HP Managed Power Distribution Unit User's Guide

Abstract

This document is for the person who installs and maintains HP PDU products. HP assumes you are qualified in the installation of electrical equipment and trained in recognizing hazards in products with hazardous energy levels.

Part Number: 793528-001 EN
September 12, 2014
Edition: 1

Special Symbols

The following are examples of symbols used on equipment 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

Chapter 1 Introduction

Description

The HP MA (Managed) PDU (Power Distribution Unit) is an intelligent MA PDU that is designed to distribute power to multiple loads for data center equipment installed in a rack. The HP MA PDUs are 1Ph (single-phase) and 3Ph (three-phase) MA PDUs with monitoring at the input, branch, and individual outlet control and monitoring.

Each MA PDU provides power distribution to IT loads through multiple C19, C13, and NEMA 5-20R outlet types on 1PH and 3PH models. The number and location of outlets vary by model. The MA PDUs allow you to connect and manage these outlets from a single power connection. The MA PDUs can be managed from a local interface, a CLI (Command Line Interface) interface, or a Web interface.

HP MA PDUs are designed to be installed in HP 10000 series racks or Intelligent series racks, but can be used in other standard data center racks. The MA PDUs vary in form factor height and several mounting configurations are available, depending on the model.

Figure 1 shows an example of a MA PDU installed in a rack.

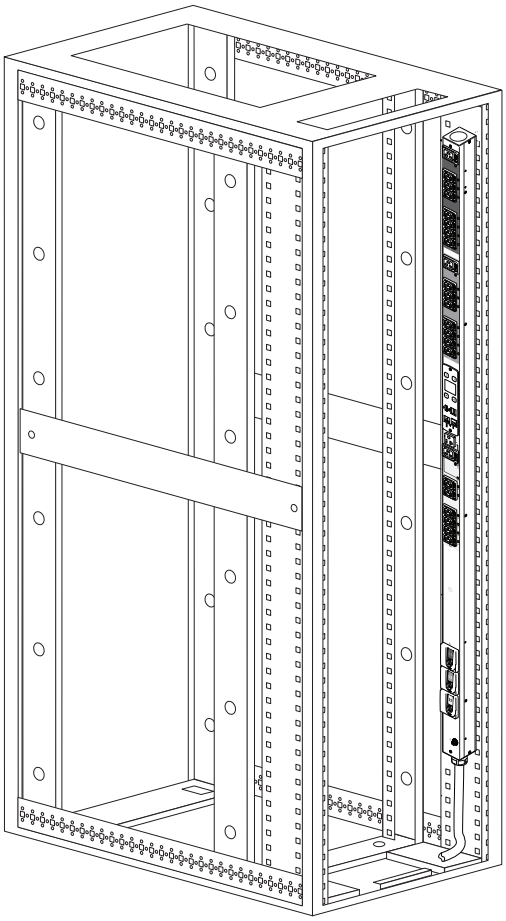


Figure 1. Example HP MA PDU Installed (Bottom Entry Method)

HP MA PDU Models

The MA PDUs are available in 22U and 42U form factor heights for standard racks. These models are designed for NA (North American), NA/JP (North American/Japanese), INTL (International), and WW (WorldWide) markets.

NOTE The WW market includes both INTL and NA models.

The PDU models support 1Ph or 3Ph applications and provide between 8 and 24 outlets. All models feature an LCD window, a set of communication port connectors, a reset button, and operation buttons. The MA PDUs have either attached or detachable input power cords. Circuit breakers are provided on most models.

NOTE For details about individual model configurations, see "Specifications" on page 137.

MA PDU Models

Available models include:

- H8B48A: HP 2.8kVA 120V 30A NA/JP maPDU
- H8B49A: HP 3.6kVA 200-240V 16A WW maPDU
- H8B50A: HP 4.9kVA 208V 30A NA/JP maPDU
- H8B51A: HP 7.3kVA 200-240V 32A INTL maPDU
- H8B52A: HP 8.6kVA 208V 30A 3Ph NA/JP maPDU
- H8B53A: HP 8.6kVA 208V 30A 3Ph DV NA/JP maPDU
- H8B54A: HP 11kVA 400V 16A 3Ph INTL maPDU
- H8B55A: HP 14.4kVA 208V 50A 3Ph NA/JP maPDU
- H8B56A: HP 17.3kVA 208V 60A 3Ph NA/JP maPDU

Figure 2 illustrates the 1Ph H8B48A MA PDU model.

Figure 2. 1Ph H8B48A Model

Figure 3 illustrates the 1Ph H8B49A MA PDU model.

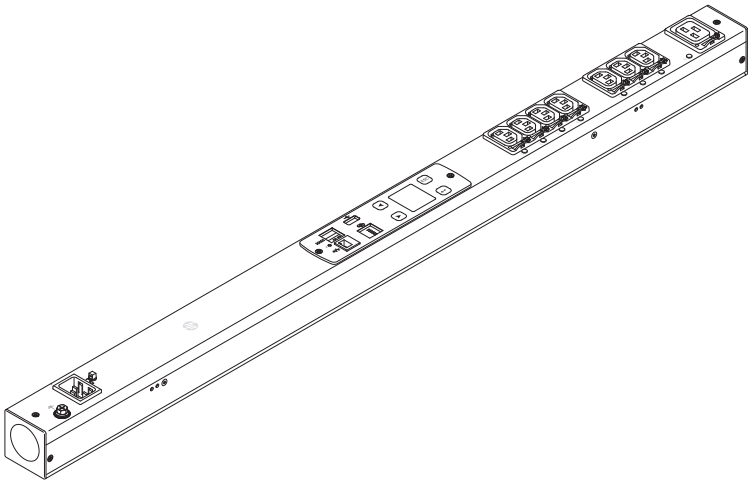


Figure 3. 1Ph H8B49A Model

Figure 4 illustrates the 1Ph H8B50A MA PDU model.

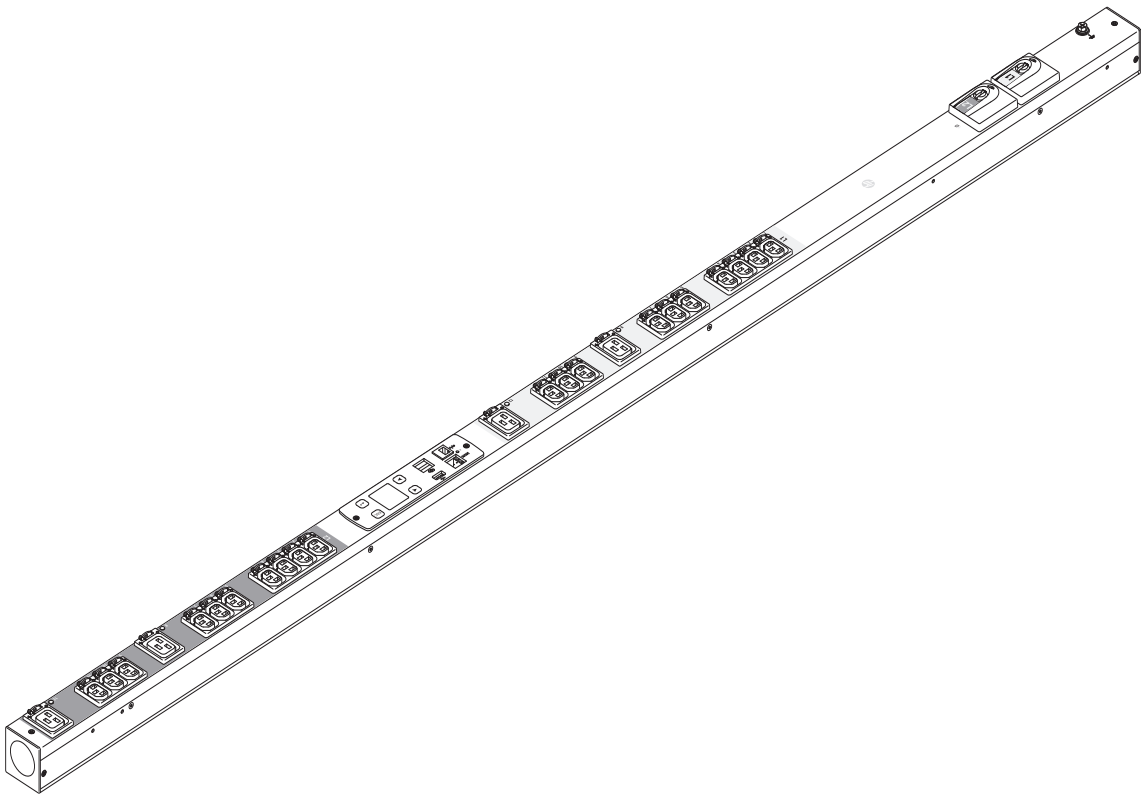


Figure 4. 1Ph H8B50A Model

Figure 5 illustrates the 1Ph H8B51A MA PDU model.

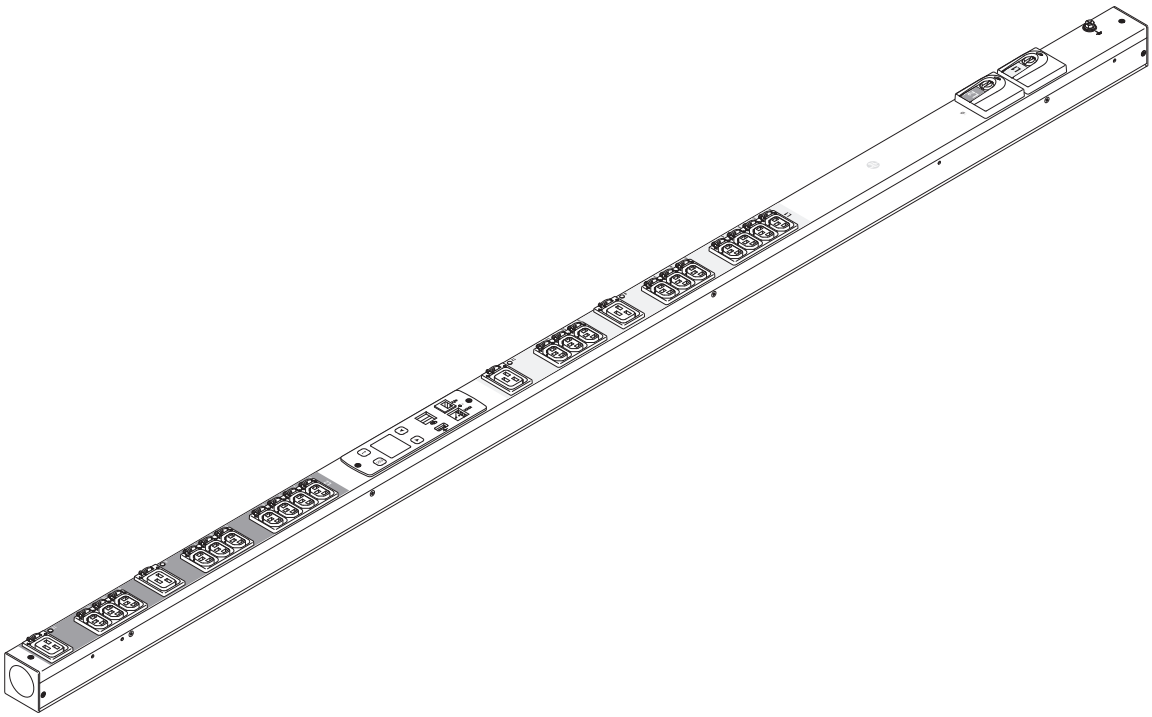


Figure 5. 1Ph H8B51A Model

Figure 6 illustrates the 3Ph H8B52A MA PDU model.

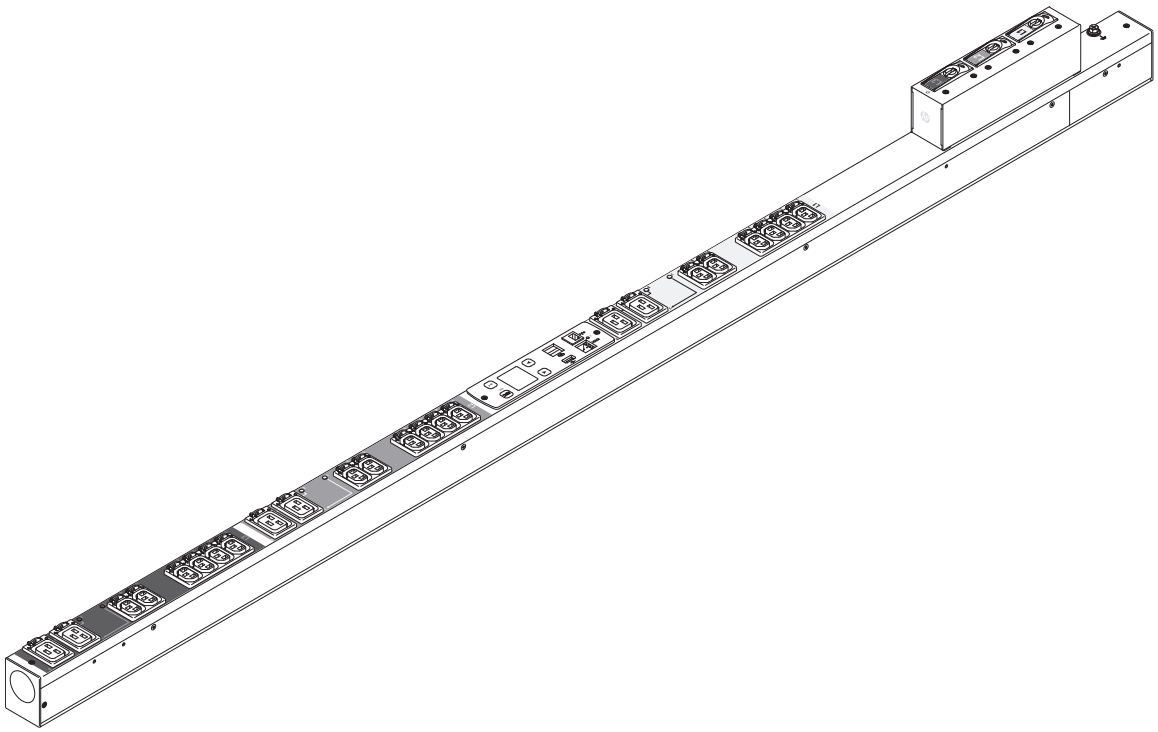


Figure 6. 3Ph H8B52A Model

Figure 7 illustrates the 3Ph H8B53A MA PDU model.

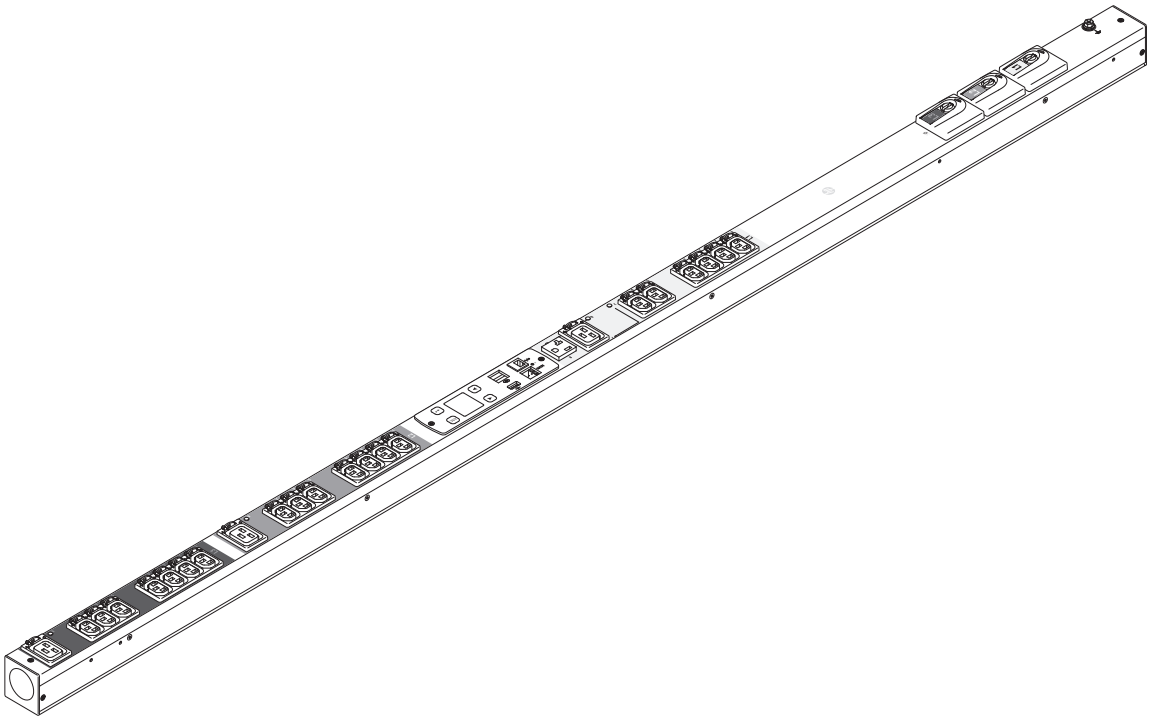


Figure 7. 3Ph H8B53A Model

Figure 8 illustrates the 3Ph H8B54A MA PDU model.

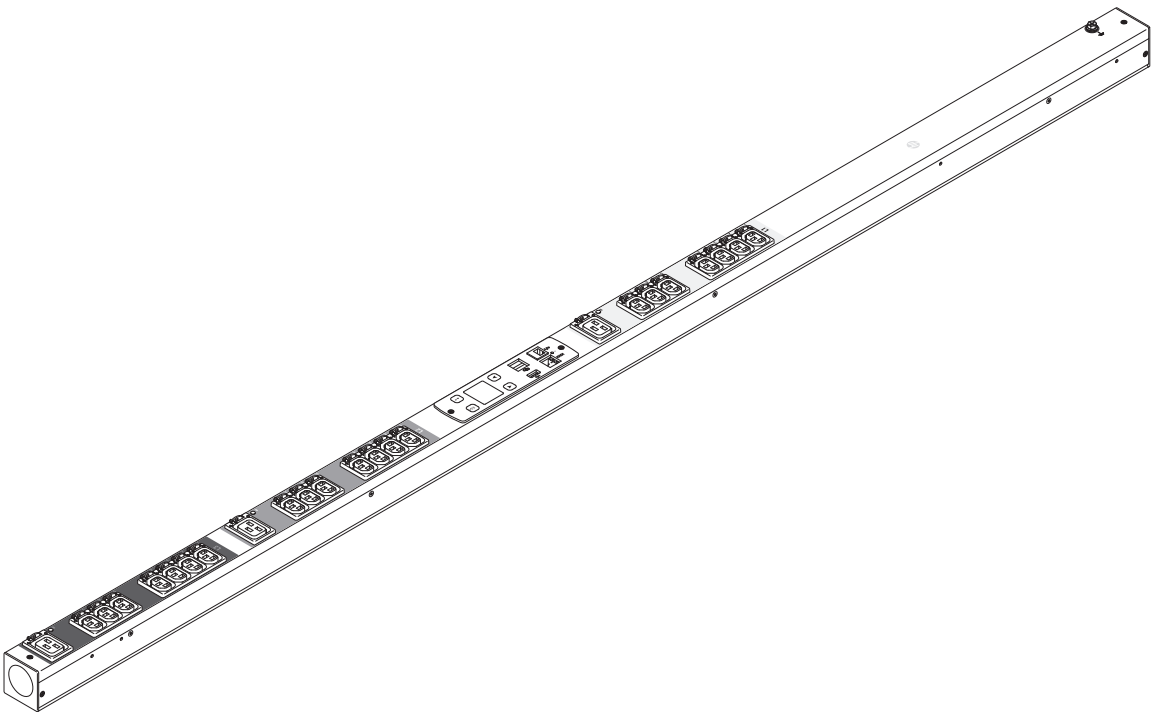


Figure 8. 3Ph H8B54A Model

Figure 9 illustrates the 3Ph H8B55A MA PDU model.

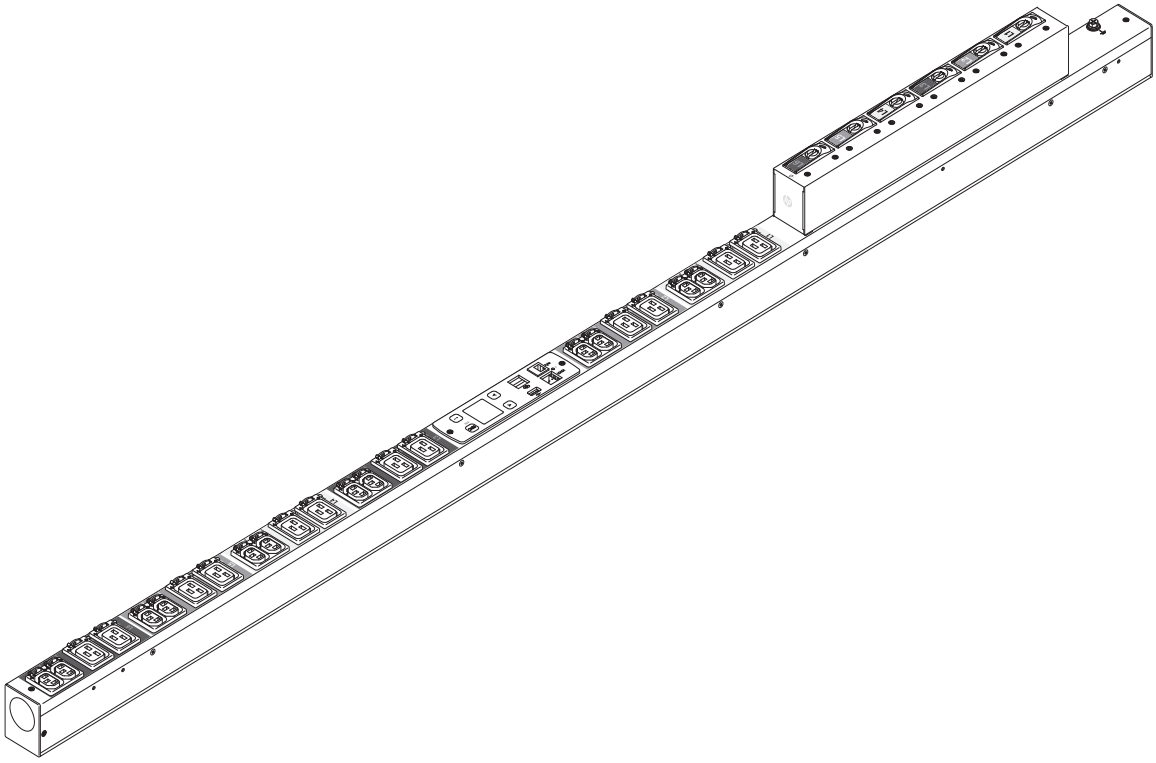


Figure 9. 3Ph H8B55A Model

Figure 10 illustrates the 3Ph H8B56A MA PDU model.

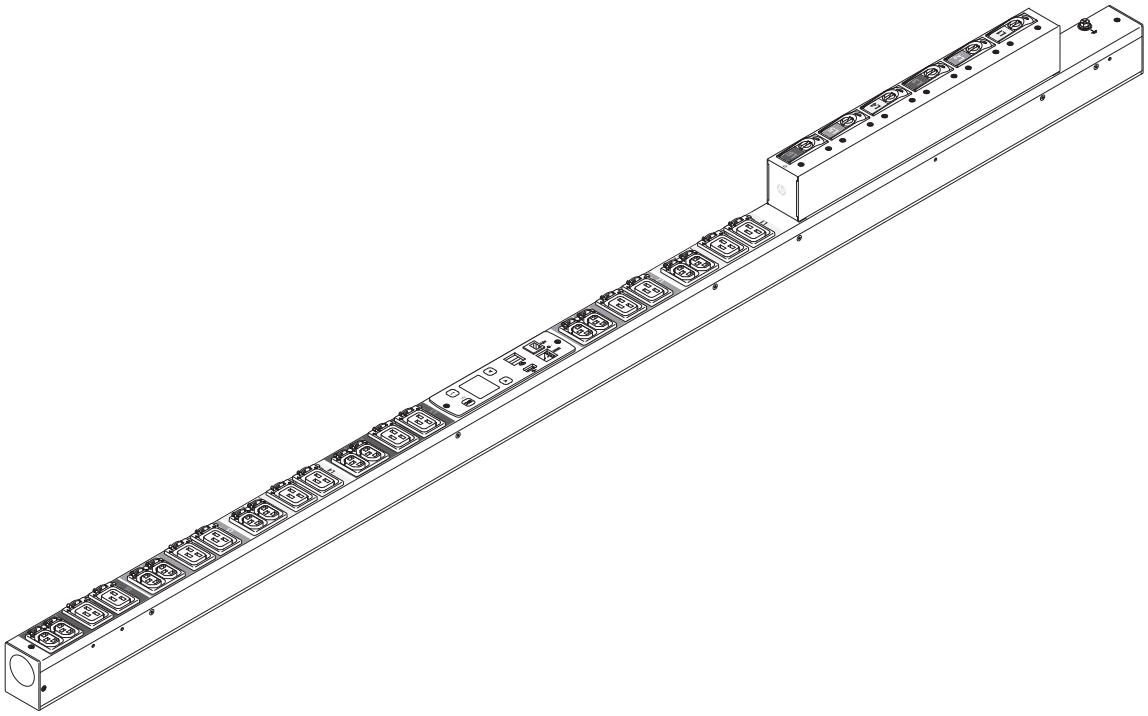


Figure 10. 3Ph H8B56A Model

Special Equipment

Environmental Monitoring Probe Equipment

Optional environmental monitoring probe (EMP) equipment provides monitoring of external temperature, humidity, and the status of contact devices (sensors), providing greater power management control and flexible monitoring. This optional equipment can be connected to the MA PDU. The monitoring firmware collects and reports data from the sensors.

NOTE EMP equipment is optional and must be purchased separately.

22U Shipping Brackets

The 22U HP MA PDUs are shipped with shipping retention brackets. The shipping retention bracket is used when a 22U MA PDU is installed into the rack and the rack is being shipped without removing the MA PDU.

Features

The MA PDUs provide outstanding performance and reliability, including the following unique benefits.

Ease of Use

- Easy and flexible rack installation
- Easy-to-use interface to display input and output status
- Remote and local firmware updates

- Top and bottom mounting in the rack
- Mounting holes on the back, left side, and right side to accommodate suitability for each customer site

Communication

- Comprehensive power management and flexible configuration through a Web browser or a serial connection, SNMP (Simple Network Management Protocol), or a console emulator, such as HyperTerminal
- Compatibility with network management tools, facilitated by SNMP protocol

Power Control Management

- Fully shrouded local branch circuit breakers on products rated over 16A (Europe)/20A (US) to protect connected equipment against overload and short circuits

Monitoring

- Monitoring the MA PDU locally or remotely through a console or network
- Monitoring data for multiple daisy-chained MA PDUs from the same network connection
- Remote monitoring of connected environmental sensors
- Dual-color LCD for higher visibility on local alarms
- External connections to allow remote management by network and serial communications (RS-232 or RJ-45 connector)
- Firmware network stack supports both IPv4 and IPv6

Configurability and Security

- Configurable alarm thresholds
- Configurable user-security and permission control
- Local and remote configuration functions available through onboard LCD display of menu selections, Web interface, or CLI interface

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 HP Managed PDU. Please read all instructions before operating the equipment and save this manual for future reference.

