Oracle® Rack Universal Power Distribution Unit User's Guide

Part No: E99009-01
May 2019

Oracle Rack Universal Power Distribution Unit User's Guide

Part No: E99009-01

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Référence: E99009-01

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation

- **Overview** – Describes how to install the hardware
- **Audience** – Technicians, system administrators, and authorized service providers
- **Required knowledge** – Advanced experience troubleshooting and replacing hardware

Product Documentation Library

Documentation and resources for this product and related products are available at `https://www.oracle.com/pls/topic/lookup?ctx=E85660-01`.

Feedback

Provide feedback about this documentation at `https://www.oracle.com/goto/docfeedback`.

Introduction

Oracle Universal HPDU is an intelligent horizontal power distribution unit (HPDU) with a vertical power strip (VPS) that allows you to monitor power in the data center.

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

The section includes the following topics:

APIPA and Link-Local Addressing

- The HPDU supports Automatic Private Internet Protocol Addressing (APIPA).
- With APIPA, the HPDU automatically configures a link-local IP address and a link-local host name when it cannot obtain a valid IP address from any DHCP server in the TCP/IP network.
- Only IT devices connected to the same subnet can access the HPDU using the link-local address/host name. Those in a different subnet cannot access it.
- After the HPDU can get a DHCP-assigned IP address, it stops using APIPA and the link-local address is replaced by the DHCP-assigned address.

Scenarios where APIPA applies:

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

Note - Configuration by connecting the HPDU to a computer using a network cable is an application of this scenario.

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

Link-local addressing:

- **IPv4 address** – Factory default is to enable IPv4 only. The link-local IPv4 address is 169.254.x.x/16, which ranges between 169.254.1.0 and 169.254.254.255.
- **IPv6 address** – A link-local IPv6 address is available only after you enable IPv6 on the HPDU.
- **Host name** – to access the HPDU instead of typing the link-local IP address. Type https://pdu.local.

HPDU Components Overview

The HPDU hardware contains the following components on the outer panels.

- "Specifications" on page 18
- "Outlets" on page 19
- "Inlet" on page 19
- "Connection Ports and Front Panel LCD Display" on page 19
- "Automatic and Manual Modes" on page 20
- "Showing the Firmware Upgrade Progress" on page 29

Specifications

This section includes the following specifications:

- "Maximum Ambient Operating Temperature" on page 18
- "Serial RS-232 RJ-45 Port Pinouts" on page 18

Maximum Ambient Operating Temperature

The maximum ambient operating temperature for the HPDU is 60 degrees Celsius.

Serial RS-232 RJ-45 Port Pinouts

The following table describes the serial RS-232 RJ-45 pin signal and direction.

Pin No.	Signal	Direction	Description
1	RTS	Output	Request to send
2	DTR	Output	Data terminal ready
3	TxD	Output	Transmit data
4	GND	N/A	Signal ground
5	DCD	Input	Data
6	RxD	Input	Receive data (data in)
7	DSR	Input	Data set ready
8	CTS	Input	Clear to send

Outlets

Standard C13 and C19 outlets are provided on the vertical power strip (VPS).

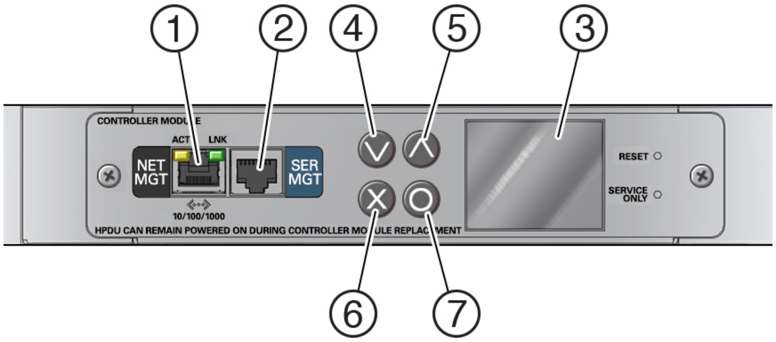
Inlet

Use the inlet to connect the input cord to the HPDU. The HPDU input cord is detachable and as either a low-voltage (LV) 208V Delta 60A version or a high-voltage (HV) 240V Wye 30/32A version.

Note - There is no power switch on the HPDU.

Connection Ports and Front Panel LCD Display

On the controller module, the connection ports allow you to connect the HPDU to your computer. You can use the LCD display on the front panel to view the HPDU information.



Callout	Description
1	NET MGT port for Ethernet connection
2	SER MGT port for RS-232 connection
3	LCD display
4	Down arrow button (V) moves the selection bar down in the menu
5	Up arrow button (/\) moves the selection bar up in the menu
6	Back button (X) moves to the previous selection or switches between Automatic and Manual modes
7	OK button (O) confirms what you select and continues with the operation

Automatic and Manual Modes

After powering on or resetting the HPDU, the front panel LCD displays dots and a logo, and enters Automatic mode. In Automatic mode, the display cycles through the inlet and breaker information when there are no alerts. In Manual mode, the display changes so that you can navigate the menus and alerts.

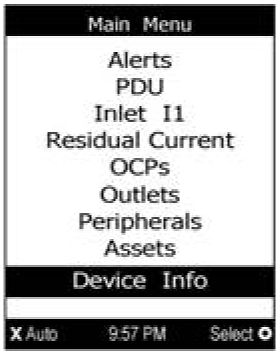
▼ Operating the LCD Display

1. **Press OK or X to enter Manual mode, where the Main menu displays.**
2. **Use the Control buttons to operate the display.**
3. **To return to Automatic mode, press X.**

Main Menu

The Main Menu contains menu commands that vary, depending on the HPDU model.

To select a menu command, press the Up or Down arrow button in the Main menu, and press OK. To return to the Main menu, press X.



Main Menu Command	Function
Top Bar	Shows current menu name or alert.
Alerts	Indicates all alerted sensors, if any.
PDU	Shows internal beeper states, total active HPDU power, total active HPDU energy, and 12V power supply status.
Inlet I1	Shows the inlet I1 information.
Residual Current	Shows a list of overcurrent protector information.
OCPs	Back control button or switch between Automatic and Manual modes
Device Info	Shows the HPDU information, such as IP and MAC address.
Bottom Bar	Shows Auto or Manual mode, current time, and Select with OK button to select a menu command.

Alerts

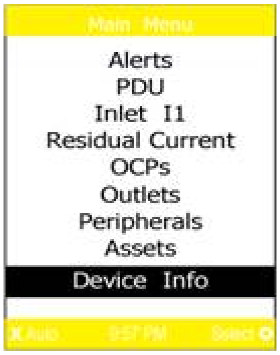
When an alert occurs, the display stops cycling through the inlet information, and warns you by showing the alerts notice with yellow or red top and bottom bars in the Main Menu. The alerts appear in Automatic or Manual mode.

In Automatic mode, if an alert occurs, the LCD display automatically shows a yellow or red screen which indicates the total number of alerted sensors and information of the latest transitions.

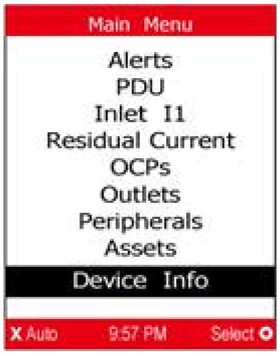
- When all alerted sensors enter the warning levels, the screen background is yellow.
- When at least one of the alerted sensors enters the critical level, the screen background is red.

In Manual mode, both the top and bottom bars are yellow or red to indicated the presence of any alert.

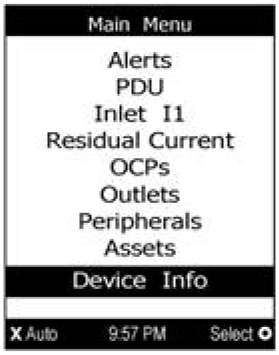
- **Yellow bars** – Indicate a warning.



- **Red bars** – Indicate a critical warning.



