

Table 11. PDU and User Alarms and Events

Type Code	Identification and Index Code	Alarm or Event	Description
2	201000	Dry Contact 1 Not Active	The signal for Dry Contact 1 is active.
2	201100	Dry Contact 1 Active	The signal for Dry Contact 1 is not active.
2	202000	Dry Contact 1 Open	Dry Contact 1 is open.
2	202100	Dry Contact 1 Closed	Dry Contact 1 is closed.
2	203000	Dry Contact 2 Not Active	The signal for Dry Contact 2 is active.
2	203100	Dry Contact 2 Active	The signal for Dry Contact 2 is not active.
2	204000	Dry Contact 2 Open	Dry Contact 2 is open.
2	204100	Dry Contact 2 Closed	Dry Contact 2 is closed.
2	205000	Sensor Probe Communication Failure Cleared	Sensor Probe communication failure is cleared
2	205100	Sensor Probe Communication Failure	Sensor probe communication failure detected
2	208000	Sensor Probe Not Connected	Sensor probe not connected since firmware startup
2	208100	Sensor Probe Connected	Sensor probe connected at least once since firmware startup
2	206000	Humidity No Threshold	No humidity threshold has been triggered.
2	206100	Humidity Warning Low Threshold	The humidity level reading is less than the value configured as the low humidity warning threshold.
2	206200	Humidity Critical Low Threshold	The humidity level reading is less than the value configured as the low humidity critical threshold.
2	206300	Humidity Warning High Threshold	The humidity level reading is greater than the value configured as the high humidity warning threshold.
2	206400	Humidity Critical High Threshold	The humidity level reading is greater than the value configured as the high humidity critical threshold.
2	207000	Temperature No Threshold	No temperature threshold has been triggered.
2	207100	Temperature Warning Low Threshold	The temperature level reading is less than the value configured as the low temperature warning threshold.
2	207200	Temperature Critical Low Threshold	The temperature level reading is less than the value configured as the low temperature critical threshold.
2	207300	Temperature Warning High Threshold	The temperature level reading is greater than the value configured as the high temperature warning threshold.

Table 11. PDU and User Alarms and Events (Continued)

Type Code	Identification and Index Code	Alarm or Event	Description
2	207400	PDU Temperature Critical High Threshold	The temperature level reading is greater than the value configured as the high temperature critical threshold.
2	211000	PDU Input 1 Current No Threshold	No section current threshold has been triggered.
2	211100	PDU Input 1 Low Current Warning	The current amperage (A) reading for the specified section is less than the value configured as the low current warning alarm threshold.
2	211200	PDU Input 1 Low Current Critical	The current amperage (A) reading for the specified section is less than the value configured as the low current critical alarm threshold.
2	211300	PDU Input 1 Over Current Warning	The specified section current amperage (A) reading is greater than the value configured as the over current warning threshold.
2	211400	PDU Input 1 Over Current Critical	The specified section current amperage (A) reading is greater than the value configured as the over current critical alarm threshold.
2	212000	PDU Input 1 Voltage No Threshold	No section voltage threshold has been triggered.
2	212100	PDU Input 1 Low Voltage Warning	The specified section voltage reading is less than the value configured as the low voltage warning threshold.
2	212200	PDU Input 1 Low Voltage Critical	The specified section voltage reading is less than the value configured as the low voltage critical threshold.
2	212300	PDU Input 1 Over Voltage Warning	The specified section voltage reading is greater than the value configured as the over voltage warning threshold.
2	212400	PDU Input 1 Over Voltage Critical	The specified section voltage reading is greater than the value configured as the over voltage critical threshold.
2	213000	PDU Input 1 Frequency OK	Utility frequency is within the +/- 3 Hz of Nominal frequency.
2	213100	PDU Input 1 Frequency Out of Range	Utility frequency greater or less than +/- 3 Hz of Nominal frequency.
2	214000	PDU Input 2 Current No Threshold	No section current threshold has been triggered.
2	214100	PDU Input 2 Low Current Warning	The current amperage (A) reading for the specified section is less than the value configured as the low current warning alarm threshold.
2	214200	PDU Input 2 Low Current Critical	The current amperage (A) reading for the specified section is less than the value configured as the low current critical alarm threshold.
2	214300	PDU Input 2 High Current Warning	The specified section current amperage (A) reading is greater than the value configured as the over current warning threshold.
2	214400	PDU Input 2 High Current Critical	The specified section current amperage (A) reading is greater than the value configured as the over current critical alarm threshold.
2	215000	PDU Input 2 Voltage No Threshold	No section voltage threshold has been triggered.
2	215100	PDU Input 2 Low Voltage Warning	The specified section voltage reading is less than the value configured as the low voltage warning threshold.