For safety, environmental, and regulatory information, see *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the HP website (http://www.hp.com/support/Safety-Compliance-EnterpriseProducts).

DANGER

This MA PDU contains **LETHAL VOLTAGES**. All repairs and service should be performed by **AUTHORIZED SERVICE PERSONNEL ONLY**. There are **NO USER SERVICEABLE PARTS** inside the MA PDU. The installation of options, routine maintenance, and service of this product must be performed by individuals who are knowledgeable about the procedures, precautions, and hazards associated with AC power products.

IT IS ESSENTIAL THAT THIS EQUIPMENT IS CONNECTED TO AN ELECTRICAL SUPPLY THAT HAS PROTECTIVE GROUND CONDUCTOR.

WARNING

HIGH LEAKAGE CURRENT. It is essential that you make an earth connection before connecting the supply.

CAUTION

- To reduce the risk of fire or electric shock, install this MA PDU in a temperature and humidity controlled, indoor environment, free of conductive contaminants. Do not operate near water or excessive humidity (90% maximum noncondensing).
- Ambient temperature must not exceed 0°C to 50°C (32°F to 122°F) on all INTL and WW models.
- Ambient temperature must not exceed 0°C to 60°C (32°F to 140°F) on all NA/JPN (except as noted previously).
- 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. When using a backup UPS, power the computer, monitor, and appliance off the supply.
- The installation power outlet used for the power supply to this equipment must be installed near the equipment and must be easily accessible. If the PDU does not provide an input branch circuit breaker, a socket-outlet or disconnection device must be installed near the PDU 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 THE POWER SUPPLY PLUG.
- This MA PDU is intended for providing power to equipment only. Secondary (satellite) power strips shall not be connected to the outlets.

- The internal components can become extremely hot during operation. Allow sufficient time for the PDU to cool before handling.
- This equipment is intended for installation in Restricted Access Locations such as computer rooms, network closets, and equipment racks.
- 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 to provide systems compliant with relevant standards.

⚠ CAUTION

This product contains a lithium battery on the internal eNMC module:

- The battery is not user-replaceable. There is a danger of explosion if the battery is not correctly replaced. The battery must be replaced with the same (or equivalent) type of battery.
- The battery is not user-replaceable. However, 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

The 22U and 42U HP Managed PDUs are mounted vertically inside rack structures. Use the information in this chapter to prepare, install, and connect the MA PDU and optional accessories.

Installation Precautions

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

- Only a competent service person should install, test, or configure the MA 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 11.
- Review the documentation that comes with your rack cabinet for safety and cabling information.

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 air temperature is below 50°C (122°F).
- Take all necessary precautions to handle the weight of the devices.
- Connect all power cords to properly wired and grounded electrical outlets.
- Verify that the power outlet is near the equipment and is easily accessible so that the MA PDU can be disconnected quickly.

CAUTION

The installation power outlet used for the power supply to this equipment must be installed near the equipment and must be easily accessible. If the PDU does not provide an input branch circuit breaker, a socket-outlet or disconnection device must be installed near the PDU 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 MA PDU outlets before performing any testing.
- For units without circuit breakers (H8B49A and H8B54A), the output power cannot be turned on and off with a button or switch. These PDUs are always on when they are plugged in. These PDUs are always off when they are unplugged.
- For units with circuit breakers, 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 MA PDU, unplug it.

NOTE The illustrations in this document might differ slightly from your hardware.

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.

Installation Overview

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

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

Tools

The following tools may be needed to install the MA PDU in a rack cabinet (varies with round-, threaded-, or square-hole racks):

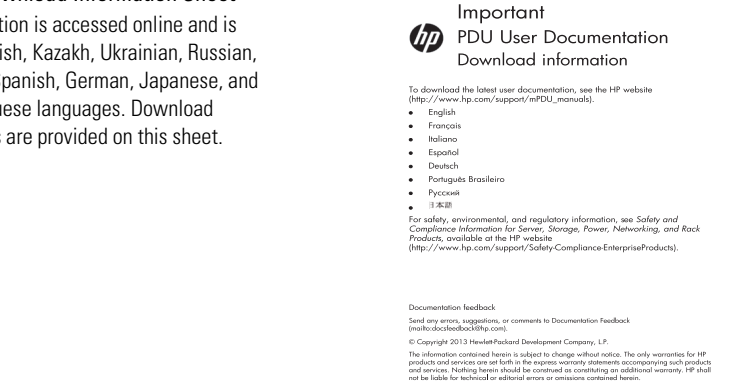
- Phillips cross-head screwdriver
- Flat-blade screwdriver
- 8.7 mm (11/32") wrench

Package Contents

Table 1 lists the parts that are included with the PDUs.

Table 1. Parts Included with HP PDU Models

Quantity	Description
1	User Documentation Download Information Sheet **NOTE** User documentation is accessed online and is available in English, Kazakh, Ukrainian, Russian, French, Italian, Spanish, German, Japanese, and Brazilian Portuguese languages. Download information links are provided on this sheet.
1	Safety/Regulatory Information Sheet



Important
PDU User Documentation
Download information

To download the latest user documentation, see the HP website (http://www.hp.com/support/mPDU_manuals).

- English
- Français
- Italiano
- Español
- Deutsch
- Português Brasileiro
- Русский
- 日本語

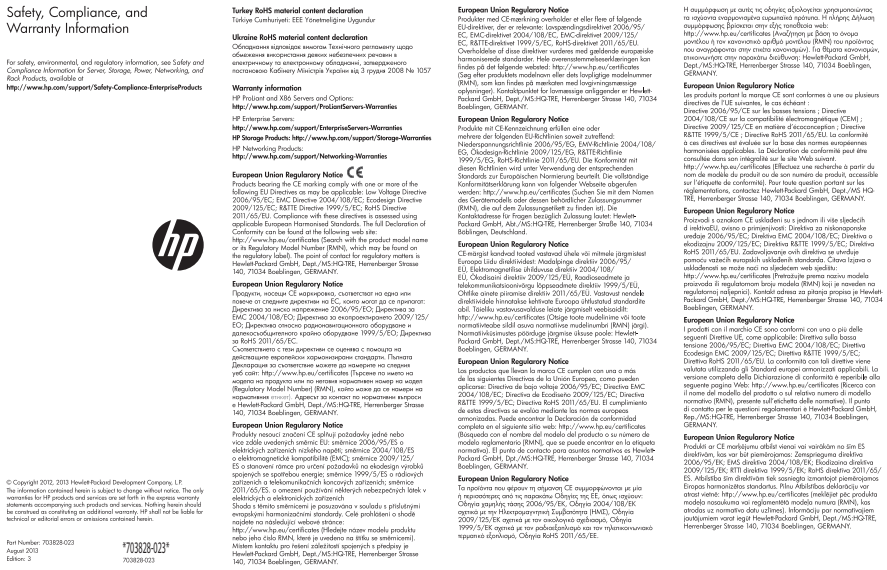
For safety, environmental, and regulatory information, see *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the HP website (http://www.hp.com/support/Safety-Compliance-EnterpriseProducts).

Documentation feedback

Send any errors, suggestions, or comments to Documentation Feedback (mailto:docfeedback@hp.com).

Part Number: 733168-001
May 2013
Edition: 1

733168-001
733168-001



Safety, Compliance, and
Warranty Information

For safety, environmental, and regulatory information, see *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at
http://www.hp.com/support/Safety-Compliance-EnterpriseProducts

Turkey RoHS material content declaration
Türkiye Cumhuriyeti: EEE Yönetmeliğine Uygundur

Ukraine RoHS material content declaration
Обладнання відповідає вимогам Технічного регламенту щодо обмеження використання деяких небезпечних речовин в електричному та електронному обладнанні, затвердженого постановою Кабінету Міністрів України від 3 грудня 2008 № 1057

Warranty information
HP ProLiant and X86 Servers and Options:
http://www.hp.com/support/ProLiantServers-Warranties

HP Enterprise Servers:
http://www.hp.com/support/EnterpriseServers-Warranties
HP Storage Products: http://www.hp.com/support/Storage-Warranties
HP Networking Products:
http://www.hp.com/support/Networking-Warranties

European Union Regulatory Notice CE
Products bearing the CE marking comply with one or more of the following EU Directives as may be applicable: Low Voltage Directive 2006/95/EC, EMC Directive 2004/108/EC, Ecodesign Directive 2009/125/EC, R&TTE Directive 1999/5/EC, RoHS Directive 2011/65/EU. Compliance with these directives is assessed using applicable European Harmonised Standards. The full Declaration of Conformity can be found at the following web site:
http://www.hp.eu/certificates (Search with the product model name or its Regulatory Model Number (RMN), which may be found on the regulatory label). The point of contact for regulatory matters is Hewlett-Packard GmbH, Dept./MS:HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

European Union Regulatory Notice
Продукти, носещи CE маркировка, съответстват на една или повече от следните директиви на ЕС, които могат да се приложат: Директива за ниско напрежение 2006/95/ЕО; Директива за ЕМС 2004/108/ЕО; Директива за екопроектиране 2009/125/ЕО; Директива относно радиосъоръженията и далекосъобщителното крайно оборудване 1999/5/ЕО; Директива за RoHS 2011/65/ЕС.
Съответствието с тези директиви се оценява с помощта на действащите европейски хармонизирани стандарти. Пълната Декларация за съответствие можете да намерите на следния уеб сайт: http://www.hp.eu/certificates (Търсене по името на модела на продукта или по неговия нормативен номер на модел (Regulatory Model Number) (RMN), който може да се намери на нормативния етикет). Адресът за контакт по нормативни въпроси е Hewlett-Packard GmbH, Dept./MS:HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

European Union Regulatory Notice
Produkty nesoucí značení CE splňují požadavky jedné nebo více zdeše uvedených směrnic EU: směrnice 2006/95/ES o elektrických zařízeních nízkého napětí; směrnice 2004/108/ES o elektromagnetické kompatibilitě (EMC); směrnice 2009/125/ES o stanovení rámce pro určení požadavků na ekodesign výrobků spojených se spotřebou energie; směrnice 1999/5/ES o radiových zařízeních a telekomunikačních koncových zařízeních; směrnice 2011/65/ES, o omezení používání některých nebezpečných látek v elektrických a elektronických zařízeních
Shoda s těmito směrnicemi je posuzována v souladu s příslušnými evropskými harmonizačními standardy. Celé prohlášení o shodě najdete na následující webové stránce:
http://www.hp.eu/certificates (Předejte název modelu produktu nebo jeho číslo RMN, které je uvedeno na štítku se směrnicemi). Místem kontaktu pro řešení záležitostí spojených s předpisy je Hewlett-Packard GmbH, Dept./MS:HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

European Union Regulatory Notice
Produkter med CE-mærkning overholder et eller flere af følgende EU-direktiver, der er relevante: Lavspændingsdirektivet 2006/95/EC, EMC-direktivet 2004/108/EC, EMC-direktivet 2009/125/EC, R&TTE-direktivet 1999/5/EC, RoHS-direktivet 2011/65/EU. Overholdelse af disse direktiver vurderes med gældende europæiske harmoniserede standarder. Hele overensstemmelseserklæringen kan findes på det følgende websted: http://www.hp.eu/certificates (Søg efter produktets modelnavn eller dets lovpligtige modelnummer (RMN), som kan findes på mærkaten med lovgivningsmæssige oplysninger). Kontaktpunktet for lovmæssige anliggender er Hewlett-Packard GmbH, Dept./MS:HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

European Union Regulatory Notice
Produkte mit CE-Kennzeichnung erfüllen eine oder mehrere der folgenden EU-Richtlinien soweit zutreffend: Niederspannungsrichtlinie 2006/95/EG, EMV-Richtlinie 2004/108/EG, Ökodesign-Richtlinie 2009/125/EG, R&TTE-Richtlinie 1999/5/EG, RoHS-Richtlinie 2011/65/EU. Die Konformität mit diesen Richtlinien wird unter Verwendung der entsprechenden Standards zur Europäischen Normierung beurteilt. Die vollständige Konformitätserklärung kann von folgender Webseite abgerufen werden: http://www.hp.eu/certificates (Suchen Sie mit dem Namen des Gerätemodells oder dessen behördlicher Zulassungsnummer (RMN), die auf dem Zulassungsetikett zu finden ist). Die Kontaktadresse für Fragen bezüglich Zulassung lautet: Hewlett-Packard GmbH, Abt./MS:HQ-TRE, Herrenberger Straße 140, 71034 Böblingen, Deutschland.

European Union Regulatory Notice
CE-märgist kandvad tooted vastavad ühele või mitmele järgmisest Euroopa Liidu direktiividest: Madalpinge direktiiv 2006/95/EÜ, Elektromagnetilise ühilduvuse direktiiv 2004/108/EÜ, Ökodisaini direktiiv 2009/125/EÜ, Raadiosaadetmete ja telekommunikatsioniväljugu lõppseadmete direktiiv 1999/5/EÜ, Ohtlike ainete piiramise direktiiv 2011/65/EÜ. Vastavust nendele direktiividele hinnatakse kehtivate Euroopa ühtlustatud standardite abil. Täielikku vastavusavalduse leiate järgmiselt veebisaidilt: http://www.hp.eu/certificates (Otsige toote mudelinime või toote normatiivtoobe sildil asuva normatiivse mudelinumbri (RMN) järgi). Normatiivküsimustes pöörduge järgmise isikuse poole: Hewlett-Packard GmbH, Dept./MS:HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

European Union Regulatory Notice
Los productos que llevan la marca CE cumplen con una o más de las siguientes Directivas de la Unión Europea, como pueden aplicarse: Directiva de bajo voltaje 2006/95/EC, Directiva EMC 2004/108/EC, Directiva de Ecodiseño 2009/125/EC, Directiva R&TTE 1999/5/EC, Directiva RoHS 2011/65/EU. El cumplimiento de estas directivas se evalúa mediante las normas europeas armonizadas. Puede encontrar la Declaración de conformidad completa en el siguiente sitio web: http://www.hp.eu/certificates (Búsqueda con el nombre del modelo del producto o su número de modelo reglamentario (RMN), que se puede encontrar en la etiqueta normativa). El punto de contacto para asuntos normativos es Hewlett-Packard GmbH, Dpt./MS:HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

European Union Regulatory Notice
Tuotteissa, joissa on CE-merkintä, noudatetaan yhtä tai useampaa seuraavista EU-direktiiveistä sovellettavuuden mukaan: Pienjännitedirektiivi 2006/95/EY, EMC-direktiivi 2004/108/EY, Ekologisen suunnittelun direktiivi 2009/125/EY, R&TTE-direktiivi 1999/5/EY, RoHS-direktiivi 2011/65/EU. Vaatimustenmukaisuus arvioidaan soveltamalla yhdenmukaistettuja eurooppalaisia standardeja. Täydellinen vaatimustenmukaisuusvakuutus on nähtävissä seuraavassa verkko-osoitteessa: http://www.hp.eu/certificates (Hae tuotteen mallinimellä tai sen säädösten mukaisella mallinumerolla (RMN), joka löytyy säädöstarrasta). Säädöksiä koskevissa asioissa voit olla yhteydessä: Hewlett-Packard GmbH, Dept./MS:HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

European Union Regulatory Notice
Les produits portant la marque CE sont conformes à une ou plusieurs directives de l'UE suivantes, le cas échéant : Directive 2006/95/CE sur les basses tensions ; Directive 2004/108/CE sur la compatibilité électromagnétique (CEM) ; Directive 2009/125/CE en matière d'écoconception ; Directive R&TTE 1999/5/CE ; Directive RoHS 2011/65/EU. La conformité à ces directives est évaluée sur la base des normes européennes harmonisées applicables. La Déclaration de conformité peut être consultée dans son intégralité sur le site Web suivant :
http://www.hp.eu/certificates (Effectuez une recherche à partir du nom de modèle du produit ou de son numéro de produit, accessible sur l'étiquette de conformité). Pour toute question portant sur les réglementations, contactez Hewlett-Packard GmbH, Dept./MS HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

European Union Regulatory Notice
Proizvodi s oznakom CE usklađeni su s jednom ili više sljedećih direktiva(EU), ovisno o primjenjivosti: Direktiva za niskonaponske uređaje 2006/95/EC; Direktiva EMC 2004/108/EC; Direktiva o ekodizajnu 2009/125/EC; Direktiva R&TTE 1999/5/EC; Direktiva RoHS 2011/65/EU. Zadovoljavanje ovih direktiva se utvrđuje pomoću važećih europskih usklađenih standarda. Cjelovitu izjavu o usklađenosti se može naći na sljedećem web sjedištu:
http://www.hp.eu/certificates (Pretražite prema nazivu modela proizvoda ili regulatornom broju modela (RMN) koji je naveden na regulatornoj naljepnici). Kontakt adresa za pitanja propisa je Hewlett-Packard GmbH, Dept./MS:HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

European Union Regulatory Notice
I prodotti con il marchio CE sono conformi con uno o più delle seguenti Direttive UE, come applicabile: Direttiva sulla bassa tensione 2006/95/EC; Direttiva EMC 2004/108/EC; Direttiva Ecodesign EMC 2009/125/EC; Direttiva R&TTE 1999/5/EC; Direttiva RoHS 2011/65/EU. La conformità con tali direttive viene valutata utilizzando gli Standard europei armonizzati applicabili. La versione completa della Dichiarazione di conformità è reperibile alla seguente pagina Web: http://www.hp.eu/certificates (Ricerca con il nome del modello del prodotto o sul relativo numero di modello normativo (RMN), presente sull'etichetta delle normative). Il punto di contatto per le questioni regolamentari è Hewlett-Packard GmbH, Dept./MS:HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

European Union Regulatory Notice
Produkti ar CE marķējumu atbilst vienai vai vairākām no šīm ES direktīvām, kas var būt piemērojamas: Zemsprieguma direktīva 2006/95/EK; EMS direktīva 2004/108/EK; Ekodizaina direktīva 2009/125/EK; RTTI direktīva 1999/5/EK; RoHS direktīva 2011/65/ES. Atbilstība šīm direktīvām tiek sasniegta izmantojot piemērojamos Eiropas harmonizētos standartus. Pilnu Atbilstības deklarāciju var atrast vietnē: http://www.hp.eu/certificates (meklējot pēc produkta modeļa nosaukuma vai reglamentētā modeļa numura (RMN), kas atrodas uz normatīvo datu uzlīmes). Informācija par normatīvajiem jautājumiem varat iegūt Hewlett-Packard GmbH, Dept./MS:HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

European Union Regulatory Notice
Η συμμόρφωση με αυτές τις οδηγίες αξιολογείται χρησιμοποιώντας τα ισχύοντα εναρμονισμένα ευρωπαϊκά πρότυπα. Η πλήρης Δήλωση συμμόρφωσης βρίσκεται στην εξής τοποθεσία web:
http://www.hp.eu/certificates (Αναζήτηση με βάση το όνομα μοντέλου ή τον κανονιστικό αριθμό μοντέλου (RMN) του προϊόντος που αναγράφονται στην ετικέτα κανονισμών). Για θέματα κανονισμών, επικοινωνήστε στην παρακάτω διεύθυνση: Hewlett-Packard GmbH, Dept./MS:HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, GERMANY.

Part Number: 703828-023
August 2013
Edition: 3

703828-023
703828-023

Table 1. Parts Included with HP PDU Models (Continued)

Quantity	Description
1	**Installation Pack for 42U Models:** (2) Key hole buttons, (3) M4-0.5P screws SEE NOTE 1 (1) Serial cable used for RS-232 connection between the PDU and a PC (1) RJ-45 Cable (60 cm - shielded) used for Ethernet or daisy-chain connection between the PDU and a PC SEE NOTE 2 (1) Y Splitter installed in the Daisy-chain port and used for daisy-chaining three or four PDUs together (2) Cable ties

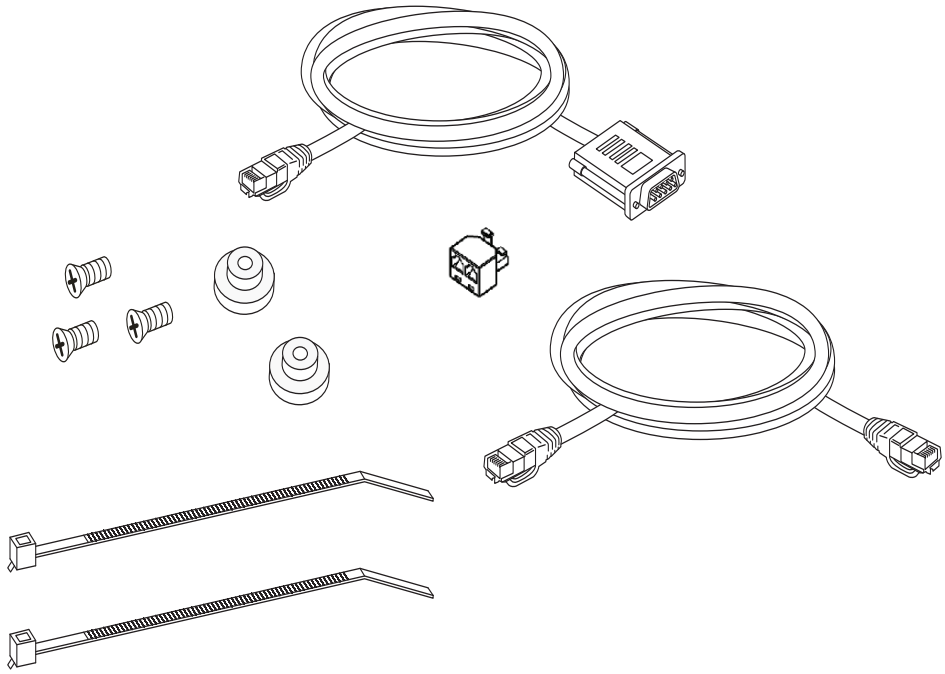
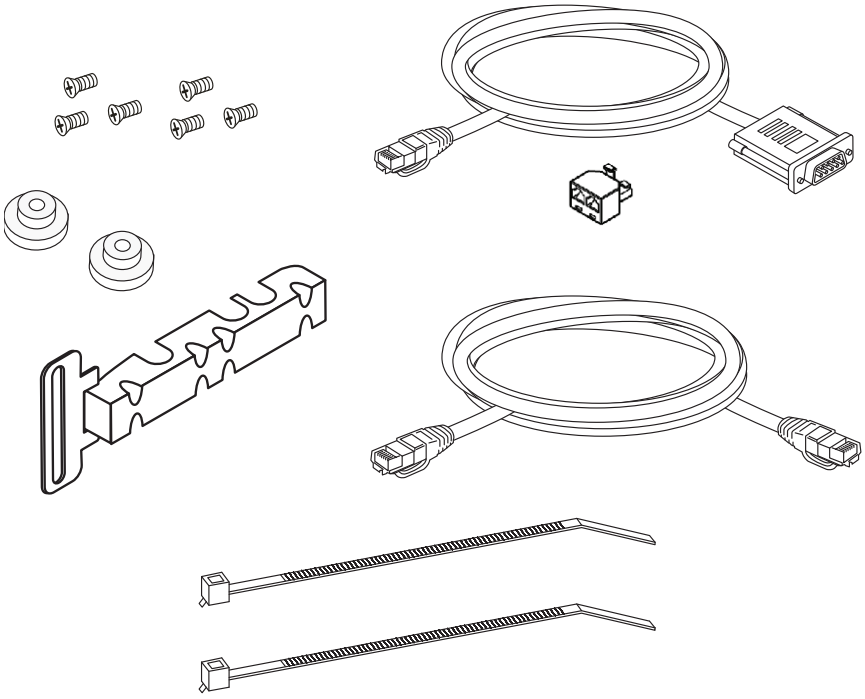


Table 1. Parts Included with HP PDU Models (Continued)

Quantity	Description
1	**Installation Pack for 22U Models:** (2) Key hole buttons, (3) M4-0.5P screws SEE NOTE 1 (1) Bracket, (3) self-tapping bracket screws (1) Serial cable used for RS-232 connection between the PDU and a PC (1) RJ-45 Cable (60 cm - shielded) used for Ethernet or daisy-chain connection between the PDU and a PC SEE NOTE 2 (1) Y Splitter installed in the Daisy-chain port and used for daisy-chaining three or four PDUs together (2) Cable ties



NOTE 1 The keyhole mounting button and screws are packaged together in a small, clear shipping bag within a larger bag or box. These parts are shipped in the carton with the MA PDU.

NOTE 2 The Ethernet cable is intended for customers with small data centers, for maintenance, or for checks in a warehouse setting. Larger data center customers may choose to use their own network cable.

IMPORTANT

Model H8B49A has an IEC 60320 C20 power input receptacle for attaching a C19 to the country-specific power cord of your choice. These cables are ordered separately.

Special Equipment

Environmental Monitoring Probe Equipment

EMP equipment with sensors can be connected to the MA PDU as an accessory that collects temperature and humidity data, as well as two dry contacts. The equipment is user-provided 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.

Shipping Retention Brackets

Shipping retention brackets can be installed to provide additional stability for the models when the MA PDU is installed in a rack and the rack is being shipped. The bracket is used only for 22U models. The 42U models can be secured for shipping within a rack using a cable tie on the power cable. Mounting screws (self-tapping screws) are supplied with the bracket in the shipping carton. When the MA PDU is unpacked, retain the brackets and mounting hardware for future use.

Secure the bracket to the rack above the MA PDU to help prevent it from shifting during transport as follows (see Figure 11):

1. Align the bracket with the top of the MA PDU model and hold it in place above the PDU.
2. Use the two bracket mounting screws to attach the bracket to the rack post.

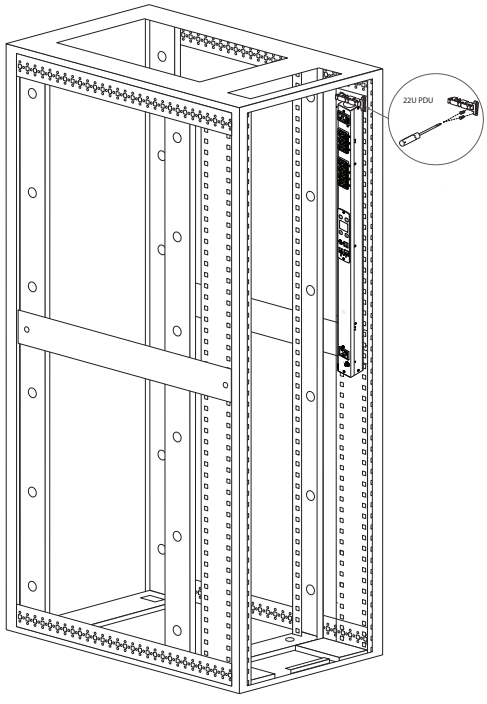


Figure 11. Installing a Bracket for Transporting a 22U PDU in the Rack

IEC Outlet Grip Plug Retention Mechanism

The HP Managed 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.