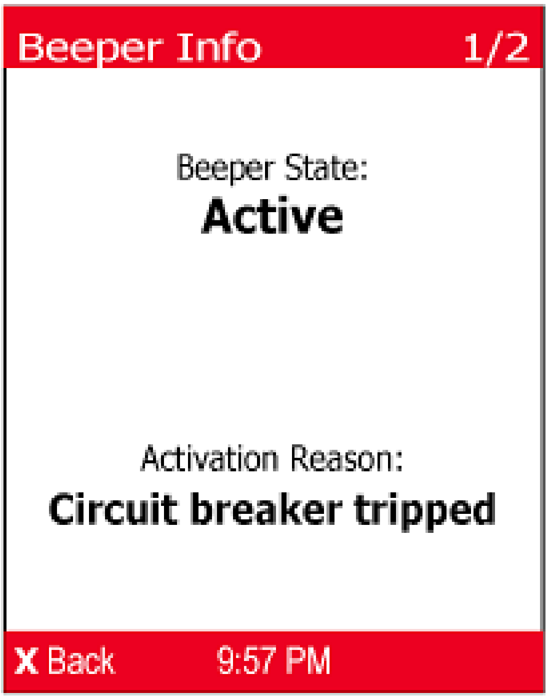
- **Black bars** – Indicate there are no alerts.



PDU

The PDU menu command shows one or all of the following information.

- Internal beeper states – Active or Off. In the Active state, the reason for turning on the beeper is indicated, and the top and bottom bars are red.



Beeper Info 1/2

Beeper State:
Active

Activation Reason:
Circuit breaker tripped

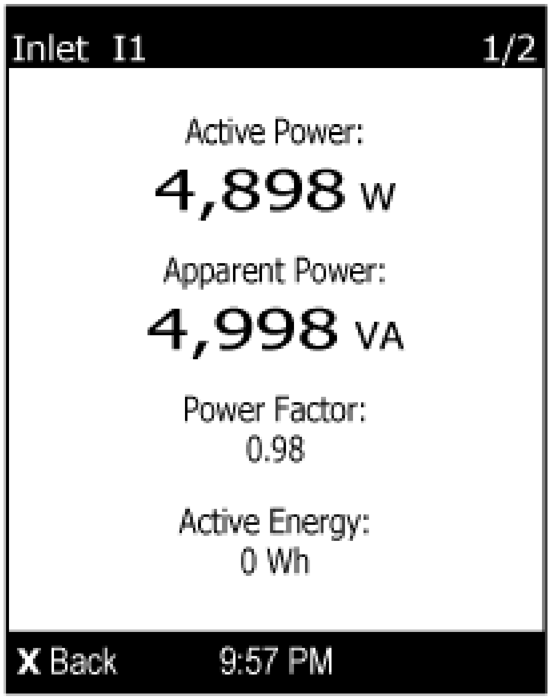
Note - The internal beeper state information is also available in the web interface Dashboard.

- Total active power of the HPDU – Available only on multi-inlet models and in-line monitors
- Total active energy of the HPDU – Available only on multi-inlet models and in-line monitors
- 12V power supply status

Inlet

The inlet information is organized into two pages. Page numbers appear in the upper right corner of the display. To view other pages, press the Up or Down arrow buttons.

The first page shows the inlet's active power (W), apparent power (VA), power factor (PF), and active energy (Wh).



Inlet I1 1/2

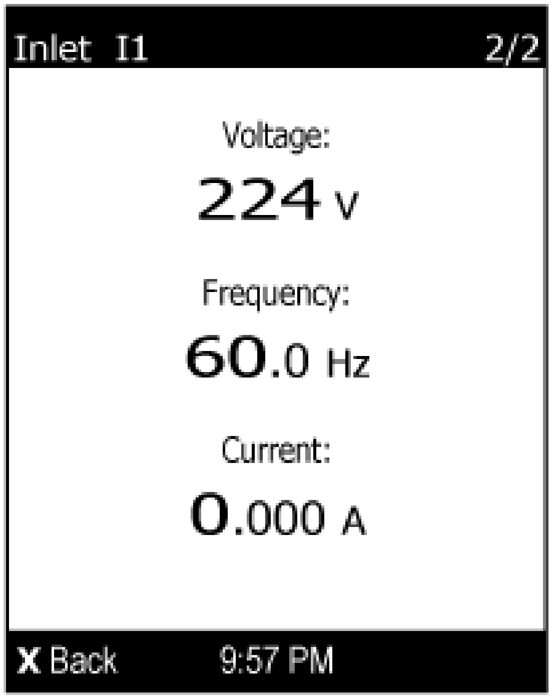
Active Power:
4,898 W

Apparent Power:
4,998 VA

Power Factor:
0.98

Active Energy:
0 Wh

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



Inlet I1 2/2

Voltage:

224 V

Frequency:

60.0 Hz

Current:

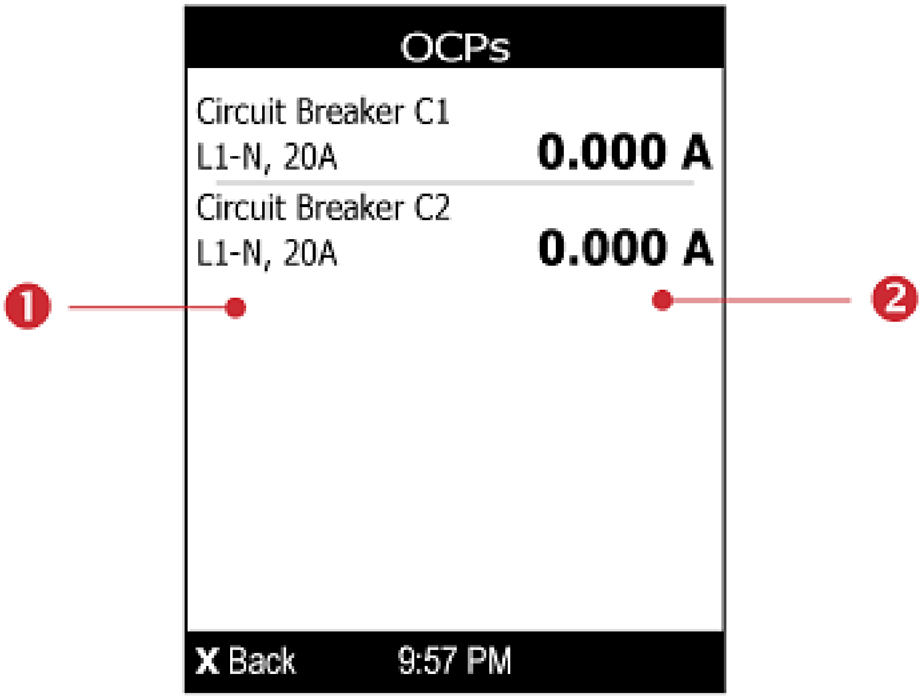
0.000 A

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

OCPs

Depending on the OCPs in the HPDU, the ICPs list is similar to following example list.

.



OCPs

Circuit Breaker C1
L1-N, 20A 0.000 A

Circuit Breaker C2
L1-N, 20A 0.000 A

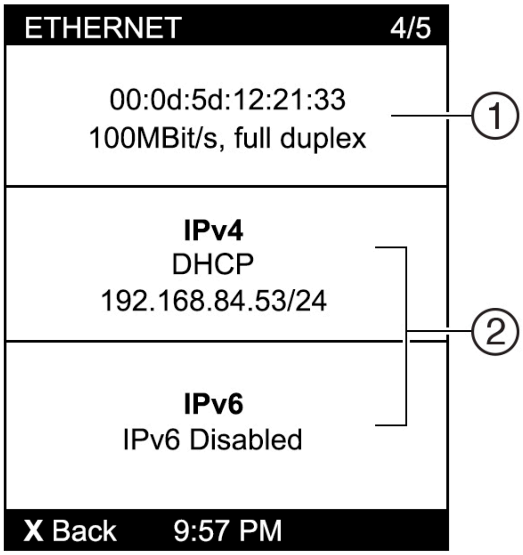
X Back 9:57 PM

Note - If your HPDU model has multiple overcurrent protectors (OCPs) and appears on multiple pages, a page number appears in the upper-right corner of the top bar. Otherwise, no page numbers appear. If the overcurrent protector you want to view is not visible, press the Up or Down arrow buttons to scroll up or down.

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

Note - If any circuit breaker trips, the list of overcurrent protectors looks slightly different from the above illustration. The tripped one shows as Open instead of a current reading.

To view the ETHERNET page, press the Down arrow button.