Table 11. PDU and User Alarms and Events (Continued)

Type Code	Identification and Index Code	Alarm or Event	Description
2	215200	PDU Input 2 Low Voltage Critical	The specified section voltage reading is less than the value configured as the low voltage critical threshold.
2	215300	PDU Input 2 High Voltage Warning	The specified section voltage reading is greater than the value configured as the over voltage warning threshold.
2	215400	PDU Input 2 High Voltage Critical	The specified section voltage reading is greater than the value configured as the over voltage critical threshold.
2	216000	PDU Input 2 Frequency OK	The frequency is not out of range.
2	216100	PDU Input 2 Frequency out of +/- 3 Hz tolerance	The frequency is out of range.
2	221000	PDU Gang Phase Input Current No Threshold	No section current threshold has been triggered.
2	221100	PDU Gang Phase Low Current Warning	The current amperage (A) reading for the specified section is less than the value configured as the low current warning alarm threshold.
2	221200	PDU Gang Phase Low Current Critical	The current amperage (A) reading for the specified section is less than the value configured as the low current critical alarm threshold.
2	221300	PDU Gang Phase Over Current Warning	The specified section current amperage (A) reading is greater than the value configured as the over current warning threshold.
2	221400	PDU Gang Phase Over Current Critical	The specified section input current amperage (A) reading is greater than the value configured as the over current critical alarm threshold.
2	222000	PDU Gang Phase Voltage No Threshold	No section voltage threshold has been triggered.
2	222100	PDU Gang Phase Low Voltage Warning	The specified section voltage reading is less than the value configured as the low voltage warning threshold.
2	222200	PDU Gang Phase Low Voltage Critical	The specified section voltage reading is less than the value configured as the low voltage critical threshold.
2	222300	PDU Gang Phase Over Voltage Warning	The specified section voltage reading is less than the value configured as the over voltage warning threshold.
2	222400	PDU Gang Phase Over Voltage Critical	The specified section voltage reading is less than the value configured as the over voltage critical threshold.
2	223000	PDU Gang Not Alarmed	No alarm has been triggered.
2	223100	PDU Gang Alarmed	An alarm has been triggered.
2	241000	Communication OK	No communication failure detected on Teridian RS-485 bus
2	241100	Communication Lost	Communication failure detected on Teridian RS-485 bus
2	251000	Daisy Chain Communication OK	No communication failure detected on Daisy Chain
2	251100	Daisy Chain Communication Alarmed	Communication failure detected on Daisy Chain
2	231000	PDU Outlet Current No Threshold	No outlet current threshold has been triggered.
2	231100	PDU Outlet Low Over Current Warning	The current amperage (A) reading for the specified outlet is less than the value configured as the low current warning alarm threshold.

Table 11. PDU and User Alarms and Events (Continued)

Type Code	Identification and Index Code	Alarm or Event	Description
2	231200	PDU Outlet Low Over Current Critical	The current amperage (A) reading for the specified outlet is less than the value configured as the low current critical alarm threshold.
2	231300	PDU Outlet High Over Current Warning	The specified outlet current amperage (A) reading is greater than the value configured as the over current warning threshold.
2	231400	PDU Outlet High Over Current Critical	The specified outlet input current amperage (A) reading is greater than the value configured as the over current critical alarm threshold.
2	232000	PDU Outlet switch off	The specified outlet is Off.
2	232100	PDU Outlet switch on	The specified outlet is On.
3	300100	Communication module restarted	The communication module has been restarted by the user.
3	300200	Ethernet cable connected	The Ethernet cable is connected.
3	300300	Ethernet cable not connected	The Ethernet cable is not connected.
3	300400	Factory reset requested by <interface>	A factory reset has been requested through the specified user interface.
3	300500	Ethernet card restart requested by <interface>	An Ethernet card restart has been requested through the specified user interface.
3	300600	Switch to bootloader mode for upgrade by <interface>	A Switch to bootloader mode for upgrade has been requested through the specified user interface.
3	300700	PDU & System Log cleared	The PDU & System Log have been cleared.
3	300800	Daisy Chain device does not answer	The Daisy Chain device does not answer.
3	300900	Time changed	The time was changed by the user.
3	301000	Daisy chain device connected	The daisy chain device is connected.
3	301100	Daisy chain device disconnected	The daisy chain device is disconnected.
3	301200	Upgrade request by user	An upgrade was requested by the user.
3	301300	Sensor connected	The sensor was connected.
3	301400	Sensor disconnected	The sensor was disconnected.
3	301500	Send mail test by user	The user sent a mail test.
3	301600	User logged in	The specified user logged in by the specified protocol.
3	301700	User logged out	The specified user logged out by the specified protocol.
3	301800	User logged in FTP	The specified user logged in by FTP.
3	301900	User logged out FTP	The specified user logged out by FTP.
3	302000	User failed to log FTP	The specified user failed to log by FTP.
3	302100	Ethernet card restart in USB mode	The Ethernet card has been restarted in USB mode.
3	302200	Network settings file uploaded from USB	The network settings file has been uploaded from the USB.
3	302300	eNMC module settings file uploaded from USB	The eNMC module settings file has been uploaded from the USB.
3	302400	PDU settings file uploaded from USB	The PDU settings file has been uploaded from the USB.

Chapter 10 Service and Support

For Lenovo in Canada or the United States, call 1-800-426-7378. For Lenovo in the European Union (EU), Asia Pacific, and Latin America countries, contact Lenovo in that country or visit the Lenovo Internet website:

- <http://support.lenovo.com/>