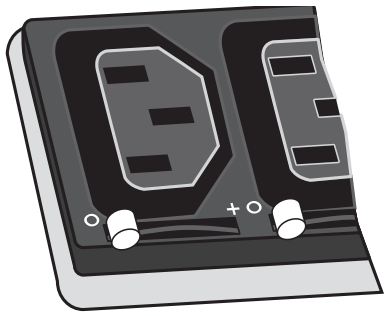


Figure 12. Plug Retention Mechanism

NOTE In the event of an emergency, only unplug the power cord when the grip plug retention mechanism is in the "+" position (plug retained). To remove the plug, gently rotate the lever to the "O" (plug freed) position and remove the plug.

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

Installing the MA PDU in a Rack Cabinet

HP MA PDUs are designed to be installed in HP 10000 series racks and Intelligent series racks, but can be installed in other data center racks.

NOTE All vertically installed MA PDU models use keyhole mounting buttons for installation in a rack cabinet.

Vertical Installation

The following vertical configurations are available:

- A single 42U MA PDU on one side or both sides of the rack
- Two 22U or 42U MA PDUs side-by-side on one side or both sides of the rack
- A single or two 22U MA PDUs on one side or both sides of the rack

NOTE Two 22U MA PDU models fit vertically in a 42U HP rack with one mounted on top of the other.

A top and button mounting button should be installed on each PDU to install it vertically. The mounting buttons are then inserted into the corresponding keyhole slot.

Installing PDUs

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

1. Locate the two keyhole mounting buttons and installation screws (supplied).
2. Decide how to orient the MA PDU in the rack.

NOTE The MA PDU orientation you choose will determine whether you install the mounting buttons on the back, left side, or right side of the MA PDU.

3. Using the supplied screws and a Phillips screwdriver, secure the top and bottom mounting buttons on the back, left side, or right side of the MA PDU. The screw should be torqued to six inch-pounds.

NOTE Make sure the screw is completely seated in the mounting button so that it is not protruding from the recessed button mounting hole.

4. Before attempting to mount the MA PDU or MA PDUs, locate the keyhole slots on the rack post that correspond with the position of the top and bottom mounting buttons.

CAUTION

Use great care in handling the PDU in the following steps. Avoid contact between the PDU and the rack because there is a risk of damage to the PDU or the rack.

5. Install the PDU or PDUs in the rack:
   - Carefully move the PDU into position against the rail.
   - Insert the top and bottom mounting buttons into the appropriate keyhole slots.
   - Push down to secure the PDU in position.
   - Repeat with any additional PDUs.
6. Continue to "Grounding the MA PDU"if you are installing a ground screw and grounding cable. Otherwise, go to "Network and Environmental Ports" on page 21.

Grounding the MA PDU

NOTE Grounding the MA PDU is optional but recommended.

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.

Neither the earth bonding screw nor the surface of the chassis around the screw is painted. This ensures that the screw and washers make contact with bare metal, not a painted surface.

The ground symbol is impressed in the chassis above the earth bonding screw.

To ground the MA PDU, connect a grounding cable (not supplied) from earth to the grounding screw shown in Figure 13.

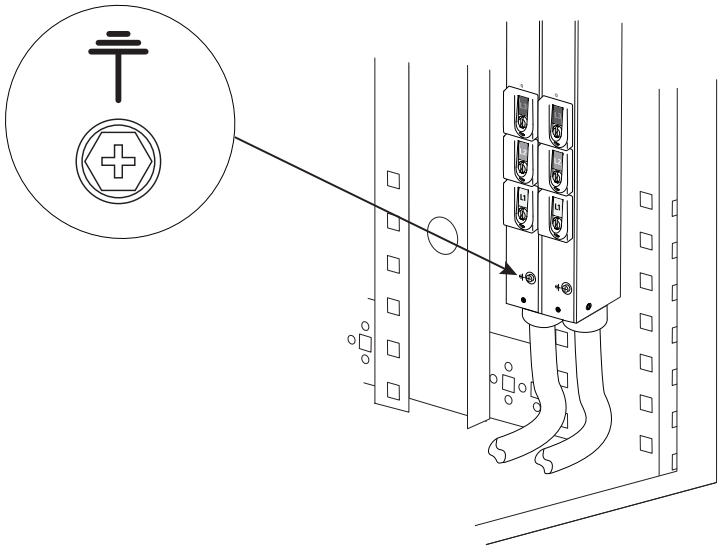


Figure 13. Grounding the MA PDU

Network and Environmental Ports

The MA PDUs provide four types of ports for network connectivity and environmental monitoring.

- To connect the MA PDU to a serial port on a computer, go to the next section, "Connecting to a Computer Serial Port".
- To connect the MA PDU to an Ethernet port and the LAN (Local Area Network), go to "Connecting to a LAN Ethernet Port" on page 22.
- To daisy-chain multiple MA PDUs, go to "Connecting Multiple MA PDUs in a Daisy Chain" on page 23.
- To connect the MA PDU to EMP equipment, go to "Connecting Optional Environmental Monitoring Probe Equipment" on page 25.

Connecting to a Computer Serial Port

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

To connect the MA PDU to a computer:

1. Verify that the computer has a communication program such as HyperTerminal.
2. Locate the DB9-to-RJ-45 cable (provided).
3. Connect the RJ-45 end of the cable to the RS-232 connector on the front panel of your MA PDU model (see Figure 14). Connect the DB9 end of the cable to the serial connector on the computer.

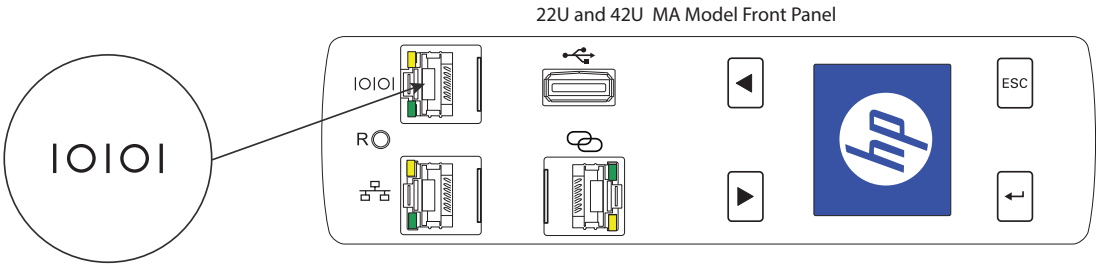


Figure 14. Connecting to a Computer Serial Port

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

4. Open the communication program on the computer and select the serial port connection (such as COM1).
5. Verify that the port settings are configured as follows:
   - Baud rate (bits per second) = 9600
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None
6. Verify that the MA PDU is turned on.
7. Press **Enter** (↵) to display the opening configuration prompt and type **admin** (the default login).
8. Press **Enter** (↵) and type **admin** (the default access password).

Connecting to a LAN Ethernet Port

Connecting the MA PDU to a LAN provides communication through an Internet or Intranet connection. You can monitor the MA PDU from any computer connected to the same network.

To connect the MA PDU to a LAN:

1. Locate the Ethernet cable (provided).

NOTE A short Ethernet cable is supplied in the MA PDU shipping carton. This cable is useful in a small data center for maintenance or for checks in a warehouse setting. Larger data center customers may choose to use their own network cable.

2. Connect one end of the cable to the Ethernet connector on the MA PDU (see Figure 15). Connect the other end of the cable to the Ethernet connector on the router (or other LAN device.

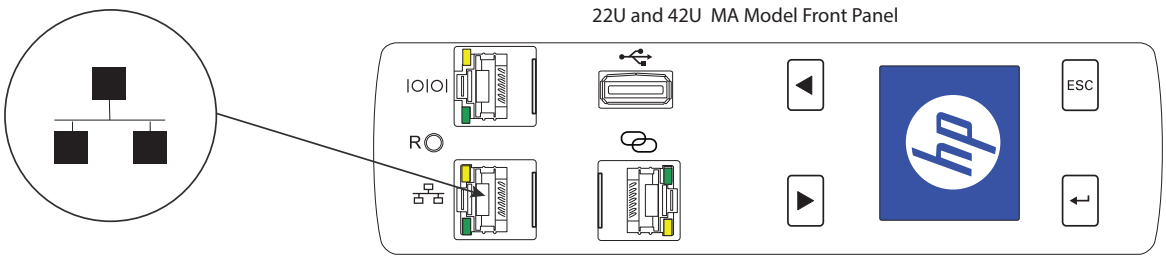


Figure 15. Connecting the MA PDU to a LAN

Connecting Multiple MA PDUs in a Daisy Chain

Multiple MA PDUs can be chained together using an Ethernet cable between the Daisy Chain ports located on the front panel. This allows access to the MA PDU data of multiple MA PDUs from the same network connection. One MA PDU is defined as the Host. This is the MA PDU with a connection to the network. The other MA PDU (or MA PDUs) are defined as Devices and they are connected to the host.

Configure the MA PDUs using the LCD or the CLI interfaces. Monitor the MA PDUs using the CLI interface or the Web interface.

To connect MA PDUs in a Daisy Chain communication configuration:

1. Locate an Ethernet cable or cables (one cable is supplied).
2. How many MA PDUs are you daisy-chaining?
   - If three or four, go to Step 3.
   - If two, go to Step 4.
3. Insert the Y splitter in the Daisy Chain connector of the middle MA PDU or MA PDUs as shown in Figure 16.
4. Connect one end of the cable to the Daisy Chain connector on one MA PDU. Connect the other end of the cable to the Daisy Chain connector on the other MA PDU or MA PDUs as shown in Figure 16.

NOTE Only one MA PDU in a daisy-chained group can have a network connection through the Ethernet port. This MA PDU is the Host and any connected MA PDUs are Devices.

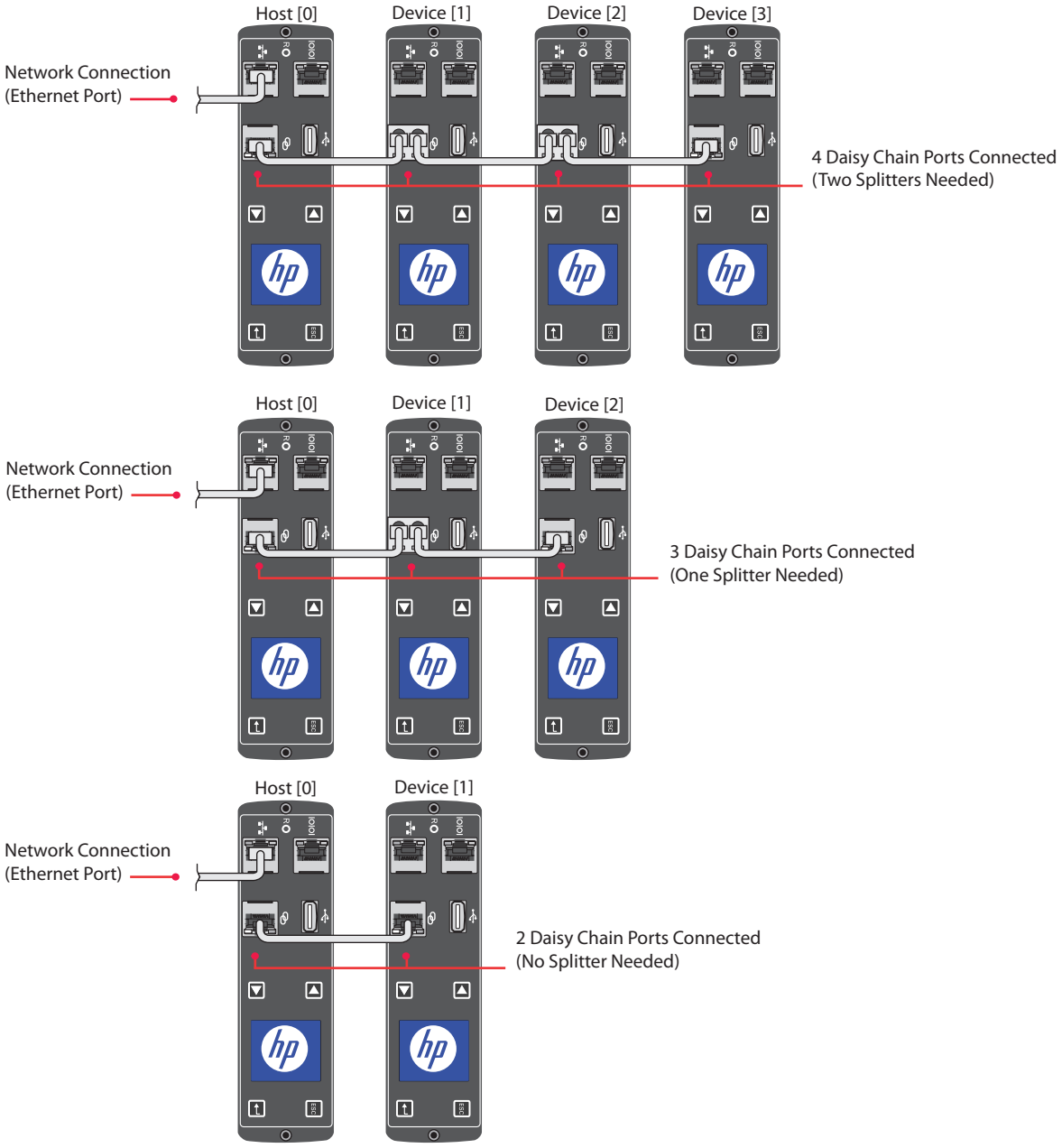


Figure 16. Locating the Daisy Chain Connector

5. Configure the MA PDUs with either the LCD interface or the CLI interface.
   - To configure the MA PDUs using the LCD interface, go to "Daisy Chain Submenu" on page 52.
   - To configure the MA PDUs using the CLI interface, go to "Serial Interface Operation" on page 92.
6. Monitor the MA PDUs with the CLI interface or the Web interface.
   - To monitor the MA PDUs using the Web interface, go to "Web Interface Operation" on page 57.
   - To monitor the MA PDUs using the CLI interface, go to "Serial Interface Operation" on page 92.

Connecting Optional Environmental Monitoring Probe Equipment

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

You can install an optional EMP now or after completing the MA PDU installation and startup. Optional EMP equipment can be installed without turning off power to the MA 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 RJ-45-to-RJ-45 Ethernet cable.
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 RJ-45 connector on the MA PDU (see Figure 17).

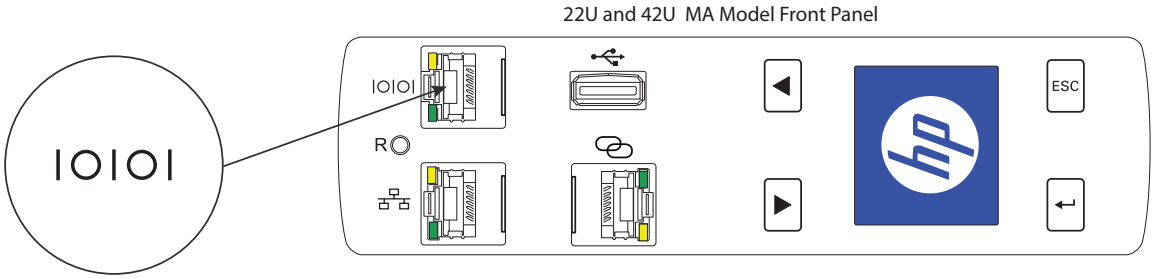


Figure 17. Connecting the EMP to the RJ-45 Serial Port Connector

NOTE The maximum cable length is 2.99m (9.8 ft).

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

Connecting the Output Devices

The MA PDU outlets are available for connecting and monitoring devices such as workstations, servers, and printers. Connect a device you want to monitor to a power outlet on the MA 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. **For MA PDUs with detachable power cords.** If the power cord is not connected, connect the power cord to the MA PDU. Otherwise, go to Step 3.
3. Route the MA PDU power cord toward a dedicated power source. 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 MA PDU into an appropriately rated outlet for its type.

NOTE 2 Do not replace or rewire the power cord.

4. Connect the power cord to a properly wired and grounded dedicated power source. The MA PDU turns on and displays the HP startup screen while starting. After five seconds, the sequence of screensaver screens for this MA PDU model begin cycling.
5. Verify that no alarms display on the LCD. To resolve alarms, see "Maintenance and Alarms" on page 121.
6. Make sure the grip plug retention lever is on the "O" position before inserting the plug.
7. Plug in your output devices to the outlet outlets on the MA 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 when setting up groups of outlets to start at the same time to avoid a large in-rush current.

8. Gently rotate the grip plug retention 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.

Operating the MA PDU

See "Operation Overview" on page 31 for instructions to operate the MA PDU, including starting and shutting down the equipment.

Chapter 4 Network Communication Configuration

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

In order to establish a network session, note the network configuration from the LCD. Users/admin can review and change the network information using CLI, Telnet, and GUI once connected.

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

The MA PDU defaults to using DHCP (Dynamic Host Configuration Protocol) when delivered. If you are unable to connect to the MA 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 CLI (command line interface).ga

The default settings are:

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

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. Obtain the IP address from the LCD home screen (see Figure 18).

Figure 18. LCD Home Screen

LCD— Static IP address

1. Disable DHCP (see Figure 19).

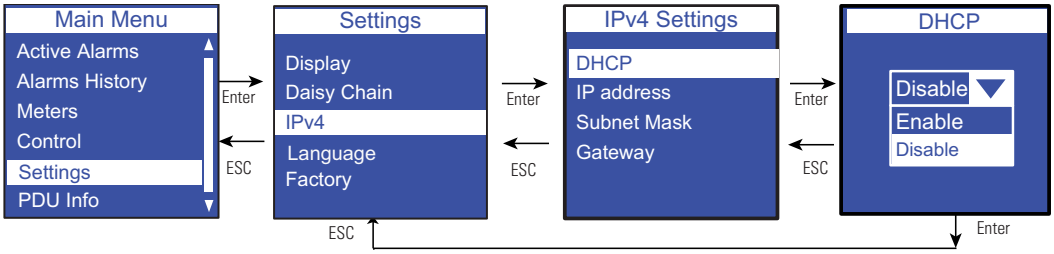


Figure 19. Disable DHCP

2. Set the static IP address (see Figure 20). Wait 10 seconds.

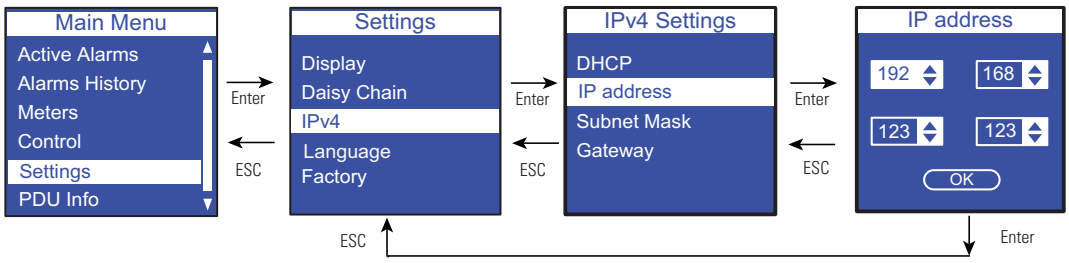


Figure 20. Set the Static IP Address

3. After 10 seconds, locate the Reset opening (labeled R) on the MA PDU (see Figure 21). Insert an electrically non-conductive probe, press the recessed button, and retract the probe. This restarts the eNMC module and applies the new settings (see Figure 21).

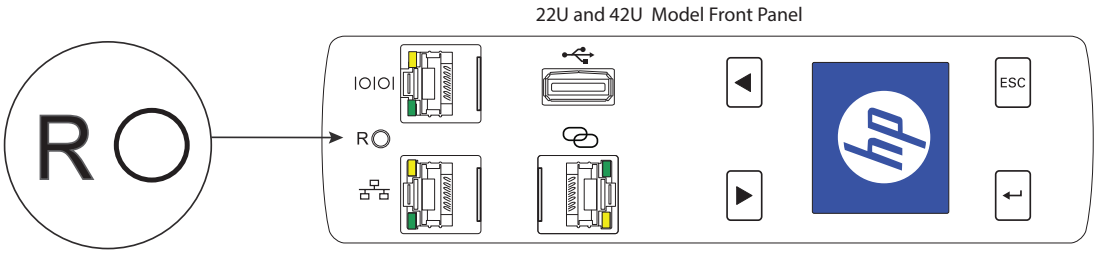


Figure 21. Reset Button

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 (admin) at the login prompt. For example:

   ```
   Enter Login: admin

   Enter Password:
   ```

2. Type admin (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. After 10 seconds, locate the Reset opening (labeled R). Insert an electrically non-conductive probe, press the recessed button, and retract the probe.

NOTE You can also connect up to four MA PDUs together using the Daisy Chain port and RJ-45 splitters. This enables multiple MA PDUs to communicate over one Ethernet port.

NOTE If you choose not to use the procedure to configure the communications module without the DHCP server installed, you can connect to the MA 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 **admin** in the User name field and **admin** in the Password field.
4. The home page opens with the MA PDU Overview page.

Chapter 5 Operation Overview

This chapter provides an overview of operation for the HP Managed PDUs.

Operation Features

Figure 22 shows isolated views of the display and connectivity areas.

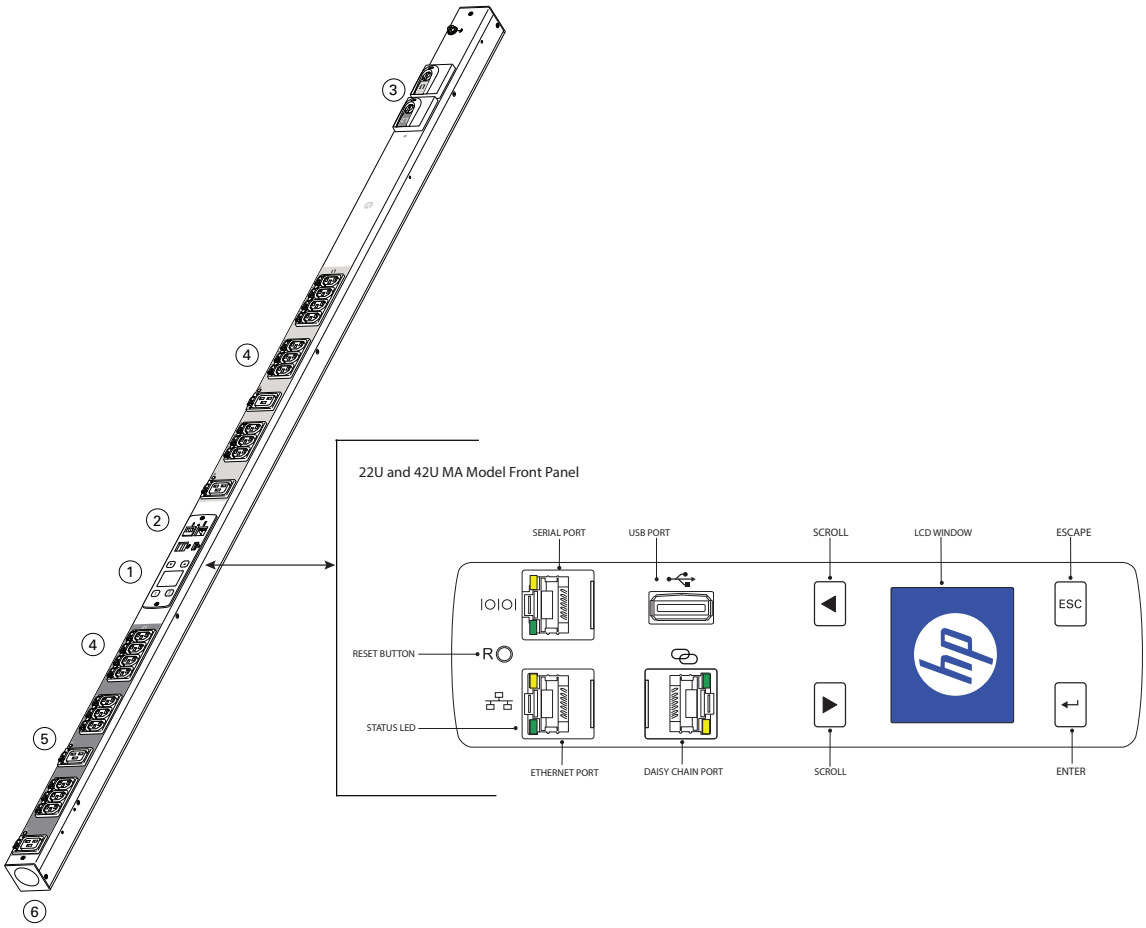


Figure 22. MA PDU Display and Connectivity

Table 2 describes the operation features shown in Figure 22.

Table 2. PDU Operation Features

Reference Number	Feature	Description
1	LCD Window	LCD Window: Displays information about load status, events, measurements, identification, and settings. The LCD also provides some basic configuration. For more information, see "Menu and Status Display" on page 34. Navigation buttons: Navigate through the display. For more information, see "Front Panel Ports, Status Indicators, and Operation Buttons" on page 35.
2	Connectivity and Monitoring ports	Serial Service and Communication Port: Connects to the serial (COM) 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 multiple MA PDUs together. USB Port: Used for Firmware upgrade. Reset Button: Restarts the MA PDU eNMC module. Resetting the MA PDU does not affect the loads. Insert and retract an electrically non-conductive probe in the reset opening to perform an eNMC module restart.
3	Circuit breakers	Activate if the load current rating of a power outlet 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** The On/Off positions are indicated on the circuit breakers. **NOTE** To manually disconnect power to a device that is connected to the MA PDU, disconnect the device's power cord from the MA PDU power outlet.
4	Power outlets	Allows you to connect one device to each outlet. The outlets are grouped by phase. Group configurations cannot be changed. For more information, see "Outlets and Circuit Breakers" on page 33.
5	Outlet indicator lights	Provides a bi-color LED to indicate the status for each output receptacle: • Solid red: Outlet off • Flashing red: Outlet on, but breaker off • Solid green: Outlet on • Flashing green: Outlet on, outlet warning or critical overload • Alternate flashing green and red: Outlet On, Breaker warning or critical overload
6	Input power cord	Allows you to connect to the power source. Input power cords are permanent for most models. Only the H8B48A model has detachable input power cords.

3Ph Configurations

The type of MA PDU input connector plug varies to accommodate different amperage ratings for 3Ph models. The IEC 60309 connector plugs are configured as delta or wye topologies as follows:

- The delta configuration uses a four-wire input connector plug with three phase wires, a protective earth (ground) wire, and no neutral wire. This is commonly expressed as 3W+PE (delta).
- The wye configuration uses a five-wire input connector plug with three phase wires, a protective earth (ground) wire, and a neutral wire. This is commonly expressed as 3W+N+PE (wye).

Pin Positions

The pin arrays are different for four-wire (delta) and five-wire (wye) 3Ph configurations. See Figure 23 for example delta and wye pin positions.