ETHERNET 4/5

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

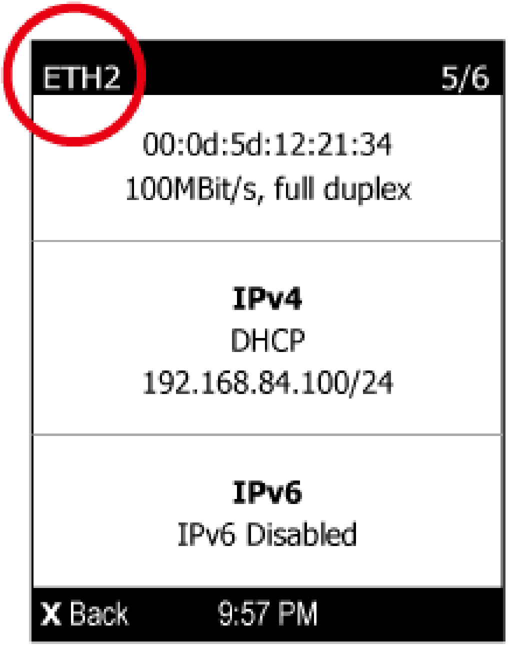
IPv4
DHCP
192.168.84.53/24

IPv6
IPv6 Disabled

X Back 9:57 PM

Callout	Description
1	Ethernet interface information ■ MAC address ■ Speed ■ Full or half duplex
2	IPv4/IPv6 network information ■ Network configuration: DHCP (or Automatic), or Static. Static represents Static IP ■ IP address ■ Prefix length, such as /24 **Note -** If you disable any Ethernet interface, the Interface Disabled message displays. If you do not enable IPv4/IPv6 settings, the IPv4 (or IPv6) Disabled message displays.

For the HPDU, there are two Ethernet pages -- ETH1 and ETH2.

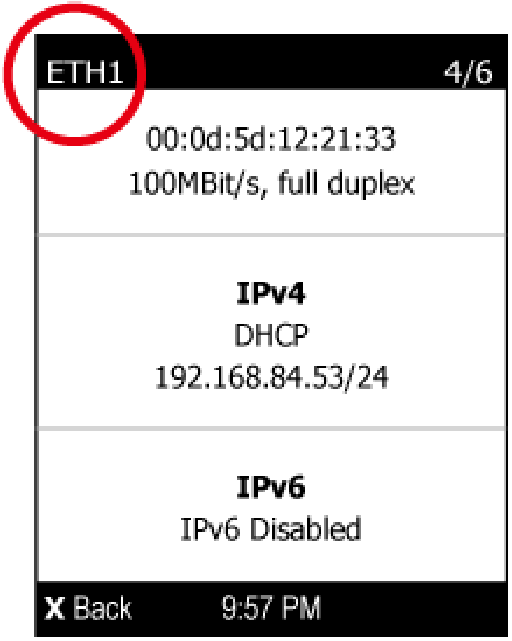


ETH2 5/6

00:0d:5d:12:21:34
100MBit/s, full duplex

IPv4
DHCP
192.168.84.100/24

IPv6
IPv6 Disabled



ETH1 4/6

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

IPv4
DHCP
192.168.84.53/24

IPv6
IPv6 Disabled

Showing the Firmware Upgrade Progress

When upgrading the HPDU, the firmware upgrade progress displays as a percentage on the display. At the end of the upgrade process, a message appears, indicating whether the firmware upgrade succeeds or fails.

Preparing for Installation

The HPDUs are designed exclusively for the Oracle Rack Cabinet family of rack cabinets. Install the HPDUs into the Oracle Rack Cabinet before installing other equipment. For information about installing equipment into the cabinets, see the *Oracle Rack Cabinet User's Guide*.

- "Safety Notices" on page 31
- "Pre-Installation Activities" on page 36
- "Tools" on page 37
- "Attach an Antistatic Wrist Strap" on page 38

Safety Notices

Caution - Read and understand all sections in this guide before installing or operating this product.

Caution - Connect this product to an AC power source whose voltage is within the range specified on the product nameplate. Operating this product outside the nameplate voltage range may result in electric shock, fire, personal injury, and death.

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

Caution - Connect this product to a protective earth ground. Never use a "ground lift adaptor" between the product's plug and the wall receptacle. Failure to connect to a protective earth ground may result in electric shock, fire, personal injury, and death.

Caution - With the exception of the controller module (see "Replace a Controller" on page 263), this product contains no user serviceable parts. Do not open, alter or disassemble this product. All servicing must be performed by qualified personnel. Disconnect power before servicing this product. Failure to comply with this warning may result in electric shock, personal injury, and death.

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

Caution - Only use this product to power information technology equipment that has a UL/ IEC 60950-1 or equivalent rating. Attempting to power non-rated devices may result in electric shock, fire, personal injury, and death.

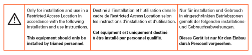
Caution - Do not use this product to power critical patient care equipment, fire or smoke alarm systems. Use of this product to power such equipment may result in personal injury and death.

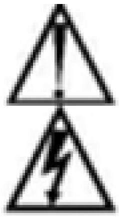
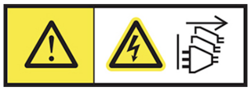
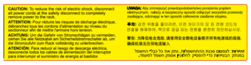
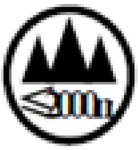
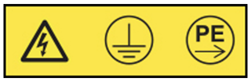
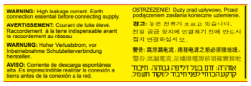
Caution - If this product is a model that requires assembly of its line cord or plug, all such assembly must be performed by a licensed electrician and the line cord or plugs used must be suitably rated based on the product's nameplate ratings and national and local electrical codes. Assembly by unlicensed electricians or failure to use suitably rated line cords or plugs may result in electric shock, fire, personal injury, or death.

Caution - This equipment is not suitable for use in locations where children are likely to be present.

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

The following table contains safety warning labels to ensure proper use of the HPDU.

Safety Warning	Warning Label
Trained personnel restricted installation	 ⚠ Only for installation and use in a Restricted Access Location in accordance with the following installation and use instructions. **This equipment should only be installed by trianed personnel.** Destiné à l'installation et l'utilisation dans le cadre de Restricted Access Location selon les instructions d'installation et d'utilisation. **Cet équipment est uniquement destiné à être installé par personnel qualifié.** Nur für installation und Gebrauch in eingeschränkten Betriebszonen gemaß der folgenden installations- und Gebrauchsabweisungen. **Dieses Gerät ist nur für den Einbau durch Persoanl vorgesehen.**

Safety Warning	Warning Label
Electric shock hazard – The mains appliance inlet and interconnecting cable are not for current interruption or disconnection under load. Always disconnect the power supply cord before servicing to avoid electrical shock.	
Multiple power source	
Disconnect devices	 **CAUTION:** To reduce the risk of electric shock, disconnect all power cords at the safety disconnect to completely remove power to the rack. **ATTENTION:** Pour réduire les risques de décharge électrique, débranchez tous les cordons d'alimentation au niveau du sectionneur afin de mettre l'armoire hors tension. **ACHTUNG:** Um die Gefahr von Stromschlägen zu vermeiden, ziehen Sie alle Netzkabel am Sicherheitstrennschalter ab, um die Stromzufuhr zum Rack vollständig zu unterbrechen. **ATENCIÓN:** Para reducir el riesgo de descarga eléctrica, desconecte todos los cables de alimentación del interruptor para interrumpir el suministro de energía al bastidor. **UWAGA:** Aby zmniejszyć prawdopodobieństwo porażenia prądem elektrycznym, należy w bezpieczny sposób odłączyć wszystkie przewody zasilające, odcinając w ten sposób całkowicie zasilanie stojaka. **주의:** 감전 위험을 줄이려면, 안전 차단기의 모 든 전원 코드의 연결을 해제하여, 랙으로 공급 되는 전원을 완전히 차단하십시오. 警告: 为降低电击危险，请使用安全断电设备断开所有电源线的连接，确保机架无任何电流输入 **זהירות:** לצמצום סכנת ההתחשמלות, נתק את כל כבלי החשמל במנתק הבטיחות כדי להפסיק לחלוטין אספקת חשמל למעמד.
For use in altitude 2,000 meters or less	
Protective conductor current	
High leakage current	 **WARNING:** High leakage current. Earth connection essential before connecting supply. **AVERTISSEMENT:** Courant de fuite élevé. Raccordement à la terre indispensable avant le raccordement au réseau **WARNUNG:** Hoher Verluststrom, vor Inbetriebnahme Schutzleiterverbindung herstellen. **AVISO:** Corriente de descarga esportánea alta. Es imprescindible realizar la conexión a tierra antes de la conexión a la red. OSTRZEZENIE! Duży prąd upływowy. Przed podłączeniem zasilania konieczne uziemienie. **경고:** 높은 전류가 흐르고 있습니다. 전원 공급 장치에 연결하기 전에 반드시 접지 연결하십시오. 警告: 高泄漏电流，连接电源之前必须接地线。 警告:高漏電流,在連接電源前須確實接地 אזהרה: זרם בעל זליגה גבוהה. חיבור קרקע הכרחי לפני חיבור למקור חשמל.