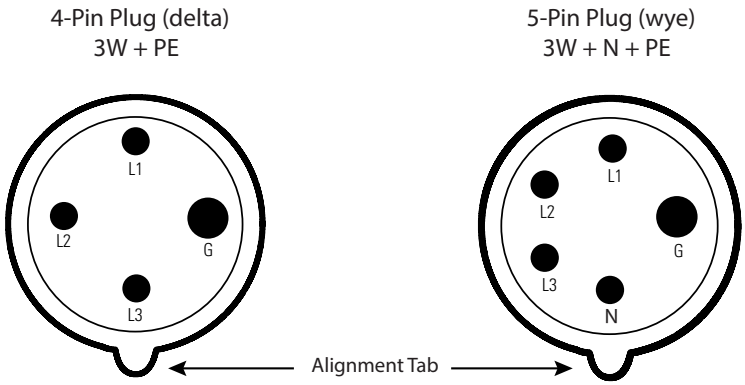


Figure 23. Example 3Ph Pin Positions

Environmental Protection

The input connector plugs have Ingress Protection (IP) ratings that specify the degree of environmental protection for electrical equipment. The IEC 60309 input connector plugs are either splash resistant (S) or waterproof (W).

- Splash resistant plugs are IP-rated at IP 44, which means the plug is protected against solid objects less than 1.0 mm in diameter.
- Waterproof plugs are IP-rated at IP 67, which means the plugs are watertight, splashproof, and dust tight.

Table 3 shows examples and descriptions of delta and wye configuration codes.

Table 3. Example 3Ph Topologies

Code	Pin Positions 4-pin Plug (delta) - 4 5-pin Plug (wye) - 5	Maximum Amperage (A) Rating	Plug (P) outlet/Socket (R) or Connector (C)	Clock Position (6 or 9)	Waterproof (W) or Splash Resistant (S)
460P9W	4	60	P	9	W
532P6S	5	32	P	6	S

Outlets and Circuit Breakers

Each MA PDU model has a specific configuration of outlets. The outlets are grouped in sets called outlet groups. Outlet groups are preset groups of individual outlets that you can identify and monitor through the different interfaces that are available with the MA PDU.

The outlets are labeled, and if the model has circuit breakers, the circuit breakers that are associated with the outlets have corresponding labels.

Menu and Status Display

The LCD provides information in English about the MA PDU and connected devices using white text on a blue background. The LCD window flashes red when any alarm is active. Basic configuration of some settings is available through the LCD. Full configuration of all settings is available through the remote interfaces.

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 51 or see Example 2 in "set command" on page 99 for more information.

LCD Window

The LCD 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.

- **EcoMode** (energy saving mode)

  This mode is activated automatically when no button is pressed for 15 minutes and no alarm is active. The backlight is turned off to conserves energy.The screen darkens.

- **Settings mode** (LCD main menu)

  The settings that display under each high level (main) menu depend on your MA PDU model.

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.

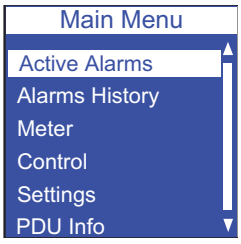


Figure 24. Menu Item Selection

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 25 is an example of the display for a 1Ph PDU.

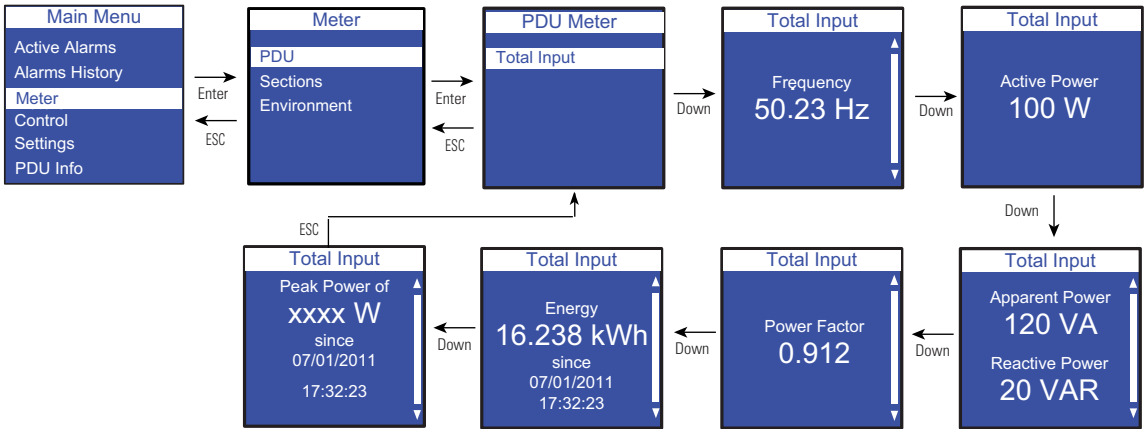


Figure 25. Example of Selected Value Display

Front Panel Ports, Status Indicators, and Operation Buttons

The MA PDU front panel includes communication and environmental monitoring ports, LED status indicators, and operation buttons. There are three different front panel versions. Although the button and port position varies, you can recognize the same button and port design from model to model (see Figure 26).

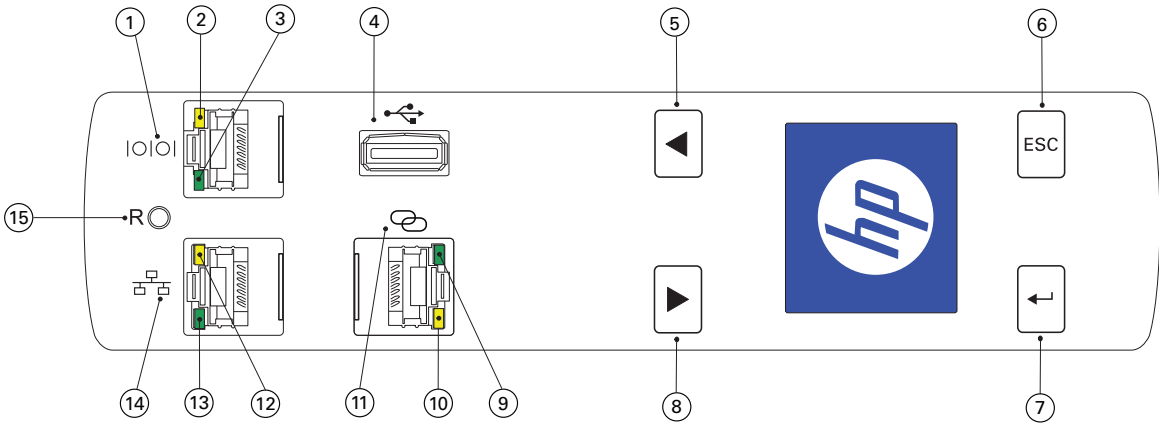


Figure 26. Front Panel Ports and Buttons (22U and 42U Front Panel)

Table 4 describes the ports and buttons identified in Figure 26.

Table 4. Communication and Environmental Monitoring Ports

Reference Number	Description
1	Service or Serial Port (Settings/Sensor)
2	Yellow Serial Service Port LED: RS-232 Operation and Activity Status **OFF**: Normal operation **FLASHING**: Communicating with EMP (if installed)
3	Green Serial Service Port LED: MA PDU Communication Status **OFF**: PDU start-up in progress **FLASHING:** Normal operation (network communication module operational)
4	USB Port: Used for Firmware upgrade
5	Backward (Down) Scroll Button
6	Escape (ESC) Button

Table 4. Communication and Environmental Monitoring Ports

Reference Number	Description
7	Enter Key
8	Forward (Up) Scroll Button
9	Green Daisy Chain Port LED: Role Assignment in Communication Protocol **ON**: Device **FLASHING**: Host
10	Daisy Chain Port Yellow LED: Transmission Activity Status **FLASHING**: PDU is transmitting data
11	Daisy Chain Port (Communication Status of Chained PDU)
12	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)
13	Green Ethernet Port LED: Operation Transfer Rate Status **OFF**: Port operating at 10 Mbits/s **ON**: Port operating at 100 Mbits/s
14	Ethernet 10/100 Base-T Port
15	Reset Button

Common Operations

Starting the MA PDU

For units without circuit breakers, the MA PDU output power cannot be turned on and off with a button or switch. These MA PDUs are always on when they are plugged in. These MA PDUs are always off when they are unplugged.

For units with circuit breakers, 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 eNMC is operational.
- If the circuit breakers are off, there is no output power, but the LCD display is on, and the eNMC is operational.
- To turn off the MA PDU completely, unplug it.

To start up the MA PDU:

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

NOTE 2 Do not replace or rewire the power cord.

1. **For MA PDUs with detachable power cords.** If the power cord is not connected, connect the power cord to the MA PDU. Then, connect the power cord to a power source. Otherwise, go to Step 2.
2. Does your MA PDU have a circuit breaker?
   - **For MA PDUs with circuit breakers.** Verify all circuit breakers are in the On position.

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

   - **For MA PDUs without circuit breakers.** Plug in the power cord.

Shutting Down the MA PDU

IMPORTANT

On models rated over 16A (Europe) / 20A (US), fully shrouded branch circuit breakers prevent accidental operation. To power cycle the HP MA PDU, unplug the power cord from the power source and then plug in the power cord.

To shut down the MA PDU:

1. Shut down the connected devices according to the manufacturer's recommended shutdown sequence.
2. Does your MA PDU have a circuit breaker?
   - **For MA PDUs with circuit breakers.** Turn each circuit breaker to the Off position.

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

NOTE 2 To remove power from the MA PDU completely, disconnect the MA PDU power cord from the power source.

   - **For MA PDUs without circuit breakers.** Unplug the power cord.

Restarting the eNMC Module

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

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

For a hardware restart, locate the Reset button (labeled R) on the MA PDU (see Figure 27). Insert an electrically non-conductive probe, press the recessed button, and retract the probe. This method is not necessarily the best choice because the eNMC module does not force the system to save the parameters in the file system before restarting.

IMPORTANT

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

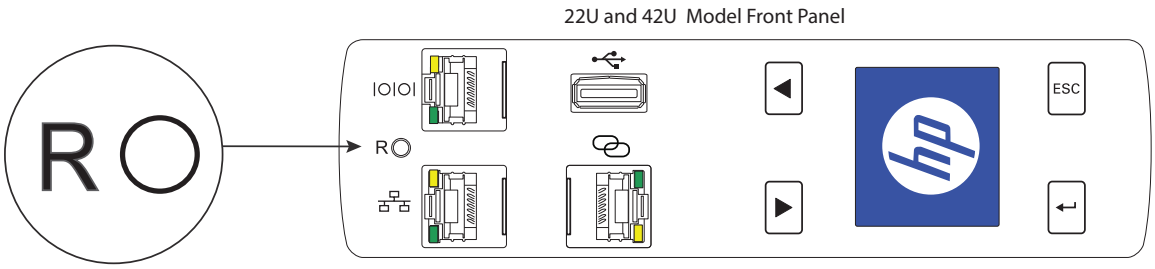


Figure 27. Reset Button

Chapter 6 LCD Interface Operation

This chapter contains operation information for the HP Managed PDUs, including:

- LCD display and control button functions
- Menu selections

NOTE The LCD language is configurable. See language settings in "Language Submenu" on page 55.

LCD Display and Control Buttons

The MA PDU has a four-button, graphical LCD display (see Figure 28). 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.

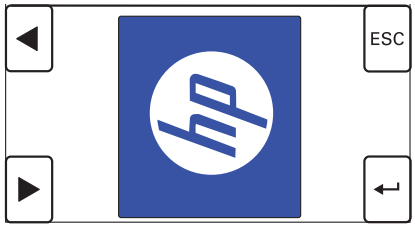


Figure 28. LCD Display

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
ESC	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 29) or 3Ph cycle (Figure 30). These cycles are not user-configurable.

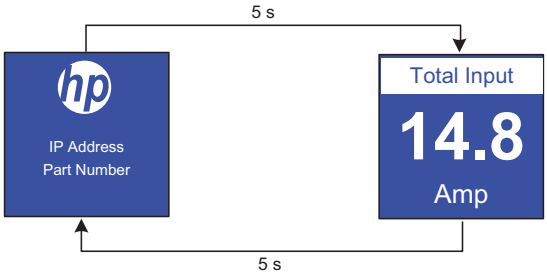


Figure 29. 1Ph Screensaver Cycle

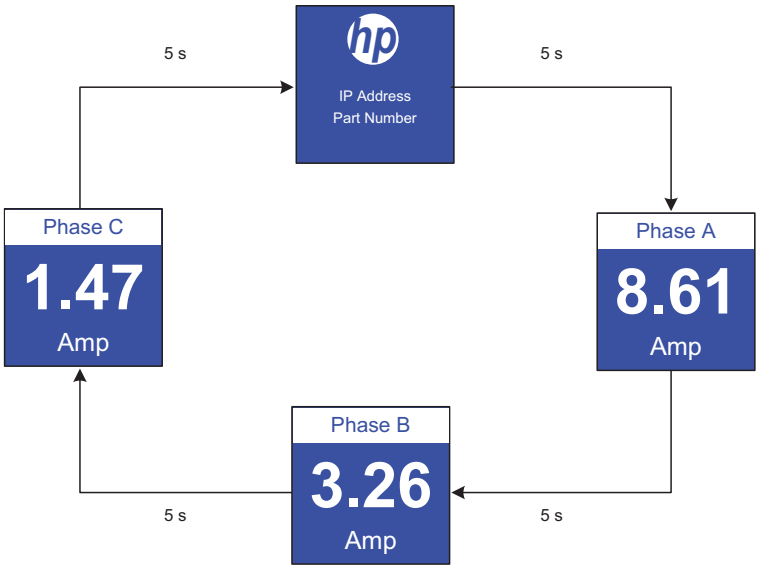


Figure 30. 3Ph Delta-configured Screensaver Cycle

Startup Screen

When the MA PDU powers up, the Startup screen displays (see Figure 31). Press **ENTER** to go to the Main Menu.

Figure 31. 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.

IMPORTANT

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

On the Main Menu, scroll up or down to highlight Control. Press **ENTER** to display the Enter Password screen. Scroll up or down in the number selection boxes to create a four-number password code. When you finish your entry, click **OK**. Press **ENTER** to return to the previous menu. A lock icon displays on the menu option you password protected.

Figure 32 illustrates the sequence to enter a password for a locked menu.

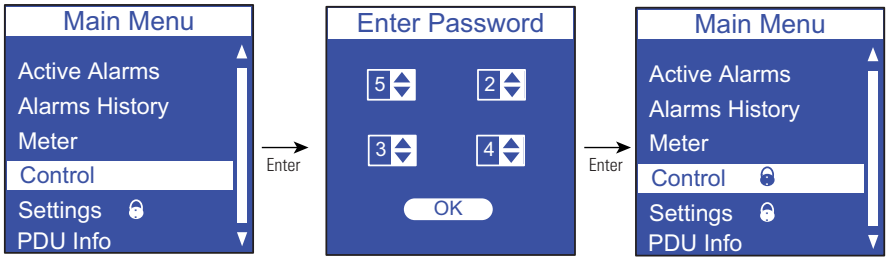


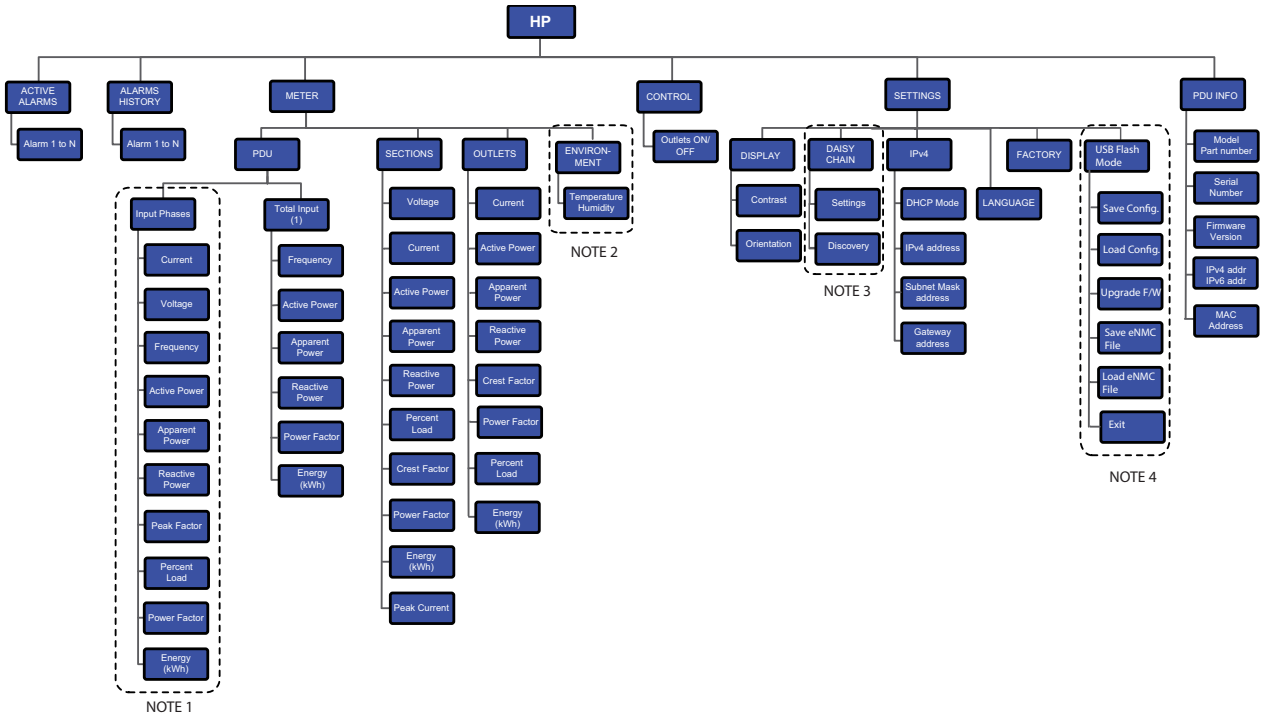
Figure 32. Password Protected Screens

Main Menu Selections

The MA PDU menu selection hierarchy provides useful performance information, alarms, MA PDU identification, and configuration settings (see Figure 33). The available menu items are illustrated in a menu hierarchy in Figure 34.

- 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 33. Main Menu Selections



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

NOTE 2 This menu and submenu are only available if an EMP is connected.

NOTE 3 This submenu is available, but can only be used for configuration Settings and Discovery when two or more MA PDUs are daisy-chained.

NOTE 4 This submenu is only available if a USB drive is detected.

Figure 34. 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 MA PDU topologies.

Table 6. Menus Available for PDU Topologies

Models	Active Alarms	Alarm History	Meter see NOTE 1							
			MA PDU							
			Input Phase	Total Input (1)	Total Input (2)	Sections	Outlets	Control	Settings	PDU Info
Managed (MA)	•	•	see NOTE 2	•	—	•	•	•	•	•

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 MA PDU has multiple phases.

Active Alarms Menu

The Active Alarms menu filters and displays only active alarms for the MA 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 35). 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.

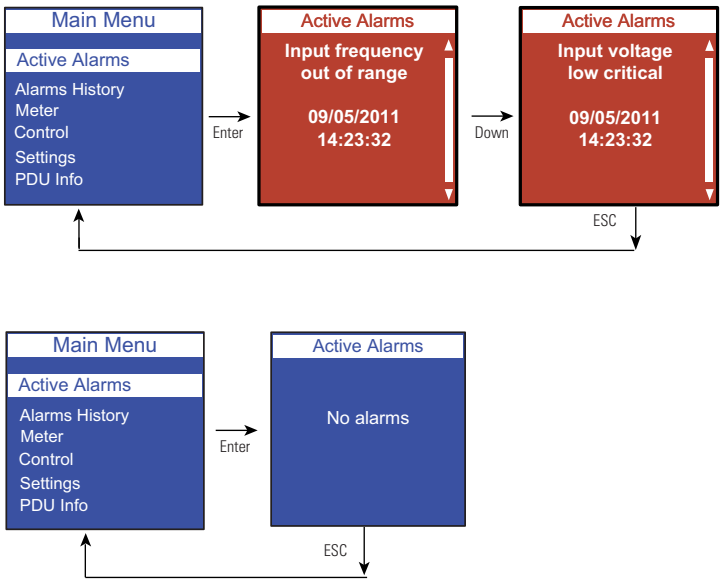


Figure 35. Example Active Alarm Displays

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 36).

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.

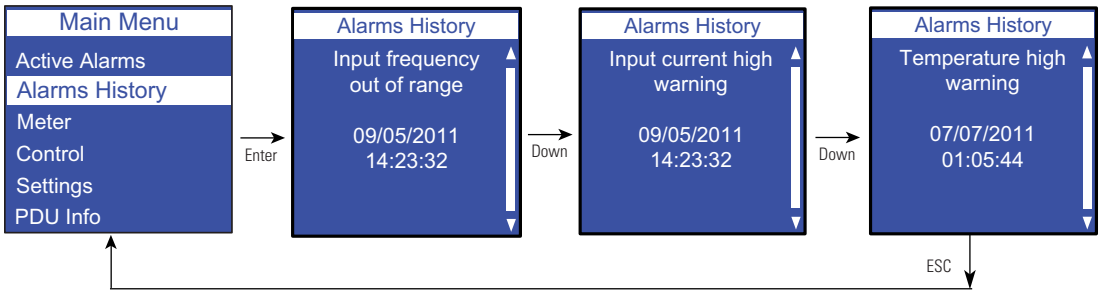


Figure 36. Example Alarm History Displays

Meter Menu

The Meter menu provides measurement data for the following submenus:

- PDU
- Sections (not available for sections that do not have current measurement)
- 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.

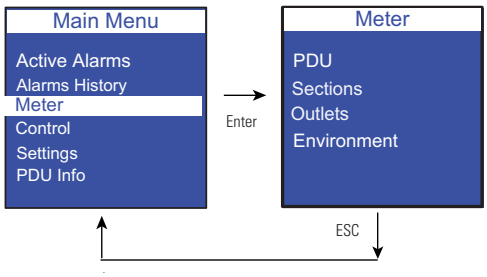


Figure 37. Example Meter Menu Display

NOTE The measurement data for each screen is refreshed every three to four seconds.

PDU Submenu

These screens display Total Input data measurements for MA PDUs. In addition to Total Input measurements, you can view Phase Input data measurements for 3Ph, split-phase, and dual input MA PDUs. Depending on the MA PDU electrical topology, different MA 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 or 3Ph 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 A, B, or C to see Phase Input measurements. Press **ESC** to return to the previous menu.

For example, Figure 38 shows a total input display for 1Ph MA PDUs.

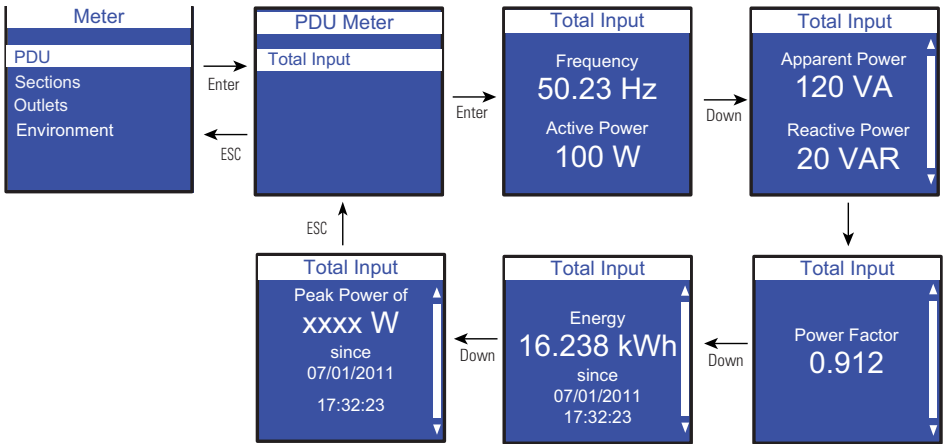


Figure 38. Example 1Ph Total Input Display

NOTE The **Total Input > Input Meter** selection screens will be different for 1Ph and 3Ph MA PDUs.

Figure 39 shows an input phase display for wye-wired 3Ph MA PDUs.

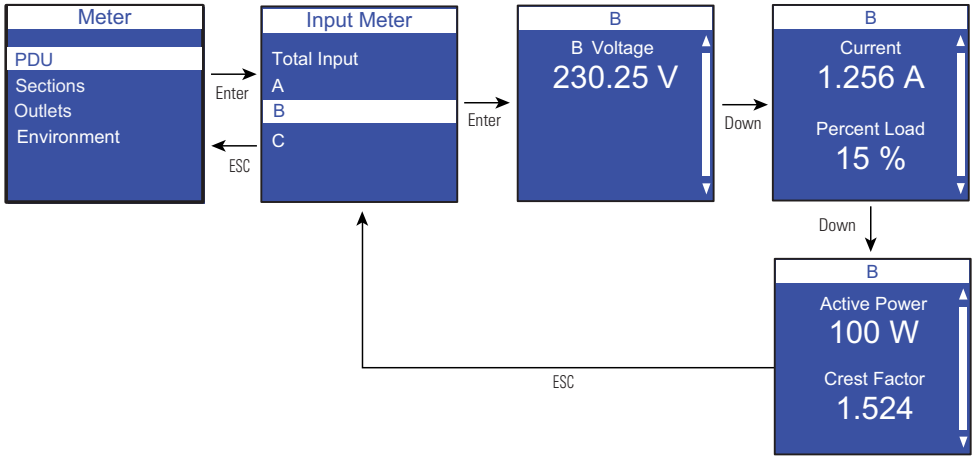


Figure 39. Example 3Ph Input Phase (wye-wired) Display

Sections Submenu

Section measurements include voltage data for all MA PDU sections. Other sections measurements are only available on MA PDUs that have current measurement capabilities (see Figure 40).

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.

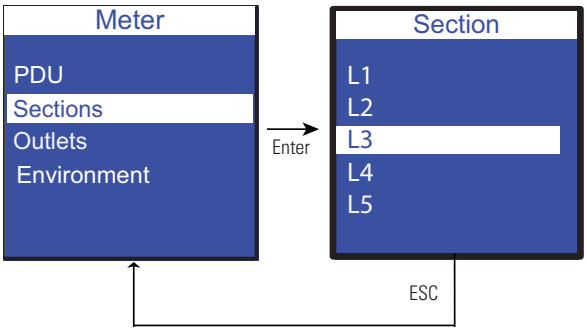


Figure 40. Example Section Submenu Display

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 41).

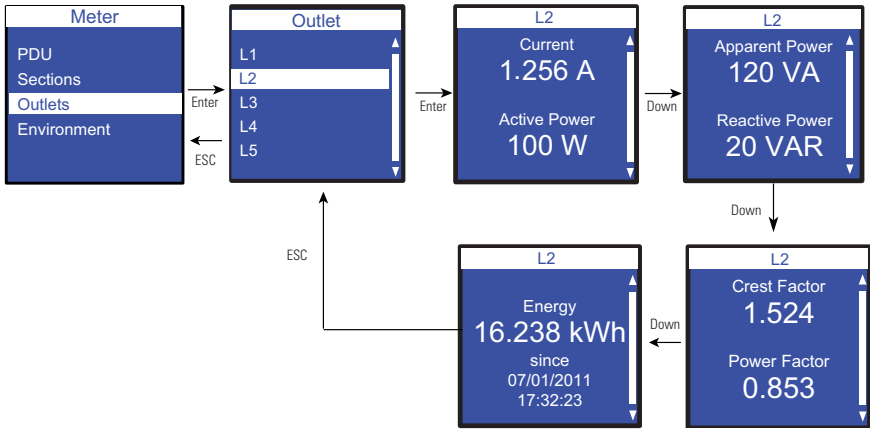


Figure 41. Example Outlets Submenu Display

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.)

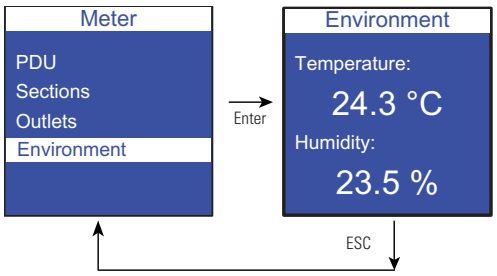


Figure 42. Example Environment Submenu Display

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 43).

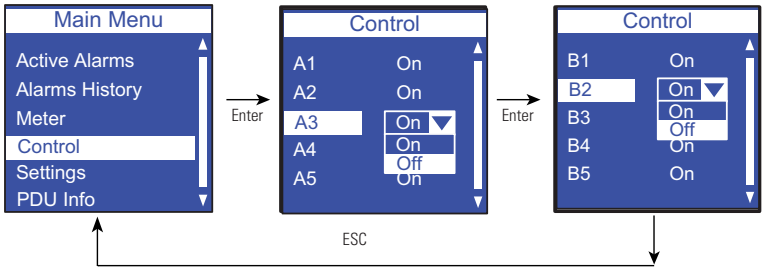


Figure 43. Example Control Submenu Display

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.

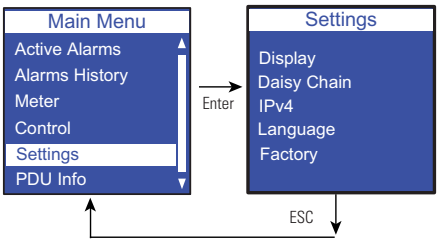


Figure 44. Example Settings Menu Display

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.

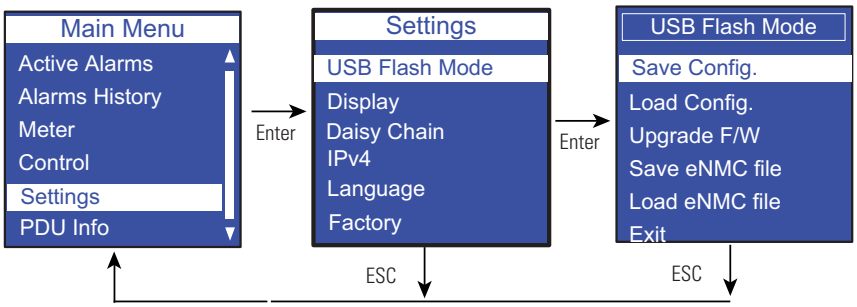


Figure 45. Example Settings USB Flash Mode Menu Display

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 MA PDUs of the same model and hardware configuration, you can copy the customized setting files from one MA PDU and upload the files to the rest of the MA 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 MA PDU when replicating configurations regardless of part number.
- eNMC/config/ConfigurationPdu.xml - Contains all the user-configurable settings related to the MA 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 PNx to PNy (part number x to part number y).

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

1. Make sure the 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.
7. Click **OK** to continue when a successful pop-up message displays the following:
   - 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.
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.

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

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

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

2. Make sure the 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.
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

See "Replace the MA PDU eNMC Module" on page 121 to understand this selection in proper context. This procedure is used as part of the eNMC module replacement procedure. Each eNMC module has a hardware configuration file that can only be used on the specified MA PDU model. This procedure allows you to copy the PDU hardware configuration file from a working eNMC module 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 MA 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 MA PDU.

IMPORTANT

This MA PDU must be of the same model type and configuration as the MA 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 MA PDU hardware configuration file to the USB drive. The file will save to the eNMC/config/hw path at the USB drive root directory.

NOTE 1 The eNMC/upgrade/hw directory contains only one file named epdu_cfg_HPModelNumber_HP AssemblyNumber_vx_x.xml. For example, the HP file name for model H8B48A would be: epdu_cfg_H8B48A_767160-001_vx_x.xml (where x_x is a file revision).

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

5. See Table 8 and confirm the name of the file correctly matches your model.

Table 8. Configuration File Names

Model	MA PDU Model Configuration File Names	Description
H8B48A	epdu_cfg_H8B48A_767160-001_vx_x.xml	HP 2.8kVA 120V 30A NA/JP maPDU
H8B49A	epdu_cfg_H8B49A_767160-002_vx_x.xml	HP 3.6kVA 100-240V 16A WW maPDU
H8B50A	epdu_cfg_H8B50A_767160-003_vx_x.xml	HP 4.9kVA 208V 30A NA/JP maPDU
H8B51A	epdu_cfg_H8B51A_767160-004_vx_x.xml	HP 7.3kVA 200-240V 32A INTL maPDU
H8B52A	epdu_cfg_H8B52A_767160-005_vx_x.xml	HP 8.6kVA 208V 30A 3Ph NA/JP maPDU
H8B53A	epdu_cfg_H8B53A_767160-006_vx_x.xml	HP 8.6kVA 208V 30A 3Ph DV NA/JP maPDU
H8B54A	epdu_cfg_H8B54A_767160-007_vx_x.xml	HP 11kVA 400V 16A 3Ph INTL maPDU
H8B55A	epdu_cfg_H8B55A_767160-008_vx_x.xml	HP 14.4kVA 208V 50A 3Ph NA/JP maPDU
H8B56A	epdu_cfg_H8B56A_767160-009_vx_x.xml	HP 17.3kVA 208V 60A 3Ph NA/JP maPDU

NOTE The version of the file is represented by vx_x, where x_x = number of the version. For example, a version 2.0 file would be represented as, "epdu_cfg_H8B48A_767160-001_**v2_0**.xml" in the file name.

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

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

See "Replace the MA PDU eNMC Module" on page 121 to understand this selection in proper context.This procedure is used as part of the replacement procedure.

The MA PDU hardware configuration file provides the replacement eNMC module with the characteristics of the MA 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 MA PDU hardware configuration file is detected on the USB drive.

To load the MA 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 MA 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 MA PDU hardware configuration file to the eNMC module.
5. When the file is successfully loaded, click **OK** to confirm.
6. Remove the USB flash drive and select **Exit**.

Upgrade the Firmware using USB

To upgrade the eNMC module firmware:

1. Obtain the hardware configuration file in one of the following ways:
   - Copy the hardware configuration file from another working MA PDU (must be the same model type and configuration).
   - Go to http://www.hp.com/go/rackandpower. Download the firmware upgrade package from the HP Web site and use the attached configuration files for your model.
2. Save the MA PDU model-specific hardware configuration file to your computer. See Table 8 on page 50.

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.

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 module 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. The eNMC module gets the file from the USB drive.
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 the eNMC module is restarted. This can take several minutes.

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 46).

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.

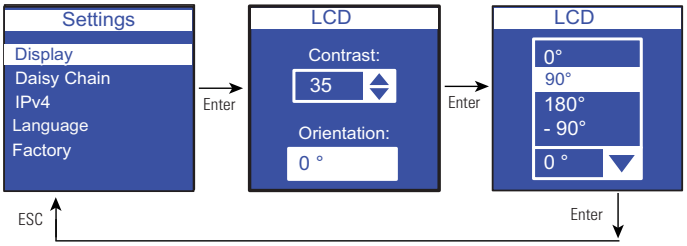


Figure 46. Example Display Submenu Displays

Daisy Chain Submenu

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

IMPORTANT

All daisy-chained PDUs should be MA PDUs. Daisy-chaining MA PDUs with any other type of PDU will generate an error.

NOTE 1 To configure and monitor the MA PDUs, they must be connected together through the Daisy Chain connector on the front panel using an Ethernet cable.

NOTE 2 The Host MA PDU must be connected to the network. There can only be one Host.

Use the Settings option for the first two configuration steps:

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

Daisy Chain Settings Options

The Daisy Chain Settings option allows you to specify the MA PDU that will be the Host (the MA PDU that has the network connection) and the MA PDU (or MA PDUs) that will be connected to it as Devices.

From the **Device MA PDU** (or MA PDUs), set the values as follows (see Figure 47):

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),** or **3 (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 the PDU is adjacent to only one other PDU.

NOTE 2 Select **Middle** when the PDU is located between two other PDUs.

NOTE 3 Always select **End** when assigning the last device in the chain when daisy-chaining three or four MA PDUs.

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

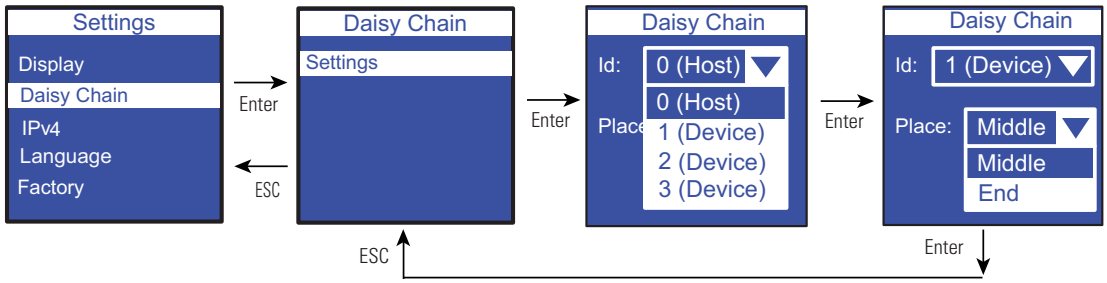


Figure 47. Example Daisy Chain Device MA PDU Setup

From the **Host MA PDU**, set the values as follows (see Figure 48):

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** from the Place: selection drop-list. Press **ENTER**.
5. Press **ESC** to return to the previous menu.

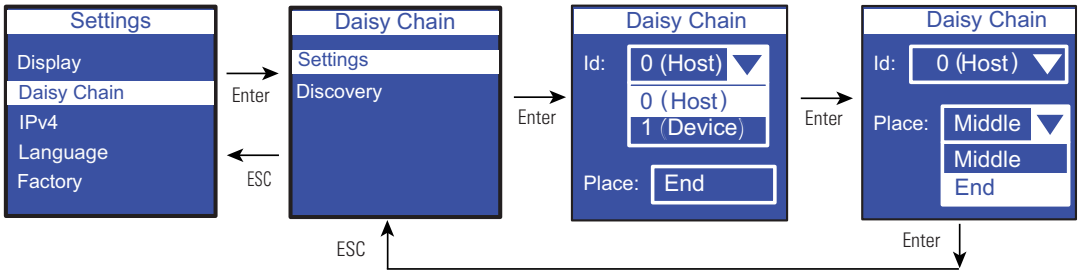


Figure 48. Example Daisy Chain Host MA PDU Setup

Daisy Chain Discovery Options

The Discovery option starts communication between the Host MA PDU and the Device MA PDU (or PDUs). This is only available for the Host MA PDU. The display you see varies depending on whether the MA PDU is communicating properly or not communicating (see Figure 49 and Figure 50).

From the Host MA 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 MA 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 MA 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 (or devices). Once corrected, select the Discovery option again.

4. Press **ENTER** to validate the Discovery.
5. Press **ESC** to return to the previous menu.

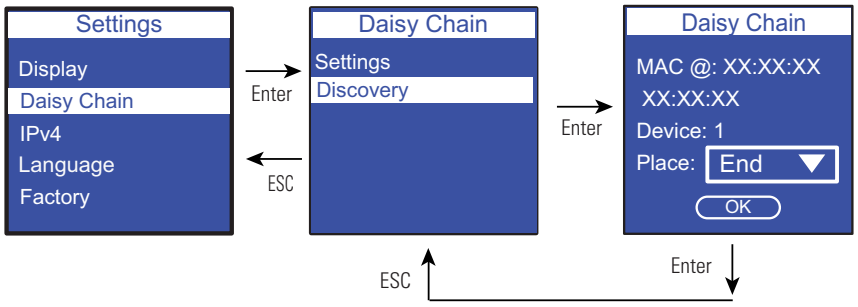


Figure 49. Example Daisy Chain MA PDU Discovery (Communicating)

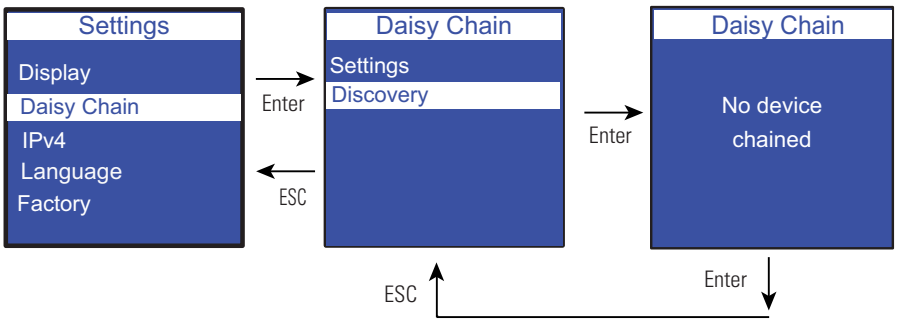


Figure 50. Example Daisy Chain MA PDU Discovery (Not Communicating)

IPv4 Submenu

The IPv4 submenu allows you to set options for:

- DHCP
- IP address
- Subnet Mask
- Gateway

Figure 51 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.

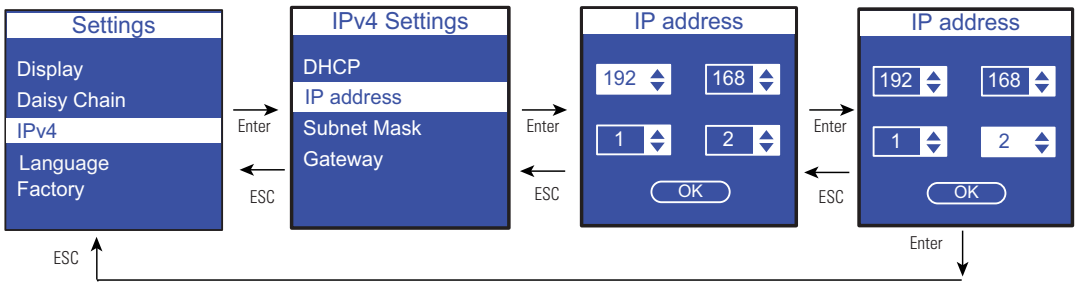


Figure 51. Example IPv4 Submenu Displays

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 52).

NOTE Available languages include English, French, German, Spanish, Portuguese, and Italian. (Russian is not currently available.)

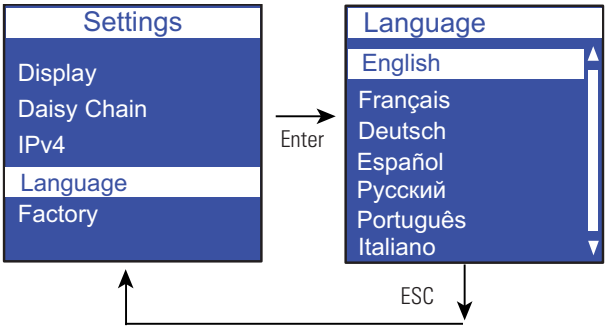


Figure 52. Example Language Setting

Factory Submenu

The Factory submenu allows you to reset the MA PDU to the factory settings (see Figure 53).

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.

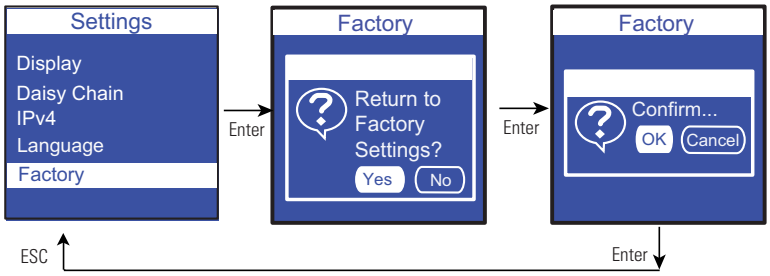


Figure 53. Example Factory Submenu Displays

MA PDU Info Menu

The MA PDU Info menu provides identification information for this MA PDU. The identification information includes the MA PDU model type and part number, serial number, eNMC firmware version number, IP address, and eNMC MAC (Media Access Control) address. These are information-only screens (see Figure 54).

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

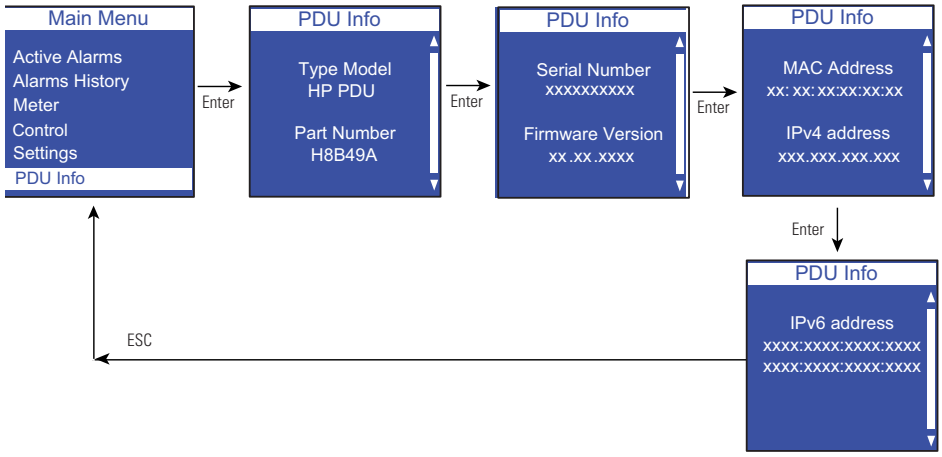


Figure 54. Example MA PDU Info Display

Chapter 7 Web Interface Operation

This chapter describes remotely configuring, managing, and monitoring an HP Managed PDU remotely through the eNMC module Web interface. This chapter describes the following:

- Navigating the Web interface
- Accessing the Web interface
- Configuring settings and monitoring the MA 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.

Navigate the Web Interface

The graphical Web interface is used to remotely monitor or configure the MA PDU (see Figure 55). The Web interface that corresponds to the MA PDU topology type displays. This section describes the functions provided by this interface.

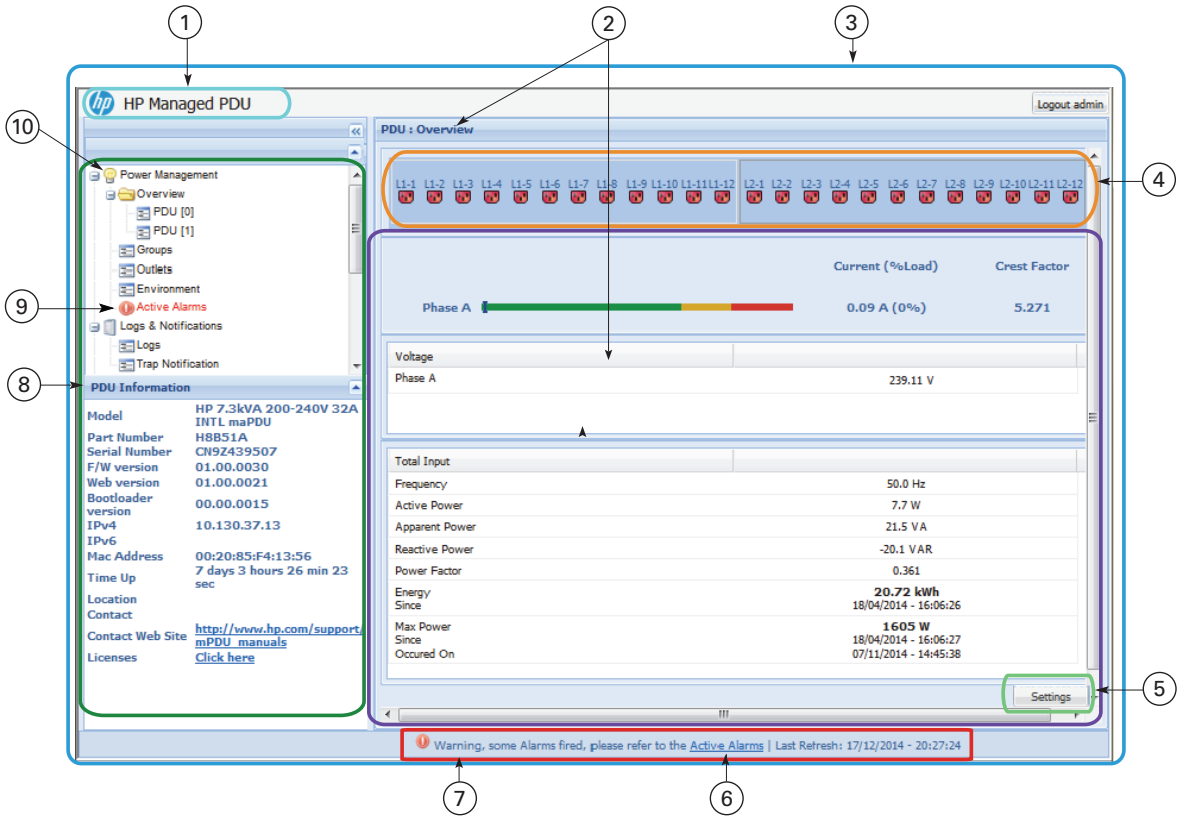


Figure 55. Navigating the Web Interface (Opening Page)

Table 9 provides descriptions of the Web interface components.

Table 9. Web Interface Region Descriptions

Area	Description
1 - Application Header Bar	The header bar identifies which 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.) The borders around the outlet groups emulate the colors that are printed on the PDU. **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 9. Web Interface Region Descriptions (Continued)

Area	Description
8 - MA PDU Information	This panel displays identification information for the MA PDU that is providing data. The data fields include information about the MA PDU, including a model description, part number, serial number and the current MA PDU firmware version in use. **NOTE** For daisy-chained PDUs, you can select either PDU [0] for Host data and PDU [1], [2], or [3] for Device data. This displays data for the selected PDU.
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 MA 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 MA 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 MA PDU model you are using, or models if you daisy-chain PDUs.

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
- Russian (currently unavailable)
- Polish
- Portuguese
- Czech

Access the Web Interface

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

NOTE The MA PDU defaults to using DHCP when delivered. If you are unable to connect to the MA PDU through the network connection with this default address, see "Network Communication Configuration" on page 28 for more information.

To access the Web interface:

1. Open the Web browser.
2. Enter a new MA PDU IP address or select the previously entered MA 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 56). Click **Login** to continue or **Cancel** to exit.

NOTE The default user name is "admin" and the default password is "admin."

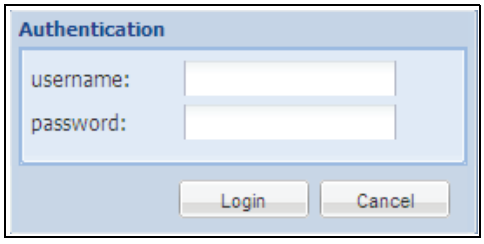


Figure 56. Login Authentication

4. The MA 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] See NOTE 1
    - PDU [2] See NOTE 1
    - PDU [3] See NOTE 1
  - Groups
  - Outlets
  - Environment
  - Active Alarms
- Logs and Notifications
  - Logs
  - Trap Notification
  - Syslog (Super User and Administrator only)
- Settings See NOTE 2
  - Access Accounts
  - System

  - Date & Time
- Network (Super User and Administrator only)
  - TCP/IP
  - SNMP
  - Energy/Wise
  - Security
    - Global
    - LDAP
    - RADIUS

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

Your access privileges determine what menu selections you can see. See "Access Privileges" on page 62 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 MA PDU Overview page. This page provides the present readings for the MA PDU that is reporting data. (If MA PDUs are daisy-chained, you can select to see Host or Device MA PDU Information.) The readings are reported per phase and, for 3Ph MA 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.

You can select the Outlets or Groups page to manage outlets or groups of outlets. These Settings pages provide 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 121 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 MA PDU-users, and remote MA PDU-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 MA PDU or 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 NTP (Network Time Protocol) server. You can set the time zone and have the option of allowing DST (Daylight Savings Time).

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 HP MA PDU MIB (Management Information Base) 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 LDAP (Lightweight Directory Access Protocol) 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 76).

User roles can be assigned these access privilege levels:

- SuperUser Administrator
- Local or Remote Administrators
- PDU-User

SuperUser 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 MA 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 and password is "admin" and 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.

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
- 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 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.

Local or Remote 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.

Read-Only Access

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

- Access to up-to-date MA 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 LDAPsettings
- 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.

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.
- 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 SSL (Secure Sockets Layer) or SSH (Secure Shell) sockets are allowed.
  - Only two secure sessions can be running at the same time.
  - Only an administrator can have two simultaneous sessions open in HTTP/HTTPS (Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure), 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 the PDU Data

NOTE Menu selections for PDU [0], [1], [2], or [3] only display if the MA PDUs are configured in a daisy-chained configuration. If provided, selecting either PDU [0] or PDU [1], [2], or [3] displays the Overview page for the specified MA 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 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 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 located in the lower, right-hand corner of the Web interface screen. The Settings dialog displays.
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**.

Groups

NOTE In the toolbar, **Turn On/Off Groups** will only appear for PDUs with outlets that can be controlled.

Review/Modify the PDU Groups

1. Access the Web interface and log in.
2. Under Power Management, select Groups. The Groups page displays.
3. Review basic monitoring information for Groups measurement settings.

NOTE Click the red arrow next between the Current (%Load) and the voltage columns to see additional Section outlet information.

4. **For users with Read Write access.** To apply an operative action to all outlets in a selected group, select the corresponding checkbox and select one of the following values from the Turn On/Off Groups drop-down list in the top bar, then click **Save**.
   - **On**: Turn on the selected group of outlets.
   - **Off**: Turn off the selected group of outlets.
   - **Reboot**: Reboot the selected group of outlets.
5. To modify PDU threshold values for a specified group, click the link on the group friendly name. The Group Settings dialog displays.
6. **Administrator or User with Read/Write privileges only.** To specify the duration outlets in this group will be Off before switching On during a reboot, type the number of seconds the outlets should be Off in the Power Reboot Period text box. Click **Save**.

NOTE This setting overwrites the Power Reboot Period defined for individual outlets on the Outlet Settings dialog.

7. 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
8. To reset the threshold values to the default values, click **Default**, then click **Save**.
9. To reset a kilowatt hour (kWh) counter to zero, click **Reset kWh**, then click **Save**.
10. To reset the maximum current counter to zero, click **Reset Max Current**, then click **Save**.

Outlets

Review/Modify the PDU Outlets

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 select one of the following values from the Turn On/Off Groups drop-down list in the top bar, then click **Save**.
   - **On**: Turn on the outlet.
   - **Off**: Turn off the outlet.
   - **Reboot**: Reboot the outlet.
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**.

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 67). 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 your 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**.

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 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 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 77.

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 80).

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 an Admin or PDU 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 CSV File From the Web Interface

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.