Safety Instructions

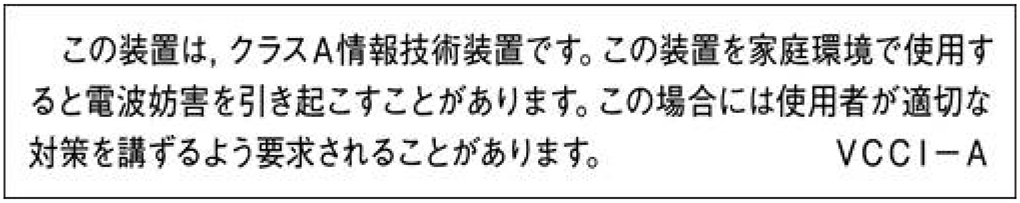
- Installation of this product should only be performed by a person who has knowledge and experience with electric power.
- Ensure the line cord is disconnected from power before physically mounting or moving the location of this product.
- This product is designed to be used within an electronic equipment rack. The metal case of this product is electrically bonded to the line cord ground wire. A threaded grounding point on the case may be used as an additional means of protectively grounding this product and the rack.

- Examine the branch circuit receptacle that will supply electric power to this product. Make sure the receptacle’s power lines, neutral and protective earth ground pins are wired correctly and are the correct voltage and phase. Make sure the branch circuit receptacle is protected by a suitably rated fuse or circuit breaker.

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)



この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　VCCI－A

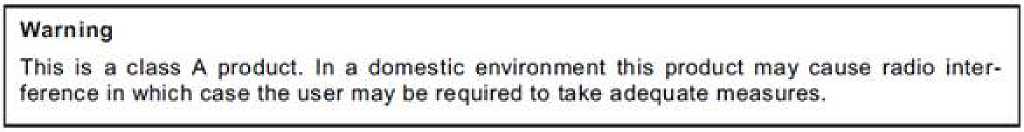
The manufacturer is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, modification of the product, or other events outside of the manufacturer’s reasonable control or not arising under normal operating conditions.

If a power cable is included with this product, it must be used exclusively for this product.

CE

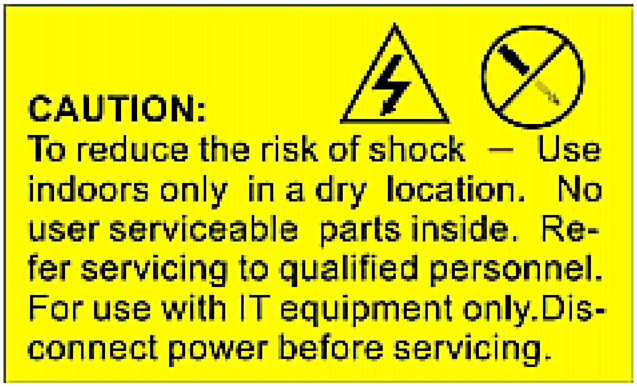
c UL US
LISTED

1F61
I.T.E.



Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.



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

ESD Precautions

Electronic equipment is susceptible to damage by static electricity. Use a grounded antistatic wrist strap, footstrap, or equivalent safety equipment to prevent electrostatic damage when you install or service the server.

Caution - To protect electronic components from electrostatic damage, which can permanently disable the server or require repair by service technicians, place components on an antistatic surface, such as an antistatic discharge mat, an antistatic bag, or a disposable antistatic mat. Wear an antistatic grounding strap connected to a metal surface on the chassis when you work on server components.

Electromagnetic Compatibility Notifications

Electromagnetic (EMC) Notification	Description	Standard Number	Standard Clause
European Notification		EN 55032, CISPR 32	EN 55032, cl. 7

Electromagnetic (EMC) Notification	**Description**	**Standard Number**	**Standard Clause**
	This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference. European Notification Section Warning: This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.		
Canadian Notification	This Class A digital apparatus complies meets all requirements of the Canadian Interference-Causing Equipment Regulations. Cet appareil numérique de la classe A respecte toutes les exigencies du Règlement sur le matériel brouilleur du Canada.	IC (Industry Canada)	
Republic of Korea Notification	이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다	KN 32	KN 32 2015-12, cl. 7

Electronic equipment is susceptible to damage by static electricity. Use a grounded antistatic wrist strap, footstrap, or equivalent safety equipment to prevent electrostatic damage when you install or service the server.

Caution - To protect electronic components from electrostatic damage, which can permanently disable the server or require repair by service technicians, place components on an antistatic surface, such as an antistatic discharge mat, an antistatic bag, or a disposable antistatic mat. Wear an antistatic grounding strap connected to a metal surface on the chassis when you work on server components.

Pre-Installation Activities

Before you install the rack, perform the following activities:

- "Unpacking the Product and Components" on page 37
- "Preparing the Installation Site" on page 37

- “Checking the Branch Circuit Rating” on page 37

▼ Unpacking the Product and Components

1. **Remove the HPDU device and VPS from the box in which they were shipped.**
2. **Compare the serial number of the equipment with the number on the packing slip located on the outside of the box and verify that they match.**
3. **Inspect the equipment carefully. If any of the equipment is damaged or missing, contact Oracle Support at `https://support.oracle.com`.**

▼ Preparing the Installation Site

1. **Make sure the installation area is clean and free of extreme temperatures and humidity.**
2. **Allow sufficient space around the HPDU device for cabling and outlet connections.**
3. **Review the “Safety Notices” on page 31.**

Checking the Branch Circuit Rating

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

Tools

Prior to installing a HPDU into your rack, prepare the work area and assemble the following tools:

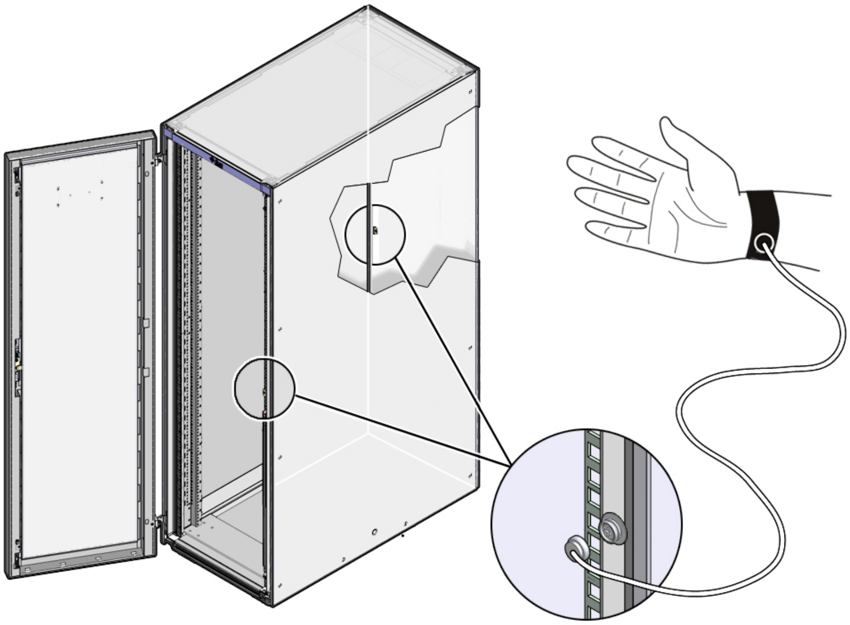
- Torx T25 screwdriver (included in the rack shipping kit)
- HPDU and VPS mounting brackets, M5 thread forming screws, and cage nuts (included in the HPDU mount shipping kit)

You also must supply:

- Antistatic wrist strap
- Clean work table, or area, near the rack

▼ Attach an Antistatic Wrist Strap

- **Attach a wrist strap to your wrist and to the ESD grounding jack on the rear rail of the rack.**



Installing HPDUs In To an Oracle Rack

Always install the HPDUs prior to installing equipment into the rack. Complete these tasks to install the HPDU and connect it to the installation site AC power source.