Download the Japanese-specific Event Log as a CSV File From the PDU to Excel

1. Start Excel.
2. On the Data tab, select Get External Data, then select From Text (see Figure 57).

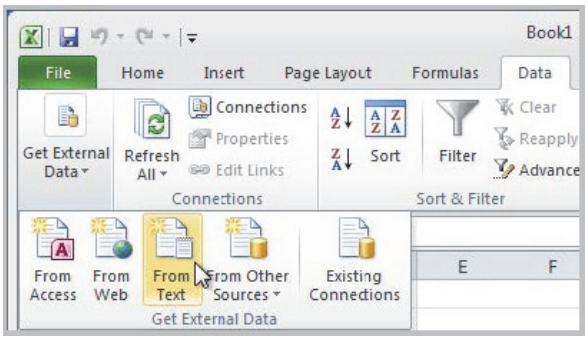


Figure 57. Excel Data Tab Selections

3. Browse and select the appropriate file with *.csv selected.
4. Click **Import**. The Text Import wizard starts.
   a. Ensure that the Delimited option is selected.
   b. In File origin, select 65001. In Unicode, select UTF-8. Click **Next**.
   c. In the Delimiters section, select Comma. Click **Next**.
   d. Click **Finish**.
5. Select the destination for importing your data and click **OK**.
6. Observe that the data appears in the spreadsheet with correct Japanese and English text (see Figure 58).

	A	B	C	D	E	F
120	533DA0E1	03/04/2014	17:56:49	0	301600	User logged in HTTP (admin)
121	533DA359	03/04/2014	18:07:21	0	301600	ユーザーログイン： HTTP (admin)
122	533DA43F	03/04/2014	18:11:11	0	301700	ユーザーログアウト： HTTP (admin)
123	533DA446	03/04/2014	18:11:18	0	301600	ユーザーログイン： HTTP (admin)
124	533DAAA1	03/04/2014	18:38:25	0	301600	User logged in HTTP (admin)

Figure 58. Japanese-specific CSV Event Log File

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 83.)
   - **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 83.)
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 83).

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 eNMC module is running in Normal Operation mode.
- The eNMC module is connected to the Local Area Network (LAN).
- The 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 83.

Syslog

Retrieve/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:
   - the port number and the protocol selection to either UDP or TCP from the Protocol drop-down list
   - the message transfer method according to:
     - 5424: Syslog Protocol IETF
     - 5425: TLS
     - 5426: Transfer over UDP
     - 6587: Transfer over TCP
     - 3167: Syslog protocol IETF (obsolete)
   - the facility code used for all messages from 1 to 23
   - the 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.
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 MA 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:
    - Check the LCD Password check box 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 87).

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 59).

Figure 59. 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 PDU 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 Card Data

1. Access the Web interface and log in.
2. Under Settings, select System. The System Settings page displays.
3. In the PDU 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.
   ```

Configure the PDU

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

Date & Time

Manual Configuration of 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.

Automatic Configuration of 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. If desired, check the Daylight Saving Time option.
9. Click **Save**.

NOTE The 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 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 MA PDU host name (used for DNS resolution).
     - Type the MA 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 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 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, click 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, click 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 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

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 eNMC module.

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

NOTE 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. xxx.xxx.xxx.xxx`

Enable/Disable the Telnet Interface

NOTE Selecting a console type on the Security page makes the corresponding port entry box active.
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 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 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, check the **FTP Enable** check box to enable FTP, or uncheck the box to disable it.
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 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 set 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**.

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:** LDAP attribute of the user object which is used to store the 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 10 provides authentication error messages and descriptions of possible causes.

Table 10. 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	1. Bad value in the Password field of the Search User. 2. 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 MA PDU remote group defined in the Remote Group Access MA 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 MA 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 MA PDU.

This attribute must be added in the RADIUS server configuration and must be sent for each remote user allowed to access to the MA 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 8 Serial Interface Operation

This section describes the CLI (Command Line Interface) commands used to remotely configure and monitor the HP Managed PDU through the serial interface connection or network connection between the HP HP MA (Managed) PDU (Power Distribution Unit) and a laptop or workstation.

Access to a CLI is provided through a terminal emulation program, such as HyperTerminal, Telnet, or SSH.

For example, open a saved HyperTerminal connection as follows:

1. Select **Start > All Programs > Accessories > Communications > HyperTerminal > *saved connection name*.ht**.
2. On the New Connection dialog, select **File > Open**. The Open dialog displays. In the File Name window, select the saved connection file you intend to use. Click **Open**.
3. The HyperTerminal session window opens for the connection you selected. Press any key to display the banner. To open an authentication session, type your user name to log in.

NOTE See "Network Communication Configuration" on page 28 for more information creating a serial connection and configuring the network.

Supported Commands

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

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

NOTE Commands are case-sensitive. Parameters and attributes are not. 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.

NOTE You must be logged into the MA 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 for objects.

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

Name                                Unit   RO/RW  Type
System.Network.DHCP                 RW            0: Disabled
                                                  1: Enabled
```

Example 2

```
pdu#0>info PDU.*

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

Example 3

```
pdu#0>info System.*

Name                                                Unit   RO/RW  Type
System.NetworkManagementSystem.Count                       RO     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.*
```

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

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

Example 2

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

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 separate 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 Degree (0U)
<1> = Rotation 90 Degree (1U)
<2> = Rotation 180 Degree (0U)
<3> = Rotation 270 Degree (1U)

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>
```

pdu command

Use this command to access different PDUs on the daisy chain.

Usage

```
PDU#0>pdu <value>
```

where:

<value> = 0 for the host; 1, 2, or 3 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

This section includes tables that define PDU CLI objects (Table 11) and System CLI Objects (Table 12 on page 111).

Table 11. PDU CLI Objects

XML Object Name	Type	Description	Unit	Access
Environment.ChangedStatus.CommunicationLost	Timestamp	Timestamp of last changing state of the alarm that has the same name in the collection PresentStatus.	s	RO
Environment.ChangedStatus.OverHumidity	Timestamp	Timestamp of last changing state of the alarm that has the same name in the collection PresentStatus.	s	RO
Environment.ChangedStatus.OverTemperature	Timestamp	Timestamp of last changing state of the alarm that has the same name in the collection PresentStatus.	s	RO
Environment.Humidity	Measure	Measured Humidity on environmental monitoring probe. 0 when no probe is connected or when the probe does not have a humidity sensor.	d%	RO
Environment.Input[1].ChangedStatus.Alarm	Timestamp	Timestamp of last changing state of the alarm that has the same name in the collection PresentStatus.	s	RO
Environment.Input[1].iName	String[31]	Contact 1 friendly name	-	RW
Environment.Input[1].PresentStatus.Alarm	AlarmL1	Dry Contact alarm. Set according to the dry contact State and the parameter State[0] or [1].Level 0: Alarm not active 1: Alarm active Ex: State=0 AND State[0].Level=3 then Alarm=1	-	RO
Environment.Input[1].PresentStatus.State	Measure	Dry Contact state 0: Open 1: Close	-	RO
Environment.Input[1].State[0].Level	Parameter	Dry contact Config 1: Open makes just informational 0 into State. 2: Open makes Warning trap 3: Open makes Alarm trap	-	RW
Environment.Input[1].State[1].Level	Parameter	Dry contact Config 1: Close makes just informational 0 into State. 2: Close makes Warning trap 3: Close makes Alarm trap	-	RW
Environment.Input[2].ChangedStatus.Alarm	Timestamp	Timestamp of last changing state of the alarm that has the same name in the collection PresentStatus.	s	RO
Environment.Input[2].iName	String[31]	Contact 2 friendly name	-	RW
Environment.Input[2].PresentStatus.Alarm	AlarmL1	Dry Contact alarm. Set according to the dry contact State and the parameter State[0] or [1].Level 0: Alarm not active 1: Alarm active Ex: State=0 AND State[0].Level=3 then Alarm=1	-	RO
Environment.Input[2].PresentStatus.State	Measure	Dry Contact state 0: Open 1: Close	-	RO

Table 11. PDU CLI Objects (Continued)

XML Object Name	Type	Description	Unit	Access
Environment.Input[2].State[0].Level	Parameter	Dry contact Config 1: Open makes just informational 0 into State. 2: Open makes Warning trap. 3: Open makes Alarm trap.	-	RW
Environment.Input[2].State[1].Level	Parameter	Dry contact Config 1: Close makes just informational 0 into State. 2: Close makes Warning trap. 3: Close makes Alarm trap.	-	RW
Environment.OverHumidity[1].Threshold	Parameter		d%	RW
Environment.OverHumidity[2].Threshold	Parameter		d%	RW
Environment.OverHumidity[3].Threshold	Parameter		d%	RW
Environment.OverHumidity[4].Threshold	Parameter		d%	RW
Environment.OverTemperature[1].Threshold	Parameter		d°K	RW
Environment.OverTemperature[2].Threshold	Parameter		d°K	RW
Environment.OverTemperature[3].Threshold	Parameter		d°K	RW
Environment.OverTemperature[4].Threshold	Parameter		d°K	RW
Environment.PresentStatus.CommunicationLost	AlarmL1	0: OK 1: Communication failure with the sensor probe or probe not present.	-	RO
Environment.PresentStatus.OverHumidity	AlarmL1	0: No threshold triggered 1: Warning low threshold triggered 2: Critical low threshold triggered 3: Warning high threshold triggered 4: Critical high threshold triggered	-	RO
Environment.PresentStatus.OverTemperature	AlarmL1	0: No threshold triggered 1: Warning low threshold triggered 2: Critical low threshold triggered 3: Warning high threshold triggered 4: Critical high threshold triggered	-	RO
Environment.PresentStatus.Present	Measure	0: Probe not connected 1: Probe connected	-	RO
Environment.Temperature	Measure	Measured Temperature on environmental monitoring probe. It is 0 when no probe is connected.	d°K	RO
PDU.DaisyChain[x].ChangedStatus.CommunicationLost	Timestamp	Timestamp of the last changing state of the alarm with the same name in the collection PresentStatus.	s	RO
PDU.DaisyChain[x].iName	String[15]	Daisy-chain friendly name.	-	RO
PDU.DaisyChain[x].PresentStatus.CommunicationLost	AlarmL1	0: OK 1: Communication with daisy chained device has failed.	-	RO
PDU.Gang.Count	Constant	Number of factory groups in the PDU.	-	RO
PDU.Gang[x].ActivePower	Measure	Active Power provided by the breaker/section. For a double pole breaker, the apparent power for the two poles is combined.	dW	RO

Table 11. PDU CLI Objects (Continued)

XML Object Name	Type	Description	Unit	Access
PDU.Gang[x].ApparentPower	Measure	Apparent Power provided by the breaker/section. For a double pole breaker, the apparent power for the two poles is combined.	dVA	RO
PDU.Gang[x].ChangedStatus.OverCurrent	Timestamp		s	RO
PDU.Gang[x].ChangedStatus.OverVoltage	Timestamp		s	RO
PDU.Gang[x].ConfigCurrent	Constant	Nominal Amps: 10A, 16A, 20A, .. This is useful for both breaker and outlet section.	mA	RO
PDU.Gang[x].Current	Measure	Current provided by the breaker/section. For a double pole breaker, it is calculated as the max of the two poles current.	mA	RO
PDU.Gang[x].GangID	Constant	Breaker ID = x(1,2,..)	-	RO
PDU.Gang[x].iGang	String[15]	Breaker/section silk-screened name. Example: 'A' or 'B' ….	-	RO
PDU.Gang[x].iName	String[31]	Breaker/section friendly name.	-	RW
PDU.Gang[x].InputID	Constant	Identify which Input is powering the group. This is useful when the PDI is dual Input.	-	RO
PDU.Gang[x].OverCurrent[1].Threshold	Parameter		mA	RW
PDU.Gang[x].OverCurrent[3].Threshold	Parameter		mA	RW
PDU.Gang[x].OverCurrent[4].Threshold	Parameter		mA	RW
PDU.Gang[x].OverVoltage[1].Threshold	Parameter	Threshold	cV	RW
PDU.Gang[x].OverVoltage[2].Threshold	Parameter	Threshold	cV	RW
PDU.Gang[x].OverVoltage[3].Threshold	Parameter	Threshold	cV	RW
PDU.Gang[x].OverVoltage[4].Threshold	Parameter	Threshold	cV	RW
PDU.Gang[x].PeakFactor	Measure	Crest factor of the current provided by the breaker/section. A double pole breaker is calculated as the max of the two poles crest factor.	m%	RO
PDU.Gang[x].PercentLoad	Measure	Percent load consumed by the breaker/section. It is the ratio: current consumed / the nominal current.	%	RO
PDU.Gang[x].PhaseID	Constant	Phase number that is connected to the breaker/section: 1, 2, or 3. A double pole breaker is ij. Ex: 12 if the 2 phases are L1 and L2.	-	RO
PDU.Gang[x].Pole[1].ActivePower	HideMeasure	Active Power provided by the pole.	dW	RO
PDU.Gang[x].Pole[1].ApparentPower	HideMeasure	Apparent Power provided by the pole.	dVA	RO
PDU.Gang[x].Pole[1].Current	HideMeasure	Current provided by the pole.	mA	RO
PDU.Gang[x].Pole[1].PeakFactor	HideMeasure	Crest factor of the current provided by the pole.	m%	RO
PDU.Gang[x].Pole[1].PhaseID	Constant	Phase number that is connected to the pole: 1, 2, or 3.	-	RO
PDU.Gang[x].Pole[1].PowerFactor	HideMeasure	Ratio of active power / apparent power provided by the pole of the breaker or outlet section.	m%	RO
PDU.Gang[x].Pole[1].ReactivePower	HideMeasure	Reactive Power provided by the pole.	dVAR	RO
PDU.Gang[x].Pole[1].Statistic[5].Energy	HideMeasure	Energy counter since last reset. As it is reset to 0, the related timestamp is updated with the current RTC value.	Wh	RO
PDU.Gang[x].Pole[1].Voltage	HideMeasure	Voltage Measured on the pole.	cV	RO
PDU.Gang[x].Pole[2].ActivePower	HideMeasure	Active Power provided by the pole.	dW	RO

Table 11. PDU CLI Objects (Continued)

XML Object Name	Type	Description	Unit	Access
PDU.Gang[x].Pole[2].ApparentPower	HideMeasure	Apparent Power provided by the pole.	dVA	RO
PDU.Gang[x].Pole[2].Current	HideMeasure	Current Power provided by the pole.	mA	RO
PDU.Gang[x].Pole[2].PeakFactor	HideMeasure	Crest factor of the current provided by the pole.	m%	RO
PDU.Gang[x].Pole[2].PhaseID	Constant	Phase number that is connected to the pole: 1, 2, or 3.	-	RO
PDU.Gang[x].Pole[2].PowerFactor	HideMeasure	Ratio of active power / apparent power provided by the pole of the breaker or outlet section.	m%	RO
PDU.Gang[x].Pole[2].ReactivePower	HideMeasure	Reactive Power provided by the pole.	dVAR	RO
PDU.Gang[x].Pole[2].Statistic[5].Energy	HideMeasure	Energy counter since last reset. As it is reset to 0, the related timestamp is updated with the current RTC value.	Wh	RO
PDU.Gang[x].Pole[2].Voltage	HideMeasure	Voltage Measured on the pole.	cV	RO
PDU.Gang[x].PowerFactor	Measure	Ratio of active power / apparent power provided by the breaker or outlet section.	m%	RO
PDU.Gang[x].PresentStatus.OverCurrent	AlarmL1	0: No threshold triggered 1: Warning low threshold triggered 2: Critical low threshold triggered 3: Warning high threshold triggered 4: Critical high threshold triggered	-	RO
PDU.Gang[x].PresentStatus.OverVoltage	AlarmL1	0: No threshold triggered 1: Warning low threshold triggered 2: Critical low threshold triggered 3: Warning high threshold triggered 4: Critical high threshold triggered	-	RO
PDU.Gang[x].PresentStatus.Tripped	AlarmL1	0: Normal 1: Alarm	-	RO
PDU.Gang[x].ReactivePower	Measure	Reactive Power provided by the breaker/section. For a double pole breaker, the reactive power for the two poles is combined.	dVAR	RO
PDU.Gang[x].Statistic[3].Current	Measure	Current peak consumption since last reset. As it is reset to 0, the related timestamp is updated with the current RTC value. When a value higher than the stored value is detected, the stored valued is overwritten.	mA	RO
PDU.Gang[x].Statistic[3].ModuleReset	Command	Command to Reset the stat. This command puts 0 in the max and saves the current value of Timer.	-	RW
PDU.Gang[x].Statistic[3].Reset.Time	Measure	Timestamp saved when the stat reset is performed.	s	RO
PDU.Gang[x].Statistic[3].Time	Measure	Timestamp saved at the moment where the current peak consumption is reset.	s	RO
PDU.Gang[x].Statistic[5].Energy	Measure	Energy counter since PDU startup. For a double pole breaker, it is calculated as the accumulation of the two poles energy counter.	Wh	RO
PDU.Gang[x].Statistic[5].ModuleReset	Command	Command to Reset the stat, This command does not put 0 in the counter, but saves the current value of Energy timer into the data, Reset.Energy.	-	RW
PDU.Gang[x].Statistic[5].Reset.Energy	Measure	Energy saved when the user resets the stat.	Wh	RO

Table 11. PDU CLI Objects (Continued)

XML Object Name	Type	Description	Unit	Access
PDU.Gang[x].Statistic[5].Reset.Time	Measure	Timestamp saved when the user resets the stat.	s	RO
PDU.Gang[x].Type	Constant	Type of gang: 1 : Section of outlets (with 1 measurement) 2 : Section of outlets (with 2 measurement, 1st method of wiring CT, current is max of 2 pole measures) 3 : Section of outlets (with 2 measurement, 2nd method of wiring CT, current is sum of 2 pole measures) 4 : Breaker 1 pole 5 : Breaker 2 pole (with 1 pole measurement) 6 : Breaker 2 pole (with 2 pole measurement, 1st method of wiring CT, current is max of 2 pole measures) 7 : Breaker 2 pole (with 2 pole measurement, 2nd method(PQNA) of wiring CT, , current is sum of 2 pole measures) 8 : Section of outlets (without current measurement) 9 : Section of outlets (with current and voltage measurement)	-	RO
PDU.Gang[x].Voltage	Measure	Voltage Measured on the breaker/section. For a double pole breaker, it is the Li to Lj voltage.	cV	RO
PDU.Input[1].ActivePower	Measure	Active Power Measurement. It is the accumulation of 1 or 3 phase measures.	dW	RO
PDU.Input[1].ApparentPower	Measure	Apparent Power Measurement. It is the accumulation of 1 or 3 phase measures.	dVA	RO
PDU.Input[1].ChangedStatus.FrequencyOutOfRange	Timestamp		s	RO
PDU.Input[1].Frequency	Measure	Frequency Measurement.	dHz	RO
PDU.Input[1].Mode	Constant	Wiring Mode 0: Wye Measuring 1: Delta Measuring 2: Wye Current and Delta Measuring	-	RO
PDU.Input[1].Phase.Count	Constant	Number of phase managed by the Input module.	-	RO
PDU.Input[1].Phase[x].ActivePower	Measure	Active Power Measurement.	dW	RO
PDU.Input[1].Phase[x].ApparentPower	HideMeasure	Apparent Power Measurement.	dVA	RO
PDU.Input[1].Phase[x].ChangedStatus.OverCurrent	Timestamp	Timestamp of last changing state of the alarm that has the same name in the collection PresentStatus.	s	RO
PDU.Input[1].Phase[x].ChangedStatus.OverVoltage	Timestamp	Timestamp of last changing state of the alarm that has the same name in the collection PresentStatus.	s	RO
PDU.Input[1].Phase[x].Current	Measure	Current Measurement.	mA	RO
PDU.Input[1].Phase[x].OverCurrent[1].Threshold	Parameter		mA	RW
PDU.Input[1].Phase[x].OverCurrent[3].Threshold	Parameter		mA	RW
PDU.Input[1].Phase[x].OverCurrent[4].Threshold	Parameter		mA	RW
PDU.Input[1].Phase[x].OverVoltage[1].Threshold	Parameter		cV	RW
PDU.Input[1].Phase[x].OverVoltage[2].Threshold	Parameter		cV	RW
PDU.Input[1].Phase[x].OverVoltage[3].Threshold	Parameter		cV	RW
PDU.Input[1].Phase[x].OverVoltage[4].Threshold	Parameter		cV	RW

Table 11. PDU CLI Objects (Continued)

XML Object Name	Type	Description	Unit	Access
PDU.Input[1].Phase[x].PeakFactor	Measure	Crest factor of the current provided by the phase.	m%	RO
PDU.Input[1].Phase[x].PercentLoad	Measure	Percent load consumed on the phase. It is the ratio: current consumed / the nominal current of the PDU.	%	RO
PDU.Input[1].Phase[x].PhaseID	Constant	Phase ID identifier depending of the wiring: 1: Line 1 to Neutral 2: Line 2 to Neutral 3: Line 3 to Neutral 12: Line 1 to Line 2 23: Line 2 to Line 3 31: Line 3 to Line 1	-	RO
PDU.Input[1].Phase[x].PowerFactor	HideMeasure	Ratio of active power / apparent power provided by the phase. Value 0 to 100 for Cos PHI = 0.00 to 1.00	m%	RO
PDU.Input[1].Phase[x].PresentStatus.OverCurrent	AlarmL1	0: No threshold triggered 1: Warning low threshold triggered 2: Critical low threshold triggered 3: Warning high threshold triggered 4: Critical high threshold triggered	-	RO
PDU.Input[1].Phase[x].PresentStatus.OverVoltage	AlarmL1	0: No threshold triggered 1: Warning low threshold triggered 2: Critical low threshold triggered 3: Warning high threshold triggered 4: Critical high threshold triggered	-	RO
PDU.Input[1].Phase[x].ReactivePower	HideMeasure	Reactive Power Measurement.	dVAR	RO
PDU.Input[1].Phase[x].Statistic[5].Energy	HideMeasure	Energy counter since last reset. As it is reset to 0, the related timestamp is updated with the current RTC value.	Wh	RO
PDU.Input[1].Phase[x].Statistic[5].ModuleReset	Command		-	RW
PDU.Input[1].Phase[x].Statistic[5].Reset.Energy	HideMeasure	Energy counter saved at last reset. As it is reset, the related timer updated with PDU timer since 1st restart.	Wh	RO
PDU.Input[1].Phase[x].Statistic[5].Reset.Time	HideMeasure	Timestamp saved at the moment when the related energy counter is reset.	s	RO
PDU.Input[1].Phase[x].Voltage	Measure	Voltage Measurement.	cV	RO
PDU.Input[1].PowerFactor	Measure	Ratio of active power / apparent power provided by the input. Value 0 to 100 for Cos PHI = 0.00 to 1.00	m%	RO
PDU.Input[1].PresentStatus.FrequencyOutOfRange	AlarmL1	0: Frequency OK 1: Frequency is out of +/- 3Hz tolerance	-	RO
PDU.Input[1].ReactivePower	Measure	Reactive Power Measurement. It is the accumulation of 1 or 3 phase measures.	dVAR	RO

Table 11. PDU CLI Objects (Continued)

XML Object Name	Type	Description	Unit	Access
PDU.Input[1].Statistic[3].ActivePower	Measure	Power peak consumption since last reset. As it is reset to 0, the related timestamp is updated with the current RTC value. When a value higher than the stored value is detected, the stored valued is overwritten.	dW	RO
PDU.Input[1].Statistic[3].ModuleReset	Command	Command to Reset the stat. This command puts 0 in the max and saves the current value of Timer into the data …Timer and into ...Reset.Timer.	-	RW
PDU.Input[1].Statistic[3].Reset.Time	Measure	Timestamp saved at the moment when the statistic is reset.	s	RO
PDU.Input[1].Statistic[3].Time	Measure	Timestamp saved at the moment when the statistic is reset.	s	RO
PDU.Input[1].Statistic[5].Energy	Measure	Energy counter since last reset. As it is reset to 0, the related timestamp is updated with the current RTC value. It combines the energy consumed on 1 or 3 phases.	Wh	RO
PDU.Input[1].Statistic[5].ModuleReset	Command	Command to Reset the stat. This command does not put 0 in the counter, but it saves the current value of Energy timer into the data ...Reset.Energy.	s	RW
PDU.Input[1].Statistic[5].Reset.Energy	Measure	Energy saved at the instant the user resets the stat.	Wh	RO
PDU.Input[1].Statistic[5].Reset.Time	Measure	Timestamp saved at the instant the user resets the stat.	s	RO
PDU.Input[1].Type	Constant	List types of PDU Input plugs.	-	RO
PDU.MeasurementBoard.Gateway.Address	HideMeasure	Address of the teridian module to be accessed.	-	RW
PDU.MeasurementBoard.Gateway.Command	HideMeasure	Write: command to the Gateway 0: None 1: Read 2: Write Read: return the CR of last command to the Gateway: 0: Success <> 0 , Access failed for the following reasons: 1: Command Unknown. 2: Gateway not enabled. 3: Address out of range. 4: Register out of r.	-	RW
PDU.MeasurementBoard.Gateway.Count	HideMeasure	Number of 32 bits data to be read or write in consecutive READ or WRITE request. 1 to 8.	-	RW
PDU.MeasurementBoard.Gateway.Register	HideMeasure	Address of the register to be read or write.	-	RW
PDU.MeasurementBoard.Gateway.Switchable	HideMeasure	0: The gateway is disabled. 1: The gateway is enabled.	-	RW
PDU.MeasurementBoard.Gateway[x].Value	HideMeasure	1 up to 8 consecutive register values can be read or write with the gateway in one request. NOTE: Follow these steps to read registers from the board: 1. Write 1 in Command 2. Read Command, check it is 0 3. Read the data that had been read into Value	-	RW

Table 11. PDU CLI Objects (Continued)

XML Object Name	Type	Description	Unit	Access
PDU.MeasurementBoard[x].PresentStatus.CommunicationLost	Measure	Communication status with the acquisition card ICM & SM: 0: Communication OK 1: Communication failed.	-	RO
PDU.OutletSystem.Outlet.Count	Constant	Total Number of outlets	-	RO
PDU.OutletSystem.Outlet[x].ConfigCurrent	Constant	Nominal Amps: 10A, 15A, 16A, 20A, ..	mA	RO
PDU.OutletSystem.Outlet[x].GangID	Constant	Breaker/section index where the Outlet is connected. It is the x of Gang[x] collection.	-	RO
PDU.OutletSystem.Outlet[x].iName	String[31]	Outlet friendly name.	-	RW
PDU.OutletSystem.Outlet[x].OutletID	Constant	Numbering of the outlet into the breaker/section module. 1 to 56.	-	RO
PDU.OutletSystem.Outlet[x].PhaseID	Constant	Phase ID that powers the outlet: - 1, 2, 3 to identify a simple phase. - 12, 23, 31 to identify a composed phase.	-	RO
PDU.OutletSystem.Outlet[x].PoleID	Constant	Pole ID of the breaker/section where the Outlet is connected. Two cases are: - Section or Single pole breaker, always 0. - Double pole breaker: 0: when powered between 2 poles 1: when powered by pole 1 voltage. 2: when powered by pole 2 voltage.	-	RO
PDU.OutletSystem.Outlet[x].PresentStatus.SwitchOnOff	Measure	0: Outlet not powered 1: Outlet powered	-	RO
PDU.OutletSystem.Outlet[x].Type	Constant	Types of PDU outlets: unknown (0), iecC13 (1), iecC19 (2), uk (10), french (11), schuko (12), nema515 (20), ema51520 (21), nema520 (22), nemaL520 (23), nemaL530 (24), nema615 (25), nema620 (26), nemaL620 (27), nemaL630 (28), nemaL715 (29), rf-203P 277v (30)	-	RO
PDU.PowerSummary.ChangedStatus.CommunicationLost	Timestamp	Communication intra modules have failed.	s	RO

Table 11. PDU CLI Objects (Continued)

XML Object Name	Type	Description	Unit	Access
PDU.PowerSummary.ConfigActivePower	Constant	PDU Nominal Active Power	W	RO
PDU.PowerSummary.ConfigCurrent	Constant	PDU PDU total rating current.	mA	RO
PDU.PowerSummary.ConfigVoltage	Constant	PDU rating voltage.	V	RO
PDU.PowerSummary.iManufacturer	String[31]	Manufacturer Name. Example: "HP"	-	RO
PDU.PowerSummary.iName	String[31]	Unit friendly name.	-	RW
PDU.PowerSummary.iPartNumber	String[15]	Part Number.	-	RO
PDU.PowerSummary.iProduct	String[63]	Product Name.	-	RO
PDU.PowerSummary.iReferenceNumber	String[31]	Technical Reference of firmware.	-	RO
PDU.PowerSummary.iSerialNumber	String[15]	Serial Number.	-	RO
PDU.PowerSummary.iVersion	String[15]	F/W Version.	-	RO
PDU.PowerSummary.PDUType	Constant	Feature Topology of the PDU: 0: Unknown 1: SW (Switched) 2: AM (Advanced Monitored) 3: MA (Managed) 4: MI (Monitored)	-	RO
PDU.PowerSummary.PresentStatus.CommunicationLost	AlarmL1	Communication intra modules have failed.	-	RO
PDU.PowerSummary.Temperature	Measure	Internal Temperature.	d°K	RO
PDU.PowerSummary.Time	Measure	Unix timestamp that is refreshed from the RTC.	s	RW
PDU.PowerSummary.Timer	Measure	Time elapsed since the 1st start of the device.	s	RO

Table 12. System CLI Objects

XML Object Name	Access right	Type	Description	Access	Default Value
System.Bootloader.iVersion	admin	String:15		RO	""
System.Bootloader.Mode	superadmin	BootMode	0: Normal 1: Upgrade 2: Passthru 3: ATE 4: Bootstrap	RW	0
System.Contact	admin	String:31		RW	""
System.DaisyChain.Count	admin	Integer0to65535		RO	1
System.DaisyChain.DeviceId	admin	DaisyChainDeviceId	0: Host 1: Device 1 2: Device 2 3: Device 3	RW	1
System.DaisyChain.Position	admin	DaisyChainPosition	0: Middle 1: End	RW	0

Table 12. System CLI Objects (Continued)

XML Object Name	Access right	Type	Description	Access	Default Value
System.DaisyChain.Status	admin	DaisyChainStatus	0: No Communication 1: Communication OK 2: Communication failed 3: Host conflict 4: Device conflict	RO	0
System.Display.Contrast	admin	Integer25to45		RW	32
System.DaisyChain[x].DeviceId	admin	DaisyChainDeviceId	0: Host 1: Device 1 2: Device 2 3: Device 3	RO	1
System.DaisyChain[x].MacAddress	admin	String:17		RO	"00:00:00:00:00:00"
System.DaisyChain[x].Position	admin	DaisyChainPosition	0: Middle 1: End	RO	0
System.DaisyChain[x].Status	admin	DaisyChainStatus	0: No Communication 1: Communication OK 2: Communication failed 3: Host conflict (not implemented) 4: Device conflict	RO	0
System.Display.Contrast	admin	Integer25to45		RW	32
System.Display.Password	superadmin	Password:4		RW	
System.Display.Password.IsEnable	superadmin	ControlState		RW	1234
System.Display.Language	superadmin	DisplayLanguage	0: English 1: French 2: German 3: Spanish 4: Russian 5: Portuguese 6: Italian	RW	
System.Display.LcdRotation	admin	LcdRotation	0: Rotation 0 Deg(0U) 1: Rotation 90 Deg(1U) 2: Rotation 180 Deg(0U) 3: Rotation 270 Deg(1U)	RW	0
System.Email.Count	admin	Integer0to65535		RO	NB_EMAIL_NOTIFICATIONS
System.Email.Sender	admin	String:31		RW	"PDU@hp.com"

Table 12. System CLI Objects (Continued)

XML Object Name	Access right	Type	Description	Access	Default Value
System.Email[x].Description	admin	String:63		RW	"||||||||"
System.Email[x].EventList.All	admin	EventType	0: None 1: All Alarms	RW	0
System.Email[x].Events.Log	admin	ControlState	0: Disabled 1: Enabled	RW	0
System.Email[x].Recipient	admin	String:127		RW	"email1@recipient.com|email2@recipient.com|email3@recipient.com|email4@recipient.com|email5@recipient.com|email6@recipient.com|email7@recipient.com|email8@recipient.com|email9@recipient.com"
System.Email[x].Report.Hour	admin	Time0to23hours		RW	0
System.Email[x].Report.Next	admin	Time0to31days		RW	0
System.Email[x].Report.Periodicity	admin	Time0to28days		RW	0
System.Email[x].Selected	admin	ControlState	0: Disabled 1: Enabled 2: Deleted	RW	0
System.Email[x].Test	admin	Boolean		WO	0
System.Ethernet.iVersion	admin	String:15		RO	"00.00.0022" "00.00.0029" "00.00.0030"
System.Ethernet.MacAddress	admin	String:31		RO	"00:00:00:00:00:00"
System.Ethernet.Mode **NOTE:** Reboot is required.	admin	EthMode	0: Auto Negotiation 1: 100 Mbps Full Duplex 2: 100 Mbps Half Duplex 3: 10 Mbps Full Duplex 4: 10 Mbps Half Duplex	RW	0
System.FactoryReset	admin	Boolean		WO	0
System.FirmwareUpgrade	admin	Boolean		RW	1
System.FirmwareUpgradeMode	admin	ControlState	0: Disabled 1: Enabled	WO	0
System.FormatFS	superadmin	ControlState	0: Disabled 1: Enabled	WO	0
System.KeepDC	admin	ControlState		RW	0
System.KeepIP	admin	ControlState	0: Disabled 1: Enabled	RW	0

Table 12. System CLI Objects (Continued)

XML Object Name	Access right	Type	Description	Access	Default Value
System.Language	admin	Language	2: English (ENG) 3: French (FRE) 4: Spanish (SPA) 5: German (GER) 6: Italian (ITA) 7: Chinese Simplified (CHI) 8: Japanase (JPN) 9: Korean (KOR) 10 : Chinese Traditionnal (CHT) 11 : Russian (RUS) 12 : Portuguese (POR) 13 : Czech (CZE) 14 : Polish (POL)	RW	2
System.Location	admin	String:31		RW	""
System.Login	superadmin	String:31		RW	"admin"
System.LogReset	admin	Boolean		WO	0
System.Network.Authentication.AuthMethod	admin	AuthMethod	1: Local Authentication 2: LDAP Authentication 3: Radius Authentication	RW	1
System.Network.Authentication.AuthOrder	admin	AuthOrder	1: Local 2: External then Local 3: Local then External 4: External	RW	1
System.Network.Authentication.MaxSessionTime	admin	Integer0toFFFFFFFF		RW	0xFFFFFFF
System.Network.Authentication.SessionTime	admin	Integer0toFFFFFFFF		RW	300
System.Network.DHCP **NOTE:** Reboot is required.	admin	ControlState	0: Disabled 1: Enabled	RW	1
System.Network.DomainName **NOTE:** Reboot is required.	admin	String:63		RW	"pdu.domain.com"
System.Network.EnergyWise.Enable	admin	ControlState	0:Disable 1:Enable	RW	0
System.Network.EnergyWise.Domain	admin	String:63		RW	“MyDomain”
System.Network.EnergyWise.Secret	admin	ControlState		RW	0
System.Network.EnergyWise.SecretKey	admin	Password:63		RW	“”
System.Network.EnergyWise.RemotePort	admin	Integer1to65535		RW	43440
System.Network.EnergyWise.ListenPort	admin	Integer1to65535		RW	48296

Table 12. System CLI Objects (Continued)

XML Object Name	Access right	Type	Description	Access	Default Value
System.Network.EnergyWise.SdkVersion	admin	String:31		RO	RELEASE 1.2.0
System.Network.EnergyWise.SeqId	admin	Integer0to4294967295		RW	0
System.Network.EnergyWise.ThresholdLevel	admin	Integer0to10		RW	4
System.Network.EnergyWise.State	admin	String:31		RO	""
System.Network.EnergyWise.Cmd	admin	EnergyWiseCmd		RW	0
System.Network.FTP.Access	admin	ControlState	0: Disabled 1: Enabled	RW	1
System.Network.HostName **NOTE:** Reboot is required.	admin	String:31		WO	"PDU$x"
System.Network.HTTP.Access **NOTE:** Reboot is required.	admin	ControlState	0: Disabled 1: Enabled	RW	1
System.Network.HTTP.Port **NOTE:** Reboot is required.	admin	Integer1to65535		RW	80
System.Network.HTTPS.Port **NOTE:** Reboot is required.	admin	Integer1to65535		RW	443
System.Network.IPAddress **NOTE:** Reboot is required.	admin	IPv4		RW	"192.168.123.123"
System.Network.IPGateway **NOTE:** Reboot is required.	admin	IPv4		RW	""
System.Network.IPMask **NOTE:** Reboot is required.	admin	IPv4		RW	"255.255.0.0"
System.Network.IPv6Address1 **NOTE:** Reboot is required.	admin	IPv6		RW	""
System.Network.IPv6Address2	admin	IPv6		RO	""
System.Network.IPv6AutoConfig **NOTE:** Reboot is required.	admin	ControlState	0: Disabled 1: Enabled	RW	0
System.Network.IPv6DefaultGateway **NOTE:** Reboot is required.	admin	IPv6		RW	""
System.Network.IPv6Enable **NOTE:** Reboot is required.	admin	ControlState	0: Disabled 1: Enabled	RW	0
System.Network.IPv6LocalAddress	admin	IPv6		RO	""
System.Network.IPv6Status	admin	NetworkIpv6Status	0: Invalid 1: Valid 2: Manual Configuration	RO	0
System.Network.Ldap.AuthMechanism	admin	LdapAuthMechanism	0: Simple 7: Digest MD5	RW	0

Table 12. System CLI Objects (Continued)

XML Object Name	Access right	Type	Description	Access	Default Value
System.Network.Ldap.GroupSearch.AuthzMode	admin	LdapAuthorization Mode	0: No Authorization 1: By User Attribute 2: By Group	RW	0
System.Network.Ldap.GroupSearch.BaseDn	admin	String:99		RW	""
System.Network.Ldap.GroupSearch.UPSGroupNameAttr	admin	String:49		RW	""
System.Network.Ldap.GroupSearch.UserNameAttr	admin	String:49		RW	""
System.Network.Ldap.SearchMode	admin	LdapSearchMode	0: Anonymous Search 1: User Bind Search	RW	0
System.Network.Ldap.SearchUser	admin	String:99		RW	""
System.Network.Ldap.SearchUserPassword	admin	Password:49		RW	""
System.Network.Ldap.Server.Count	admin	Integer0to10	2	RO	2
System.Network.Ldap.Server[x].IsEnable	admin	ControlState	0: Disabled 1: Enabled	RW	0
System.Network.Ldap.Server[x].Port	admin	Integer1to65535		RW	389
System.Network.Ldap.Server[x].ServerName	admin	String:49		RW	"LDAP Server1|LDAP Server2"
System.Network.Ldap.Server[x].TimeOut	admin	Integer0to65535		RW	10
System.Network.Ldap.ServerType	admin	LdapServerType	0: Generic LDAP server 1: Active Directory	RW	0
System.Network.Ldap.SSLMode	admin	LdapSSLMode	0: No SSL 1: SSL (LDAPS) 2: SSL (Start TLS)	RW	0
System.Network.Ldap.UserSearch.Attribute	admin	String:49		RW	""
System.Network.Ldap.UserSearch.BaseDn	admin	String:99		RW	""
System.Network.Ldap.UserSearch.Object	admin	String:49		RW	""
System.Network.PrefixLength1	admin	Integer0to128		RW	0
System.Network.PrefixLength2 **NOTE:** Reboot is required.	admin	Integer0to128		RO	0
System.Network.PrimaryDNS **NOTE:** Reboot is required.	admin	IPv4		RW	""
System.Network.Radius.Server[x].IsEnable	admin	ControlState		RW	0
System.Network.Radius.Server[x].ServerName	admin	String:48		RW	"RADIUS Server1|RADIUS Server2"
System.Network.Radius.Server[x].SharedSecret	admin	Integer1to65535		RW	""
System.Network.Radius.Server[x].Port	admin	NasIdentifierType	65535	RW	1812
System.Network.Radius.Server[x].NasIdentiferType	admin	Integer0to255	3	RW	0
System.Network.Radius.Server[x].Retry	admin	Integer0to255	9	RW	3
System.Network.Radius.Server[x].Timeout	admin	Integer1to65535	99	RW	5
System.Network.SecondaryDNS **NOTE:** Reboot is required.	admin	IPv4		RW	""

Table 12. System CLI Objects (Continued)

XML Object Name	Access right	Type	Description	Access	Default Value
System.Network.SmtpServer.Authentication	admin	ControlState	0: Disabled 1: Enabled	RW	0
System.Network.SmtpServer.HostName	admin	String:63		RW	""
System.Network.SmtpServer.Login	admin	String:31		RW	""
System.Network.SmtpServer.Password	admin	String:31		RW	""
System.Network.SmtpServer.Port	admin	Integer1to65535		RW	25
System.Network.SNMP.Port	admin	Integer1to65535		RW	161
System.Network.SNMP.snmpVersion	admin	SNMPVersion	0: disabled 1: SNMP V1 2: SNMP V3 3: SNMP V1&V3	RW	0
System.Network.SNMP.TrapPort	admin	Integer1to65535		RW	162
System.Network.SNMP.V1.User.Count	admin	Integer0to65535		RO	SNMPV1_NBCOMMUNITIES
System.Network.SNMP.V1.User[x].SecurityRight	admin	Snmpv3VacmSecurityRight	0: No Right 1: Read-Only 2: Read/Write 3: Number	RW	0
System.Network.SNMP.V1.User[x].UserName	admin	String:24		RW	"public|private"
System.Network.SNMP.V3.User.Count	admin	Integer0to65535		RO	SNMPV3_USM_NBUSERS
System.Network.SNMP.V3.User[x].Name	admin	String:31		RW	"SNMPv3 User 1|SNMPv3 User 2|SNMPv3 User 3|SNMPv3 User 4"
System.Network.SNMP.V3.User[x].Password	admin	String:24		RW	"|||"
System.Network.SNMP.V3.User[x].PrivacyKey	admin	String:24		RW	"|||"
System.Network.SNMP.V3.User[x].SecurityLevel	admin	Snmpv3UsmLevel	0: Not Set 1: No Auth No Priv 2: Auth No Priv 3: Auth Priv	RW	0
System.Network.SNMP.V3.User[x].SecurityRight	admin	Snmpv3VacmSecurityRight	0: No Access 1: Read-Only 2: Read/Write	RW	0
System.Network.SSH.Port **NOTE:** Reboot is required.	admin	Integer1to65535		RW	22
System.Network.Syslog.Server.Count	admin	Integer0to10		RW	2
System.Network.Syslog.Server[x].IsEnable	admin	ControlState		RW	0

Table 12. System CLI Objects (Continued)

XML Object Name	Access right	Type	Description	Access	Default Value
System.Network.Syslog.Server[x].ServerName	admin	String:49		RW	"Syslog Server1|Syslog Server2"
System.Network.Syslog.Server[x].Port	admin	Integer1to65535		RW	514
System.Network.Syslog.Server[x].Protocol	admin	SyslogProtocol	0: UDP 1: TCP	RW	0
System.Network.Syslog.Server[x].BOM	admin	ControlState		RW	1
System.Network.Syslog.Server[x].MessageTransfer	admin	SyslogMessageTransfer		RW	0
System.Network.Syslog.Server[x].Facility	admin	SyslogFacility	"0: Octet Counting 1: Non Transparent Framing" "0: kernel messages 1: user-level messages 2: mail system 3: system daemons 4: security/authorization messages 5: messages generated internally by syslogd 6: line printer subsystem 7: network news subsystem 8: UUCP subsystem 9: clock daemon 10: security/ authorization messages 11: FTP daemon 12: NTP subsystem 13: log audit 14: log alert 15: clock daemon (note 2) 16: local use 0 (local0) 17: local use 1 (local1) 18: local use 2 (local2) 19: local use 3 (local3) 20: local use 4 (local4) 21: local use 5 (local5) 22: local use 6 (local6) 23: local use 7 (local7)"	RW	1

Table 12. System CLI Objects (Continued)

XML Object Name	Access right	Type	Description	Access	Default Value
System.Network.Syslog.Server[x].Test	admin	Boolean		WO	0
System.Network.Telnet.Access **NOTE:** Reboot is required.	admin	ControlState	0: Disabled 1: Enabled	RW	1
System.Network.Telnet.Port **NOTE:** Reboot is required.	admin	Integer1to65535		RW	23
System.Network.Telnet.Security **NOTE:** Reboot is required.	admin	ControlState	0: Disabled 1: Enabled	RW	0
System.NetworkManagementSystem.Count	admin	Integer0to65535		RO	NB_TRAP_RECEIVERS
System.NetworkManagementSystem[x].EventList.All	admin	EventType	0: None 1: All Alarms	RW	0
System.NetworkManagementSystem[x].HostName	admin	String:63		RW	"|||||||"
System.NetworkManagementSystem[x].Name	admin	String:31		RW	"Trap Receiver 1|Trap Receiver 2|Trap Receiver 3|Trap Receiver 4|Trap Receiver 5|Trap Receiver 6|Trap Receiver 7|Trap Receiver 8"
System.NetworkManagementSystem[x].Test	admin	Boolean		WO	0
System.NetworkManagementSystem[x].TrapCommunity	admin	String:24		RW	"public|public|public|public|public|public|public|public"
System.NetworkManagementSystem[x].TrapSnmpVersion	admin	SNMPVersion	0: Disabled 1: SNMP V1 2: SNMP V3	RW	0
System.Password	superadmin	Password:15		RW	"admin"
System.Restart	admin	Boolean		WO	0
System.Security **NOTE:** Reboot is required.	admin	ControlState	0: Disabled 1: Enabled	RW	0
System.Slip.Statistic	admin	String:31		RO	""
System.Temperature.Unit	admin	TemperatureUnit	1: °C 2: °F	RW	1
System.Time	admin	Time0to136years		RW	0
System.TimeDaylight	admin	ControlState	0: Disabled 1: Enabled	RW	0
System.TimeFormat	admin	DateTimeFormat	1: mm/dd/yyyy 2: dd/mm/yyyy 3: yyyy-mm-dd 4: dd mm yyyy	RW	2
System.TimeNtp	admin	String:63		RW	""

Table 12. System CLI Objects (Continued)

XML Object Name	Access right	Type	Description	Access	Default Value
System.TimeSync	admin	DateTimeSource	0: Manual 1: Sync NTP	RW	0
System.TimeUp	admin	Time0to136years		RO	0
System.TimeZone	admin	DateTimeTimeZone		RW	0
System.User.Count	admin	Integer0to65535		RW	MAX_NB_USERS
System.User[x].Login	admin	String:31		RW	"Account 1|Account 2|Account 3|Account 4|Account 5|Account 6|Account 7|Account 8"
System.User[x].Password	admin	Password:15		RW	"|||||||"
System.User[x].Status	admin	ControlState	0: Disabled 1: Enabled	RW	0
System.User[x].Type	admin	MultiUserType	0: local 1: remote	RW	0

Chapter 9 Maintenance and Alarms

This section explains maintenance functions for the HP Managed PDU, including:

- Preventive maintenance
- Equipment disposal
- Replacing the eNMC module
- Updating Firmware
- Alarms

Preventive Maintenance

For the best preventive maintenance, keep the area around the MA 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 MA 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.

Replace the MA PDU eNMC Module

NOTE Handle the eNMC module with care. Be aware that there is a risk of ESD (electrostatic discharge). As a preventive measure, wear ESD protection, such as an ESD shoe strap, while replacing the eNMC module. Do not put stress on the connection cable during installation.

A hardware configuration file specific to the MA PDU model needs to be uploaded to the new eNMC module so that the eNMC module knows the characteristics of the MA PDU model in which it resides (such as what type of input, how many circuit breakers, how many outlets, and how measurements should be displayed).

Typically, the eNMC module in your MA PDU will be replaced because it is not working. However, you may want to replace a working eNMC module.

Replace an eNMC that is Not Working

Either obtain the hardware configuration file from another working MA PDU of the same model type and configuration, or download the firmware from the HP Web site and use the configuration files for your model as contained in the package. Then, you need to upload the MA PDU model-specific hardware description file to the new eNMC module after it is installed.

Replace a Working eNMC

The resident MA PDU model's hardware description file can be downloaded before you remove the eNMC module. Save the file to a USB drive or save the file to your computer using FTP. Then, you can restore this file to the new eNMC module after you install it.

NOTE The eNMC module is hot-swappable. This means outlets will not be affected or change On/Off state during the replacement process.

NOTE See "USB Flash Mode Submenu" on page 48 for more information about saving and uploading the user configuration files that store the settings customized by the user, such as the network parameters, outlet names, and threshold values.

To replace the eNMC module (see Figure 60):

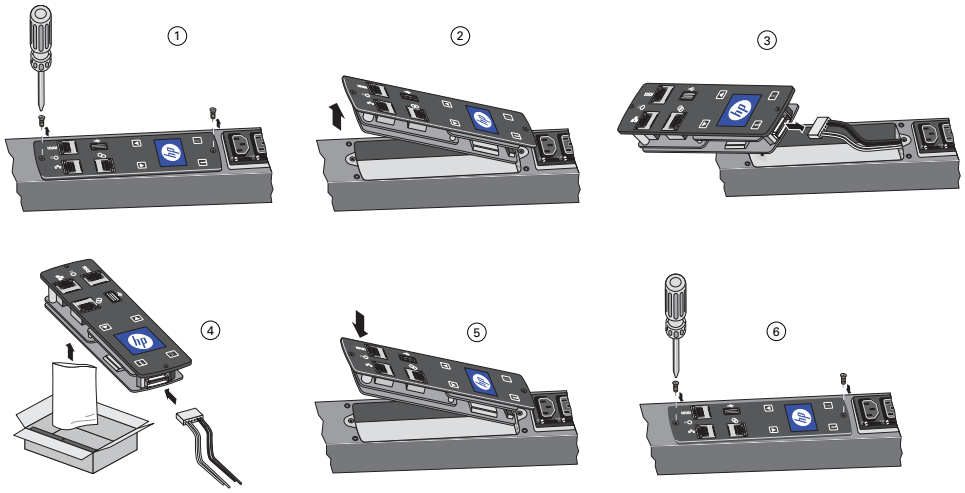


Figure 60. Replacement Procedure

1. Remove the two eNMC module mounting screws.
2. Tilt up one side of the eNMC module and locate the attached cable harness.
3. Disconnect the cable harness and remove the eNMC module.
4. Locate and unwrap the new eNMC module. Connect the cable harness to the new eNMC module.
5. Reinsert the new eNMC module.
6. Install the two eNMC module mounting screws.

NOTE After the new eNMC module is connected, the "internal communication error" message displays until the configuration file is uploaded to the eNMC module.

7. The new eNMC module will not have the same MAC address as the one you are replacing. Ensure the old MAC address label is discarded and that new MAC address label is firmly adhered to the product.
8. Download the MA PDU model's hardware configuration file using one of the following processes:
   - From the Web to your computer (go to Step 9)
   - To the USB with an MA PDU with the same configuration (go to Step 13)
9. Go to www.HP.com/support/mPDU_manuals.

10. Obtain the hardware configuration file in one of the following ways:
    - Copy the hardware configuration file from another working MA PDU (must be the same model type and configuration).
    - Download the firmware upgrade package from the HP Web site and use the attached configuration files for your model.
11. Save the MA PDU model-specific hardware configuration file to your computer. See Table 8 on page 50.

IMPORTANT

Be sure that the Configuration number on the unit rating label also appears in the file name of the model-specific MA PDU hardware configuration file.

12. Go to Step 19.
13. Make sure the eNMC module is powered ON. Connect a USB flash drive to a working MA PDU.

IMPORTANT

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

14. 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.)
15. 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.)
16. Select Save eNMC file to save the MA PDU hardware configuration file to the USB drive. The file will save to the eNMC/config/hw path at the USB drive root directory.
17. When the file is saved, click OK to confirm.
18. Disconnect the USB drive from the working MA PDU.
19. Upload the PDU hardware configuration file using one of the following processes:
    - FTP (Step 20)
    - USB (Step 30)

NOTE To perform the eNMC module configuration upload with USB, only one hardware configuration file must be stored in the USB key.

NOTE For FTP operation, FTP must be enabled (default setting) in the Web pages (**Network > Security > Global > FTP enable**).

20. Open a DOS command window on a computer that is also connected to network.
21. Change directory (CD) to the location of the XML file.

22. Open an FTP session using the following command:

    `>ftp <IPaddress>`
    where *<IPaddress>* = the IP address displayed on LCD

23. Type the default login and password ("admin" and "admin").

24. At the command prompt, type the following command:

    `>cd config/hw`

    `>dir`

25. If an MA PDU hardware configuration file (XML) file already exists, type the following command to delete the file:

    `>delete <config file>`

26. To upload the MA PDU hardware configuration file to the eNMC module, type the following command:

    `>put <config file>`
    where `<config file> = the file name to be downloaded to the eNMC module`

NOTE Keep the <config file> name exactly as it is downloaded from the website. It must begin with the prefix "epdu_cfg_*" or the eNMC module will not recognize it.

---

27. Type the following command to verify the file has been uploaded:

    `>dir`

28. Type the following command to quit the FTP session:

    `>quit`

29. Go to the "Restart the eNMC Module and Reset the MA PDU"procedure that follows.

30. Make sure the eNMC module is powered on. Connect the USB flash drive to the MA PDU with the new eNMC.

31. 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.)

32. 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.)

33. Select Load eNMC file, then click OK to upload the MA PDU hardware configuration file to the eNMC.

34. When the file is successfully loaded, click OK to confirm.

35. Remove the USB flash drive and select Exit.

36. Go to the "Restart the eNMC Module and Reset the MA PDU"procedure that follows.

Restart the eNMC Module and Reset the MA PDU

1. Restart the eNMC module using either the reset button on the LCD front panel (see "Restarting the eNMC Module" on page 37) or using a serial or network connection to a terminal emulator or Web interface.
2. Reset the MA PDU to factory default settings using one of the following:
   - Web interface "Configure PDU Network Management Card Data" on page 78 (**System > Network Management Card Configuration panel > Restore Factory default settings > Yes**)
   - LCD menu "Factory Submenu" on page 55 (**Settings > Factory > Return to Factory Settings > Yes > OK**)

NOTE Step 1 and Step 2 must be performed or the new configuration will not be properly accepted by the eNMC module.To see if the new configuration was accepted, you can check to see if the serial number displays from the PDU Info menu. If not, the new configuration was not accepted. Perform step 2 (reset to defaults) again.