- "Install a HPDU In To an Oracle Rack Cabinet 1242" on page 39
- "Install a HPDU In To an Oracle Cloud II Rack" on page 45
- "Connect the HPDU to the AC Power Source" on page 50
- "Powering on the Equipment" on page 53

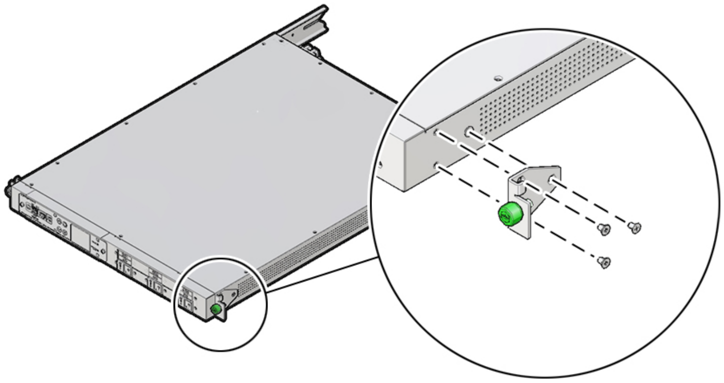
▼ Install a HPDU In To an Oracle Rack Cabinet 1242

Install two HPDUs and two Vertical Power Strips (17KVA VPS) into the Oracle Rack Cabinet 1242.

1. **Unpack the HPDUs from the packaging and place them on a clean work table.**

2. **Remove the brackets and screws from the HPDU mount shipping kit.**

3. **Secure the left and right mounting brackets on the front of each HPDU using three M4 screws per bracket.**



4. **Secure the mounting brackets with the cage nuts on the left and right RETMA rails at the back of the rack.**

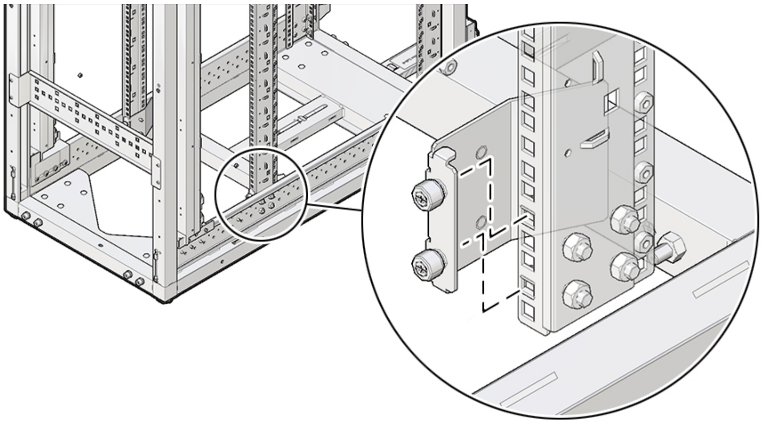
   a. **Using your equipment rack alignment template, or other equipment documentation, locate the second and fifth rail holes from the bottom.**

   Note - Use the cage nut insertion tool in the ship kit to install the cage nuts in the rails.

   b. **Align the cage nut with the square rail hole.**

   c. **Hook the side lip of the nut in the square rail hole.**

d. **Insert the tip of the cage nut insertion tool through the rail hole, hook the other side lip of the cage nut, and lever the cage nut into place.**



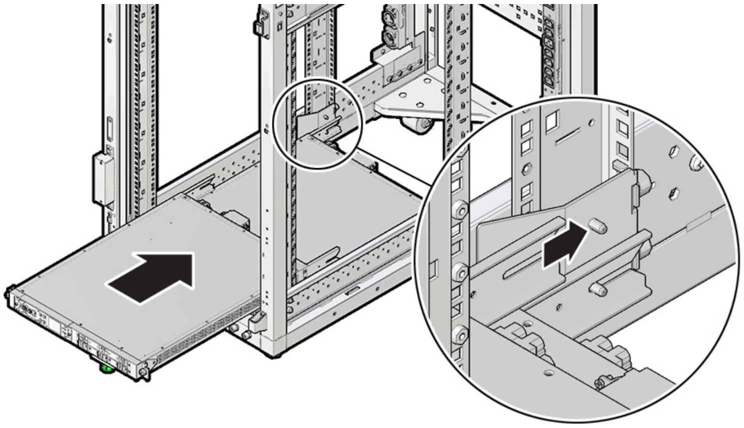
5. **Install both HPDUs.**

   a. **Slide a HPDU on the bottom of the rack from the front until the bracket catches in the square rail hole on the left and right sides of the rack.**

   b. **Verify that the HPDU slot engages the pin on the rear bracket.**

   c. **Slide the second HPDU on top of the first HPDU until it catches in the square rail hole on the left and right sides of the rack.**

d. **Verify that the slot of the second HPDU engages the pin on the rear bracket.**



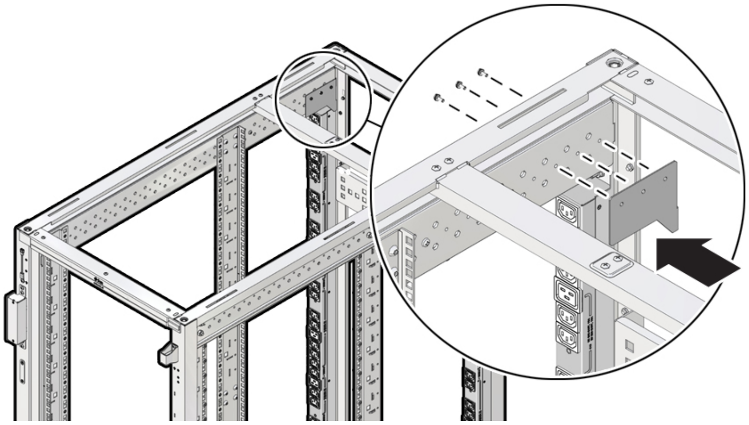
6. **In the VPS shipping kit, remove the brackets and the screws and install the VPS using the Torx T25 screwdriver.**

   a. **From the back of the cabinet, secure the top left bracket (7364703) with the stud facing the front of the rack, and the right-angle flange faces the left side of the rack, the first and third hole of the center row of holes.**

   b. **From the back of the cabinet, secure the bottom left bracket (7364704) with the stud facing the front of the rack, and the right-angle flange faces the left side of the rack, the first and third hole of the center row of holes.**

   c. **From the back of the cabinet, secure the top right bracket (7364703) with the stud facing the front of the rack, and the right-angle flange faces the right side of the rack, the first and third hole of the center row of holes, the first and third hole of the center row of holes.**

d. **From the back of the cabinet, secure the bottom right bracket (7364704) with the stud facing the front of the rack, and the right-angle flange faces the right side of the rack, starting in the first hole of the center row of holes.**

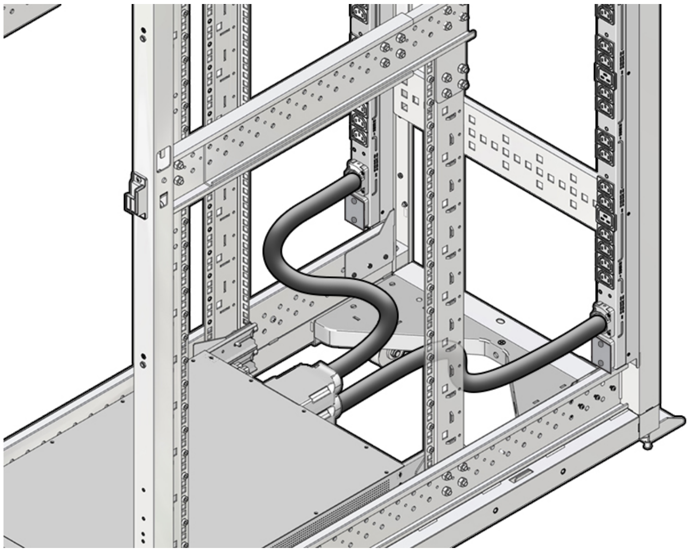


7. **Install both VPS's.**

   a. **At the back of the rack, with the PDU power cable at the bottom of the VPS, which faces the front of the rack, on the left side, align the slots at the top and bottom of the VPS with the M6 studs.**