After the MA PDU hardware configuration file is uploaded and eNMC module is rebooted and reset to factory defaults, the MA PDU settings return to default settings and the energy counter restarts from 0. Only the serial number is recovered.

Firmware Upgrade

The firmware upgrade process allows you to maintain the most current firmware by updating the eNMC 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 HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), 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 eNMC 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.

Upgrade Firmware with Hypertext Transfer Protocol

The HTTP upgrade using the Web occurs in two stages:

- Upload the binary file
- Implement the firmware

Upload 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 61). Click **Login** to continue or **Cancel** to exit.

NOTE The default user name is "admin" and the default password is "admin."

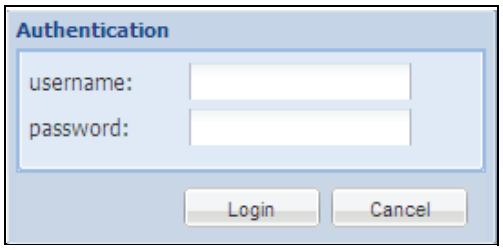


Figure 61. Login Authentication

6. The MA 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 62).
8. In the Network Management Card panel, check **Firmware upgrade enabled** and click **Browse** to find the upgrade file**.**

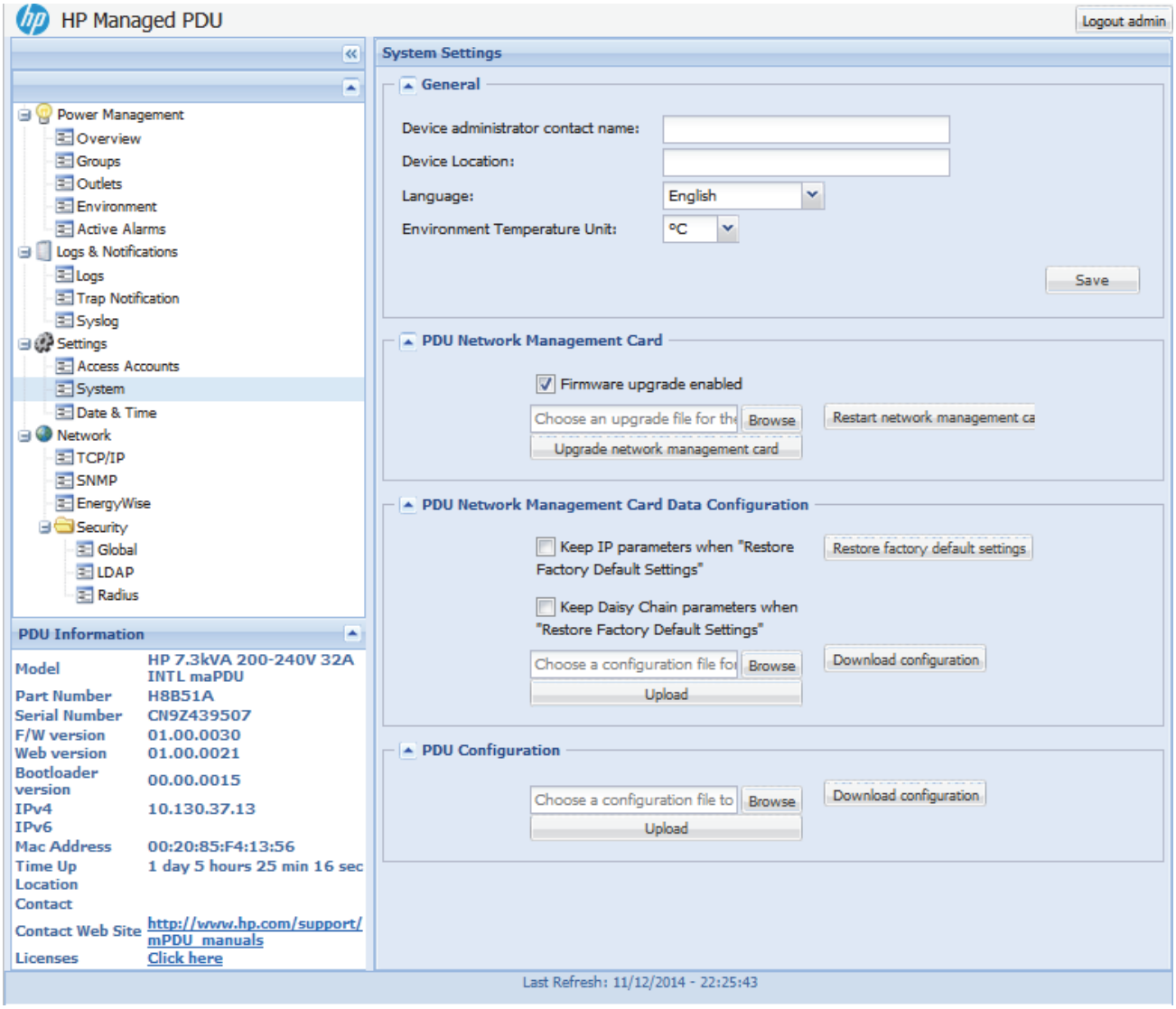


Figure 62. System Settings Page

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 eNMC 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 eNMC module, the final step is an automatic process that upgrades the firmware and refreshes the Web pages.

The eNMC 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 eNMC module reboots with the new firmware and refreshed Web pages.

Upgrade the Firmware with FTP Protocol

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 an option on the Global Security page of the Web interface.

Upload 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 eNMC module in FTP mode (see Figure 63):
   - 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 63).

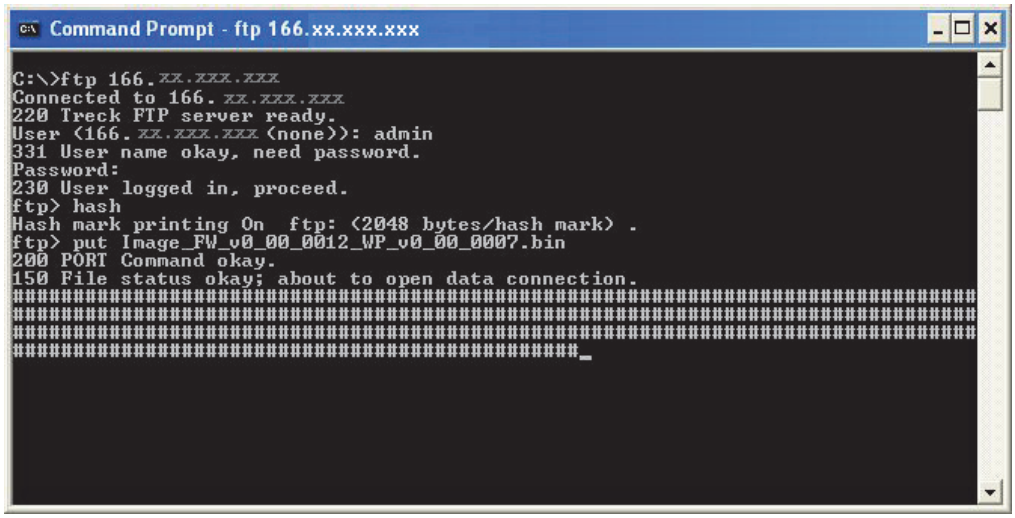


Figure 63. Launching the Upgrade

5. When the upgrade finishes, the closing message displays (see Figure 64).

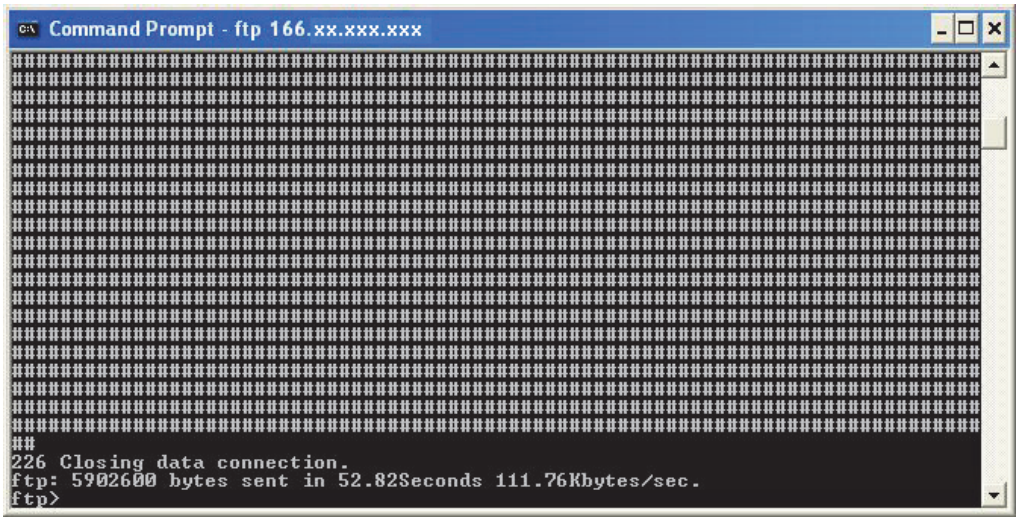


Figure 64. Closing Message

Upgrade the Firmware and Refresh Web Pages

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

The eNMC 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 eNMC module reboots with the new firmware and refreshed Web pages.

Upgrade the Firmware with the USB Port

See "Settings Menu"and "USB Flash Mode Submenu" on page 48 for more information of upgrading with the USB.

Active Alarms

The HP MA PDUs have a rich set of alarms and events to notify you of up-to-date activity and operation status. Both the local MA 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 42. For Web interface information, see "Web Interface Operation" on page 57.

- To clear flashing LCDs and the LED:
  - Press any button on the MA 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).

Define the Alarm or Event Condition

You can derive defining information about the alarm or event from the associated number code. Figure 65 shows the location of the associated number code in the Code column on the Logs page of the Web interface.

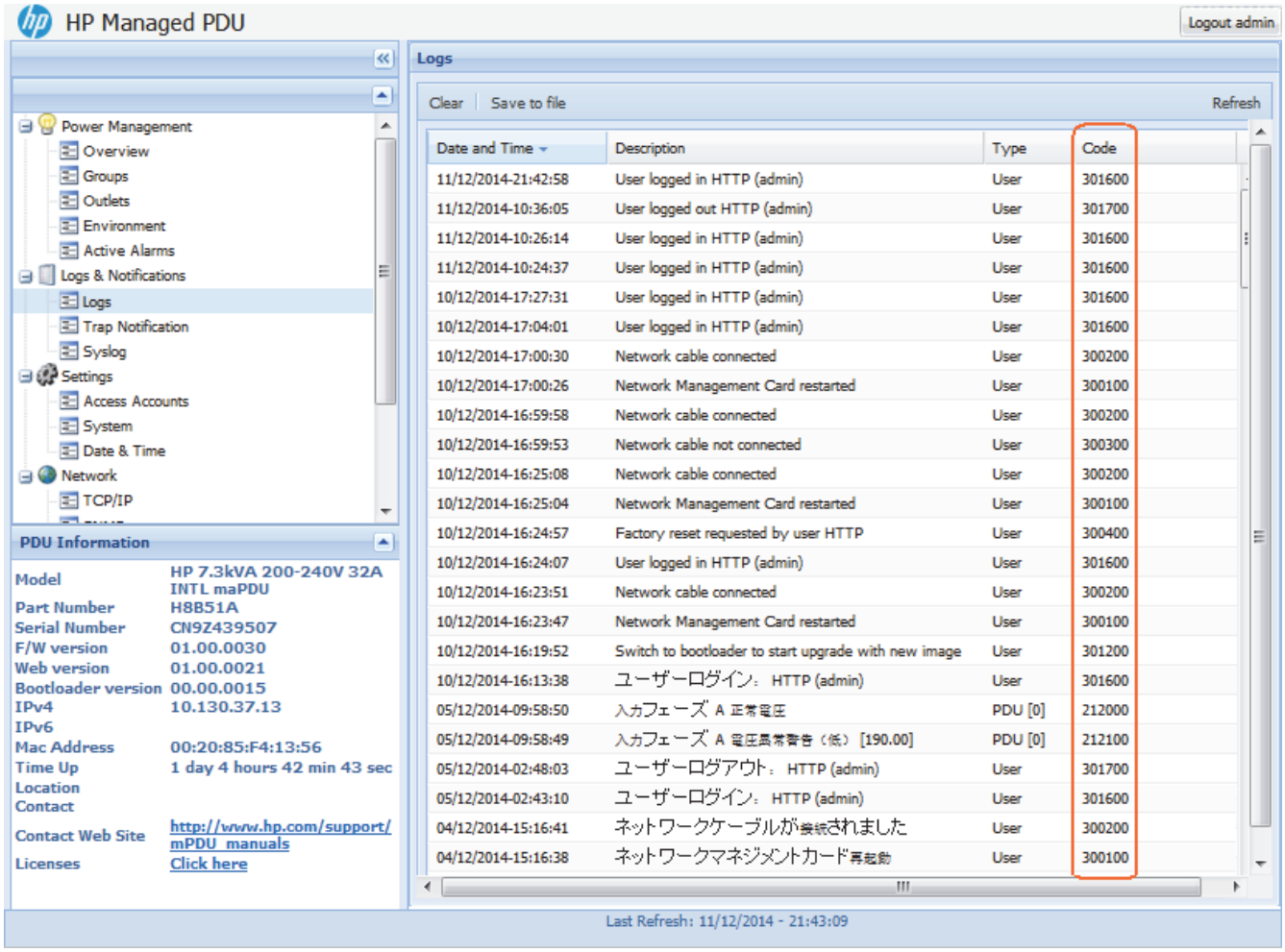


Figure 65. Location of Alarm Code on Web Interface

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.

Alarm Code Syntax

[x][yyyyy] or [x][zzz][aa]

1-Digit Type Code [x]:	**5-Digit Identification Code [yyyyy] or 3-Digit Identification code [zzz] and 2-Digit Index Code [aa]:**
0 = OS	**For Type 0 and Type 1 = Identification Code (0 to 9999)**
1 = System	**For Type 2 and Type 3 = Identification Code (0 to 999)**
2 = PDU	**and Index Code (0 to 99)**
3 = User	

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. These type codes only contain an 5-digit identification code (no index code).

Example Type 1 System Alarm Number Code

[1][02820]

Number code 102820 = No answer from a CAN device
Type Code = 1 (System)
Identification Code = 02820

Table 13 lists System alarms and events.

Table 13. 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
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

Table 13. System Alarms and Events (Continued)

Type Code	Identification Code	Alarm or Event
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	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	03585	Initialization of SSH task failed
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

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.

Example Type 2 System Alarm Number Code

[2][114][02]

Number code 211402 = PDU Critical Overcurrent L2 Phase
Type Code = 2 (PDU)
Identification = 114
Index code = 02

Table 14 lists PDU and User alarms and events.

Table 14. MA PDU and User Alarms and Events

Type Code	Identification and Index Code	Alarm or Event	Description
2	201000	Dry Contact 1 Active	The signal for Dry Contact 1 is active.
2	201100	Dry Contact 1 Not 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 Active	The signal for Dry Contact 2 is active.
2	203100	Dry Contact 2 Not 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.
2	207400	Temperature Critical High Threshold	The temperature level reading is greater than the value configured as the high temperature critical threshold.
2	211000	PDU Phase Input Current No Threshold	No section current threshold has been triggered.
2	211100	PDU 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	211200	PDU 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	211300	PDU Phase Over Current Warning	The specified section current amperage (A) reading is greater than the value configured as the over current warning threshold.

Table 14. MA PDU and User Alarms and Events (Continued)

Type Code	Identification and Index Code	Alarm or Event	Description
2	211400	PDU Phase 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 Phase Voltage No Threshold	No section voltage threshold has been triggered.
2	212100	PDU Phase Low Voltage Warning	The specified section voltage reading is less than the value configured as the low voltage warning threshold.
2	212200	PDU Phase Low Voltage Critical	The specified section voltage reading is less than the value configured as the low voltage critical threshold.
2	212300	PDU Phase Over Voltage Warning	The specified section voltage reading is greater than the value configured as the over voltage warning threshold.
2	212400	PDU Phase Over Voltage Critical	The specified section voltage reading is greater than the value configured as the over voltage critical threshold.
2	213000	PDU Frequency OK	Utility frequency is within the +/- 3 Hz of Nominal frequency.
2	213100	PDU Frequency Out of Range	Utility frequency greater or less than +/- 3 Hz of Nominal frequency.
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	241000	Communication OK	No communication failure detected on Teridian RS-485 bus

Table 14. MA PDU and User Alarms and Events (Continued)

Type Code	Identification and Index Code	Alarm or Event	Description
2	241100	Communication Lost	Communication failure detected on Teridian RS-485 bus
2	251000	Communication OK	No communication failure detected on Daisy-chained device
2	251100	Communication Lost	Communication failure detected on Daisy-chained device
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 by FTP	The specified user logged in by FTP.
3	301900	User logged out by FTP	The specified user logged out by FTP.
3	302000	User login by FTP failed	The specified user failed to log in by FTP.

Chapter 10 Specifications

This chapter lists the following specifications for the HP Managed PDU models:

- Model list
- Weights and dimensions
- Electrical input and output
- Electrical ratings
- Overcurrent protection
- Environmental and safety
- RMNs (Regulatory Compliance Model Numbers)

Model List

Table 15 lists the MA PDU models and descriptions.

Table 15. Model List

Model	Description
H8B48A	HP 2.8kVA 120V 30A NA/JP maPDU
H8B49A	HP 3.6kVA 100-240V 16A WW maPDU
H8B50A	HP 4.9kVA 208V 30A NA/JP maPDU
H8B51A	HP 7.3kVA 200-240V 32A INTL maPDU
H8B52A	HP 8.6kVA 208V 30A 3Ph NA/JP maPDU
H8B53A	HP 8.6kVA 208V 30A 3Ph DV NA/JP maPDU
H8B54A	HP 11kVA 400V 16A 3Ph INTL maPDU
H8B55A	HP 14.4kVA 208V 50A 3Ph NA/JP maPDU
H8B56A	HP 17.3kVA 208V 60A 3Ph NA/JP maPDU

Weights and Dimensions

Table 16 lists weights and dimensions for the MA PDU models.

Table 16. Weights and Dimensions

Model	Form Factor	Weight (kg)	Length in millimeters (mm)	Width in millimeters (mm)	Depth in millimeters (mm) SEE NOTE
H8B48A	42U	5.24	1689.0	52.0	65.0
H8B49A	22U	1.84	902.0	52.0	53.0
H8B50A	42U	5.33	1689.00	52.0	53.0
H8B51A	42U	4.92	1689.00	52.0	53.0
H8B52A	42U	6.23	1689.00	52.0	65.0
H8B53A	42U	6.00	1689.00	52.0	53.0
H8B54A	42U	4.60	1689.00	52.0	53.0
H8B55A	42U	9.94	1689.00	52.0	65.0
H8B56A	42U	10.47	1689.00	52.0	65.0

NOTE Circuit breakers require additional clearance.

Electrical Input and Output

Table 17 and Table 18 list the electrical input and output characteristics for the MA PDU models.

Table 17. Electrical Input and Output (All MA PDU Models)

Input Frequency	50/60 Hz ±3 Hz
Input Voltage Tolerance	+6% / -10%
Output Frequency	50/60 Hz ±3 Hz
Output Voltage Range	See Table 19 on page 138.
Output Voltage Tolerance	+6% / -10%

Table 18. Electrical Input and Output (By Model)

Model	Phases	Plug/Inlet	C13 Outlets	C19 Outlets	5-20R Outlets
H8B48A	1P	NEMA L5-30P	—	—	24
H8B49A	1P	IEC 60320 C20 SEE NOTE	7	1	—
H8B50A	1P	NEMA L6-30P	20	4	—
H8B51A	1P	IEC 60309 32A 3-wire	20	4	—
H8B52A	3P	NEMA L15-30P	18	6	—
H8B53A	3P	NEMA L21-30P	20	3	1
H8B54A	3P	IEC 60309 16A 5-wire	21	3	—
H8B55A	3P	CS8365C 50A 4-wire	12	12	—
H8B56A	3P	IEC 60309 60A 4-wire Watertight	12	12	—

NOTE See "3Ph Configurations" on page 33 for an explanation of input connector codes for 3Ph configuration topologies.

NOTE Outlets conform to the relevant outlet standard. For IEC 60320 C13 and IEC 60320 C19 outlets, the relevant standards are UL-498 and IEC 60320.

Electrical Ratings

Table 19 and Table 20 list the electrical ratings for the MA PDU models.

Table 19. Electrical Ratings

Model	Input Voltage	Output Voltage	Input Current (A)	Capacity (VA)
H8B48A	100-127V	100-127V	24	2880
H8B49A	100–240V	100–240V	16	3680
H8B50A	200–240V	200–240V	24	4992
H8B51A	200–240V	200–240V	32	7360
H8B52A	200–240V	200–240V	24	8646
H8B53A	120 / -208V	120V and 208V	24	8646
H8B54A	200/240 / -346-415V	200-240V	16	11040
H8B55A	200–240V	200–240V	40	14410
H8B56A	200–240V	200–240V	48	17292

Table 20. Output Current Ratings (All MA PDU Models)

Outlets	Ratings
IEC 60320 C13	10A
IEC 60320 C19	16A
NEMA 5-20R	16A

Overcurrent Protection

Table 21 lists the overcurrent protection requirements for the MA PDU models with outlet groups protected by circuit breakers.

Table 21. Overcurrent Protection

Model	Breaker Qty	Breaker Type SEE NOTE	Breaker Rating (A)
H8B48A	2	SP	20A
H8B49A	0	—	—
H8B50A	2	DP	20A
H8B51A	2	SP	16A
H8B52A	3	DP	20A
H8B53A	3	DP	20A
H8B54A	0	—	—
H8B55A	6	DP	20A
H8B56A	6	DP	20A

NOTE SP = Single Pole; DP = Double Pole
Each PDU has one branch-rated circuit breaker for over-current and short circuit protection on each output load segment. The breaker opens each current carrying conductor (double pole), except for line-to-neutral wiring schemes, where single-pole circuit breakers are used on the "hot" conductor only. The breakers meet the requirement of UL489 for the U.S. and IEC/EN 60934 for Europe.

Environmental and Safety

Table 22 lists the environmental specifications for all MA PDU models.

Table 22. Environmental Specifications (All PDU Models)

Operating Temperature (Room Ambient)	0°C to 50°C (32°F to 122°F) for INTL and WW models with outlet derating 0°C to 60°C (32°F to 140°F) on all other NA/JPN models (except as noted previously)
Shipping and Storage Temperature	Transit: -30°C to 60°C (-22°F to 140°F) (up to 72 h) Storage: -20°C to 60°C (-4°F to 140°F)
Relative Humidity	5–95% relative humidity
Operating Altitude	Up to 3,048m (10,000 ft) above sea level (derated for higher altitude applications)
Shipping and Storage Altitude	Up to 12,200m (40,000 ft) above sea level

Table 23 lists safety information for all MA PDU models.

Table 23. Safety Specifications (All PDU Models)

Safety Conformance	UL 60950-1, CSA 60950-1, C22.2 No.29 & No.31 (CSA), IEC/EN 60950-1
Safety Conformance (Breakers and Outlets)	Outlets: UL 498, IEC 60320 Breakers: UL 489 for the U.S. and IEC/EN 60934 for Europe
EMC (Class A), North American, Japanese and WorldWide models	FCC 47 CFR 15, Subpart B: 2009; ICES-003; VCCI
EMC (Class A), International models	EN 55022: 2007; EN 55024: 1998 + A2: 2003; CISPR Publication 22 Class A: 2006 + 2008; EN 61000-3-2 and EN 61000-3-3 (if the input current is less than or equal to 16A) EN 61000-3-11 and EN 61000-3-12 (if the input current is greater than 16A) IEC 61000-4-2; IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, IEC 61000-4-11

Table 24 lists the safety standards and country agency certifications for the MA PDU models.

Table 24. Safety Standards and Country Agency Certification

Agency RMN *	Model	CE Mark EN 60950-1	cULus UL 60950-1 *and* FCC Part 15 Subpart B: 2009 *and* ICES-003 (EMC Canada)**	CB IEC 60950-1	VCCI	DEMKO	EAC	KC K 60950-1	ACMA	Ukraine
HSTNR-P049-1	H8B48A	—	•	•	•	—	—	—	—	—
HSTNR-P048-1	H8B49A	•	•	•	•	•	•	•	•	•
HSTNR-P049-2	H8B50A	—	•	•	•	—	—	—	—	—
HSTNR-P049-3	H8B51A	•	—	•	—	•	•	•	•	•
HSTNS-P050-2	H8B52A	—	•	•	•	—	—	—	—	—
HSTNS-P050-3	H8B53A	—	•	•	•	—	—	—	—	—
HSTNS-P050-1	H8B54A	•	—	•	—	•	•	•	•	•
HSTNS-P050-5	H8B55A	—	•	•	•	—	—	—	—	—
HSTNS-P050-6	H8B56A	—	•	•	•	—	—	—	—	—

* See "Regulatory Model Numbers" information that follows.

** CAN/CSA-CEI/IEC CISPR22-10

Regulatory Model Numbers

For regulatory compliance certifications and identification, MA PDUs have been assigned a unique RMN (Regulatory Model Number). The RMN is on the product nameplate label, along with all required approval markings and information. When requesting compliance information for this product, always refer to the RMN. The RMN is not the marketing name or model number of the product.

Chapter 11 Support and Other Resources

Before You Contact HP

Be sure to have the following information available before you call HP:

- Active Health System log (HP ProLiant Gen8 or later products)

Download and have available an Active Health System log for 3 days before the failure was detected. For more information, see the HP iLO 4 User Guide or HP Intelligent Provisioning User Guide on the HP website (http://www.hp.com/go/ilo/docs).

- Onboard Administrator SHOW ALL report (for HP BladeSystem products only)

For more information on obtaining the Onboard Administrator SHOW ALL report, see the HP website (http://www.hp.com/go/OAlog).

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Product identification number
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

HP Contact Information

For United States and worldwide contact information, see the Contact HP website (http://www.hp.com/go/assistance).

In the United States:

- To contact HP by phone, call 1-800-334-5144. For continuous quality improvement, calls may be recorded or monitored.
- If you have purchased a Care Pack (service upgrade), see the Support & Drivers website (http://www8.hp.com/us/en/support-drivers.html). If the problem cannot be resolved at the website, call 1-800-633-3600. For more information about Care Packs, see the HP website (http://pro-aq-sama.houston.hp.com/services/cache/10950-0-0-225-121.html).

HP Product QuickSpecs

For more information about product features, specifications, options, configurations, and compatibility, see the product QuickSpecs on the HP Product Bulletin website (http://www.hp.com/go/productbulletin).

Documentation Feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (mailto:docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.