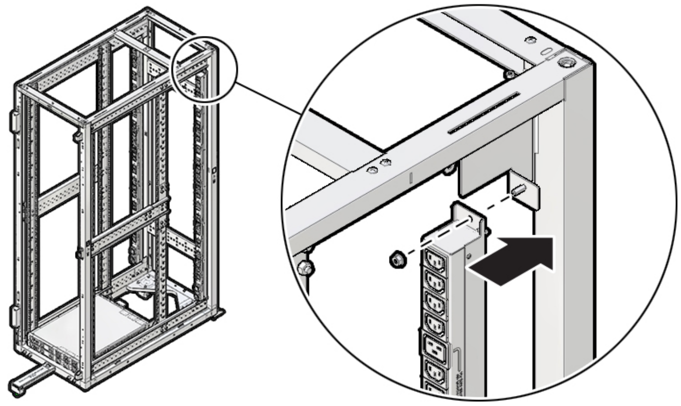
   b. **Slide the VPS into place, and using the M10 nut driver, secure the VPS with the M6 hex nuts.**

c. **Snake the HPDU power cable down and forward toward the bottom HPDU, and loop the cable to the back of the rack.**



d. **Slide the cable into the output connector, and secure it with M4 screws using a #2 Philips screwdriver, and torque to 15 in-lbs (1.7 Nm).**

e. **Repeat Steps 7a-d to install the other VPS on the right side and connect it to the top HPDU.**



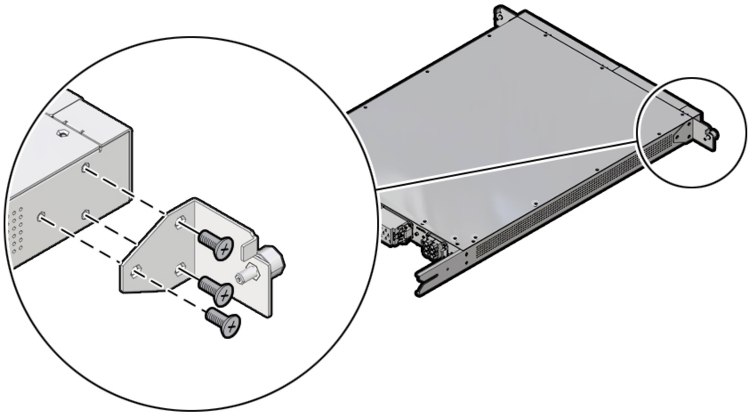
Note - For a 34KVA installation, connect the left VPS lower power cable to the HDPU1 connector, the left VPS upper power cable to the HPDU2 connector, the right VPS lower power cable to the HPDU3 connector, and the right VPS upper power cable to the HPDU4 connector.

▼ Install a HPDU In To an Oracle Cloud II Rack

Install two HPDUs and two Vertical Power Strips (17KVA VPS) into an Oracle Cloud II Rack.

1. **Unpack the HPDUs from the packaging and place them on a clean work table.**
2. **Remove the brackets and screws from the HPDU mount shipping kit.**

3. **Secure the left and right mounting brackets on the front of each HPDU using three M4 screws per bracket.**



4. **Secure the mounting brackets with the cage nuts on the left and right RETMA rails at the back of the rack.**

   a. **Using your equipment rack alignment template, or other equipment documentation, locate the second and fifth rail holes from the bottom.**

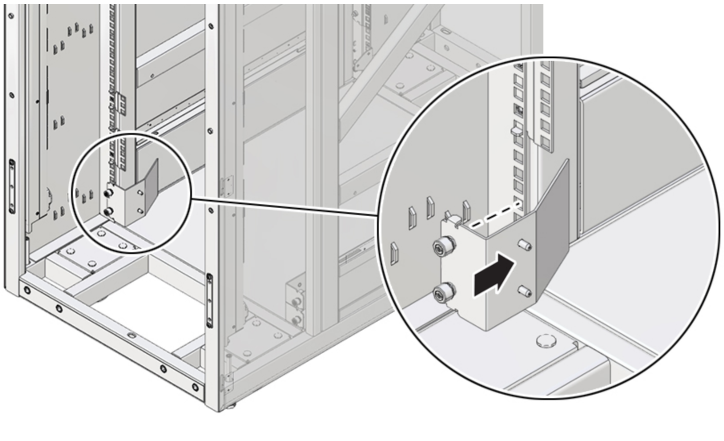
Note - Use the cage nut insertion tool in the ship kit to install the cage nuts in the rails.

---

   b. **Align the cage nut with the square rail hole .**

   c. **Hook the side lip of the nut in the square rail hole.**

d. **Insert the tip of the cage nut insertion tool through the rail hole, hook the other side lip of the cage nut, and lever the cage nut into place.**



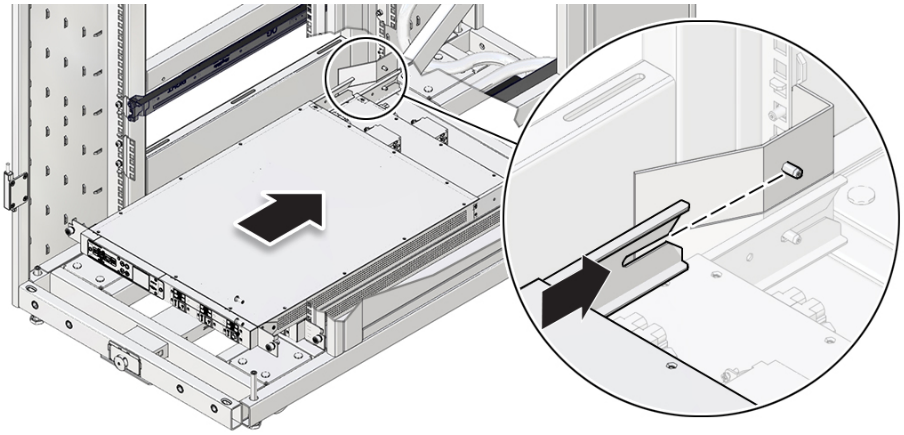
5. **Install both HPDUs.**

   a. **Slide a HPDU on the bottom of the rack from the front until the bracket catches in the square rail hole on the left and right sides of the rack.**

   b. **Verify that the HPDU slot engages the pin on the rear bracket.**

   c. **Slide the second HPDU on top of the first HPDU until it catches in the square rail hole on the left and right sides of the rack.**

d. **Verify that the slot of the second HPDU engages the pin on the rear bracket.**

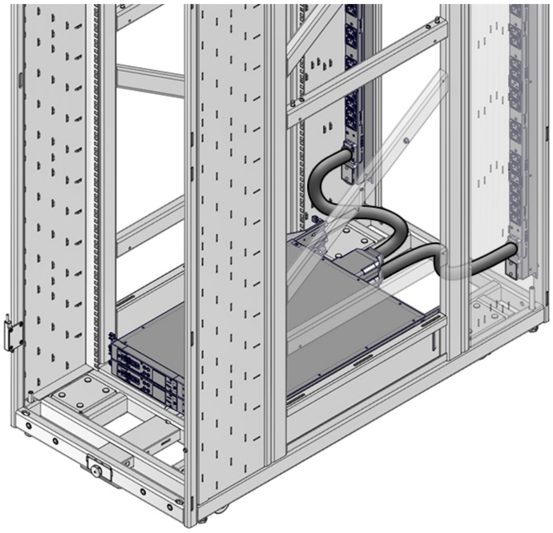


6. **Install both VPS's.**

   a. **At the back of the rack, with the PDU power cable at the bottom of the VPS, which faces the front of the rack, on the left side, align the slots at the top and bottom of the VPS with the M6 studs.**

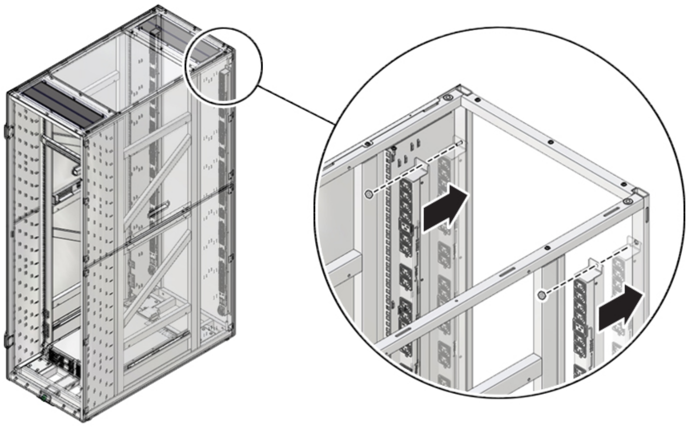
   b. **Slide the VPS into place, and using the M10 nut driver, secure the VPS with the M6 hex nuts.**

c. **Snake the HPDU power cable down and forward toward the bottom HPDU, and loop the cable to the back of the rack.**



d. **Slide the cable into the output connector, and secure it with M4 screws using a #2 Philips screwdriver, and torque to 15 in-lbs (1.7 Nm).**

e. **Repeat Steps 6a-d to install the other VPS on the right side and connect it to the top HPDU.**



Note - For a 34KVA installation, connect the left VPS lower power cable to the HDPU1 connector, the left VPS upper power cable to the HPDU2 connector, the right VPS lower power cable to the HPDU3 connector, and the right VPS upper power cable to the HPDU4 connector.

Connect the HPDU to the AC Power Source

Before connecting the HPDU to the AC power source, determine your type of HPDU for the locations of the circuit breakers.

- "Resetting a Circuit Breaker" on page 50
- "Connecting the Input Cord and To a Power Source" on page 52
- "Connecting the HPDU to Your Network" on page 53
- "Powering on the Equipment" on page 53

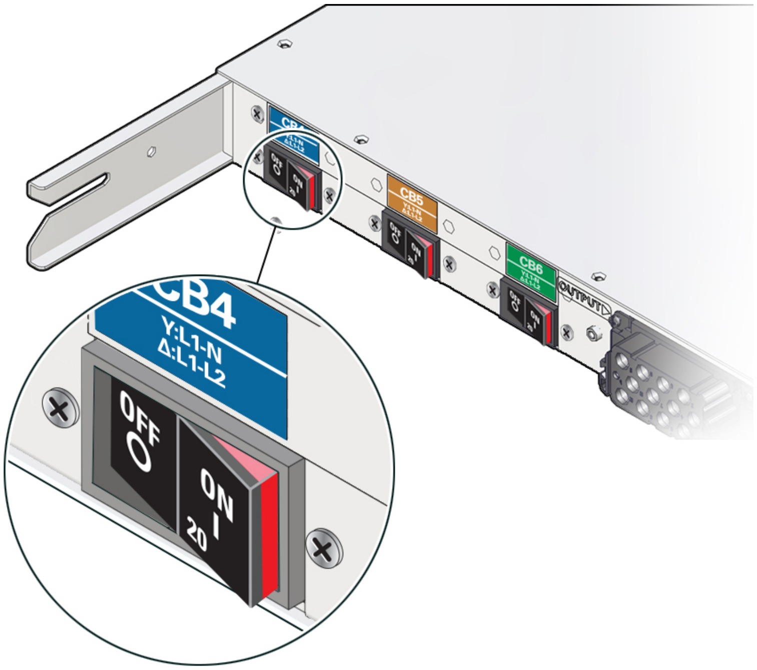
▼ Resetting a Circuit Breaker

The circuit breakers automatically trip (disconnect power) when the current flowing through the circuit breaker exceeds its rating. If a circuit breaker switches off power, the LCD display shows as open. To find which circuit breaker is open (tripped), in the Main Menu, select Alerts or OCPs.

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

Depending on the model you purchased, the circuit breaker uses a button or handle reset mechanism.

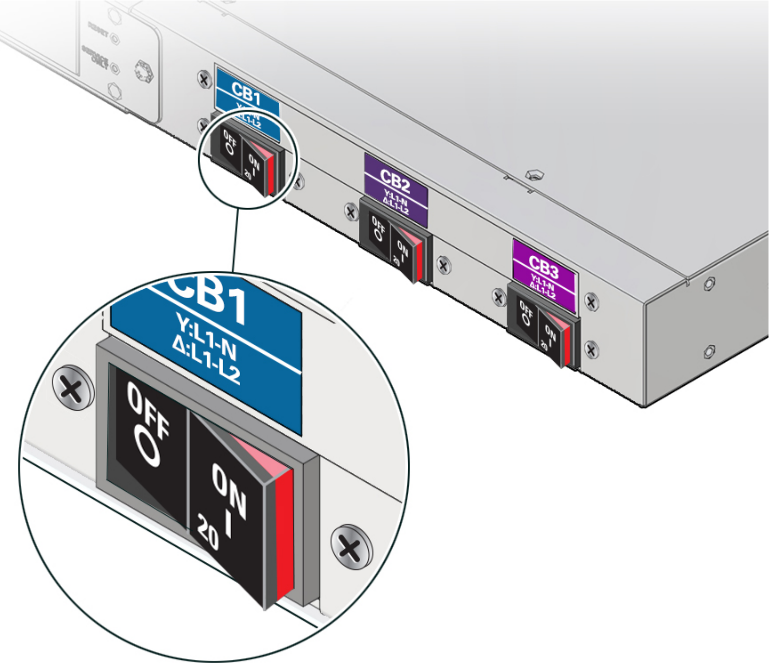
1. **Locate the circuit breakers in the back of the HPDU. For example, the following figure shows the three circuit breaker buttons at the back of the HPDU are set to OFF.**



2. **If there is an overload or short circuit, examine the HPDU and the connected equipment to remove or resolve the cause of issue. This step is required, or you cannot proceed with the next step.**

Caution - To prevent injury and equipment damage, always determine the cause of a tripped circuit breaker before resetting it.

3. **Press the OFF button until it is completely depressed on the circuit breakers in the front and back of the HPDU.**



Connecting the Input Cord and To a Power Source

1. **Secure the input cord to the HPDU by using the captive screws with a #2 Philips screwdriver and torque to 15 in-lbs (1.7 Nm).**

2. **Connect the other end of the input cord to an appropriately rated branch circuit.**

Note - For the input ratings or range of ratings, refer to the label or nameplate on the HPDU input power cable.

3. **Set all circuit breakers to ON.**

4. **To power cycle the HPDU, unplug it from the branch circuit, wait 10 seconds, and plug it back in.**

When the device powers up, a power-on self test runs and software loads for a few minutes.

When the software finishes loading, the front panel display illuminates.

▼ Connecting the HPDU to Your Network

1. **Verify that the Ethernet port of the HPDU is enabled for the connection to work properly.**

   Note - By default, the Ethernet port is enabled. See "Configuring Wired Network Settings" on page 88.

2. **To make a wired connection, connect a standard network patch cable to the SER MGT port on the HPDU.**

   ⚠ **Caution -** Accidentally plugging an RS-232 RJ-45 connector into the ETHERNET port can cause permanent damage to the Ethernet hardware.

3. **Connect the other end of the cable to the LAN.**

▼ Powering on the Equipment

- **Power on all the equipment in the rack.**

  For details about power-on procedures, refer to the equipment documentation.

Initial Configuration

This section explains how to connect an HPDU device and configure it for network connectivity.

- "Configuring the HPDU" on page 55
- "Connecting the HPDU to a Computer" on page 56
- "RJ45-to-DB9 Cable Requirements for Computer Connections" on page 57

Configuring the HPDU

You can initially configure the HPDU in either of two ways:

- TCP/IP network that supports DHCP
- Computer physically connected to the HPDU

▼ Configuring the HPDU through a DHCP Enabled Network

1. **Connect the HPDU to a DHCP IPv4 network.**
2. **Retrieve the DHCP-assigned IPv4 address by using the front panel display.**
3. **Launch a web browser to configure the HPDU.**

▼ Configuring the HPDU through a Connected Computer

1. **Connect the HPDU to a computer.**

Note - To configure multiple HPDU devices quickly, see "Bulk Configuration Methods" on page 154.

2. **To use the command line interface for configuration, see "Configure the HPDU Device and Network" on page 190.**

3. **To use the web interface for configuration, follow these steps.**

   a. **Launch the web browser on the computer.**

   b. **To access the HPDU, type the link-local IP address or pdu.local.**

Connecting the HPDU to a Computer

You can connect the HPDU to a computer for configuration in either of the following ports:

- NET MGT port
- SER MGT port

To use the command line interface (CLI) for configuration, establish an RS-232 connection.

To use the web interface for configuration, connect to the network on your computer. The HPDU is automatically configured with the following link-local addressing in any network without DHCP available. See "APIPA and Link-Local Addressing" on page 17

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

Establish one of the following connections to a computer. The NET MGT port of the HPDU must be enabled for the connection to work properly. By default, the NET MGT port is enabled.

▼ Connecting Directly to a Network

1. **Connect one end of a standard network patch cable to the ETHERNET port of the HPDU.**

2. **Connect the other end to a computer's Ethernet port.**

3. **On the connected computer, launch a web browser to access the HPDU, using either link-local addressing: `http://pdu.local` or `169.254.x.x`.**

▼ Connecting through a Serial Connection for RJ-45 RS-232 Connector

1. **Connect one end of the serial cable to the SER port on the HPDU and the other to the console port on your computer.**

Note - To configure multiple HPDU devices quickly, see "Bulk Configuration Methods" on page 154.

2. **See "RJ45-to-DB9 Cable Requirements for Computer Connections" on page 57.**

3. **"Configure the HPDU Device and Network" on page 190.**

RJ45-to-DB9 Cable Requirements for Computer Connections

An RJ45-to-DB9 or RJ45 to USB adapter/cable may be required for connecting the HPDU to a computer,

A third party RJ45-to-DB9 adapter/cable needs to meet the following requirements.

- RJ-45 to DB9 female
- RX/TX and according control pins are CROSSED

The widespread blue Cisco RJ-45 to DB9 adapter cable is highly recommended, which has the following pin assignments:

DB9 Pin Signal	DB9 Pin No.	RJ-45 Pin No.	RJ-45 Pin Signal
CTS	8	1	RTS
DSR	6	2	DTR
RxD	2	3	TxD
GND	5	4	GND

DB9 Pin Signal	DB9 Pin No.	RJ-45 Pin No.	RJ-45 Pin Signal
GND	5	5	GND
TxD	3	6	RxD
DTR	4	7	DSR
RTS	7	8	CTS
DCD	1 (Not connected)	N/A	
RI	9 (Not connected)	N/A	

Web Interface

This section explains how to use the web interface to administer the HPDU.

Supported Web Browsers

Note - Depending on the browser, the Up and Down arrows might not appear in the numeric fields. Clicking these arrows adjusts numeric values by 1.

- Internet Explorer 11
- Microsoft Edge
- Firefox 52 and later
- Safari (Mac)
- Google Chrome 52 and later
- Android 4.2 and later
- iOS 7.0 and later

▼ Logging In to the Web Interface

1. **Enable JavaScript in the web browser for proper operation.**

   Note - The first time you log in to the HPDU, for the user name, type **Admin** and for the password, type **Adm1n** (factory default admin user credentials).

2. **Open a browser and type the IP address of the HPDU.**

   Note - If link-local addressing is enabled, type `pdu.local` instead of an IP address. You also can enter the page URL so that you can immediately go to that page after login.

3. **If a security alert message appears, accept it.**
4. **On the login screen, type your user name and password (case sensitive).**
5. **If a security agreement displays, accept it by selecting the agreement check box using the keyboard, and press Enter. Otherwise, you cannot log in.**
6. **Click Login or press Enter.**

▼ Changing Your Password

You need appropriate permissions to change your password. Users without permissions must change the password.

Note - A password change request also appears if the Force Password Change option is enabled in the user account setting.

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

To change other users' passwords, Administrator Privileges are required instead.

1. **On first login, if you have both the Change Local User Management and Change Security Settings permissions, you can either change your password or ignore it.**
2. **Type the new password and click OK.**
3. **Select one of the following options:**

- **Not Now** – Ignores the request for this time only.
- **Do not ask again** – Ignores the request permanently. If you select this option, click **Not Now**.

4. **To change your password:**

   a. **Select User Management → Change Password.**

   b. **Type the current password.**

   A password comprises 4 to 64 characters. Passwords are case sensitive

   c. **Type the new password twice.**

Remembering User Names and Passwords

The HPDU supports the password manager of the following web browsers, and does not support other browser password managers.

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome

- **When the supported browser asks whether to remember the user name and password, save the login name and password.**

  For information on how to activate a web browser password manager, refer to the documentation for your browser.

Logging Out of the Web Interface

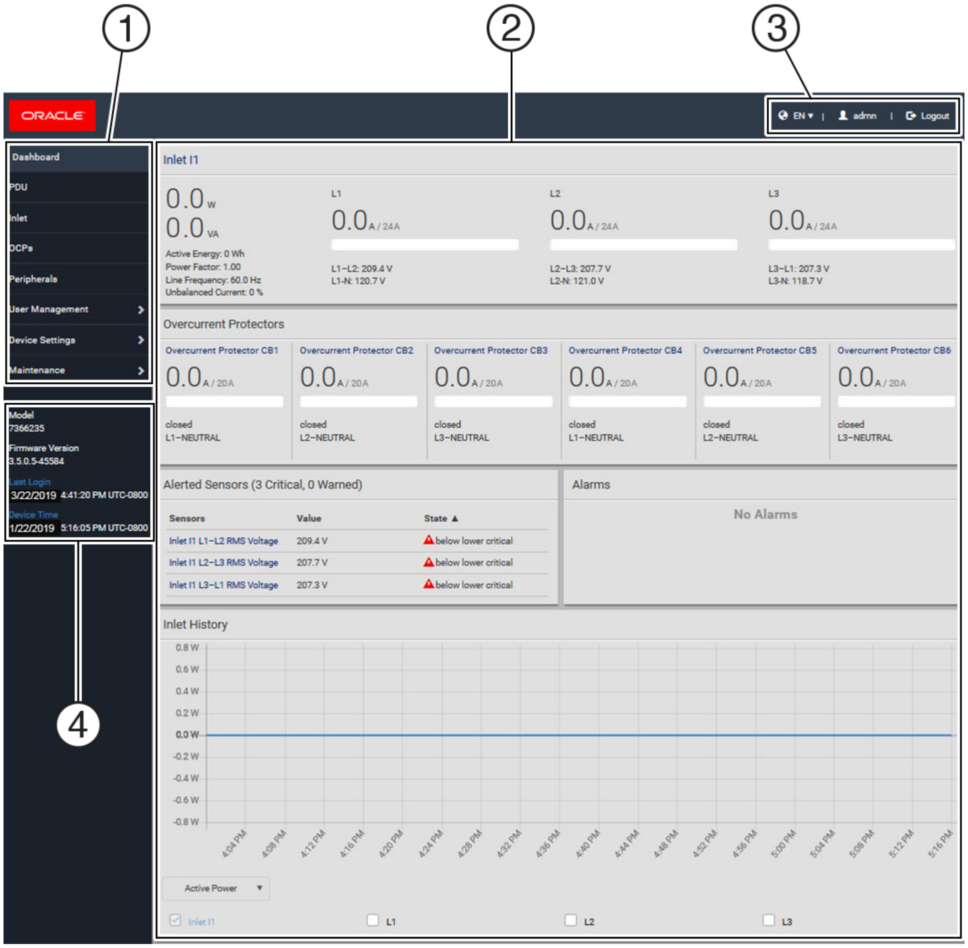
- **After finishing your tasks, log out to prevent others from accessing the HPDU web interface in either of the following ways.**

  - **Log out and keep the web browser open – Click Logout in the top-right corner of the HPDU web interface or close the PDU tab while there are other tabs available in the browser.**

  - **Log out and close the web browser – Click the top-right corner of the browser window, or select File → Close, or File → Exit.**

Web Interface Overview

The web interface Home page consists of four areas, as shown in the following illustration.



Model
7366235
Firmware Version
3.5.0.5-45584
Last Login
3/22/2019 4:41:20 PM UTC-0800
Device Time
1/22/2019 5:16:05 PM UTC-0800

Inlet I1

0.0 W
0.0 VA
Active Energy: 0 Wh
Power Factor: 1.00
Line Frequency: 60.0 Hz
Unbalanced Current: 0 %

L1	L2	L3
0.0 A / 24A	0.0 A / 24A	0.0 A / 24A
L1–L2: 209.4 V L1-N: 120.7 V	L2–L3: 207.7 V L2-N: 121.0 V	L3–L1: 207.3 V L3-N: 118.7 V

Overcurrent Protectors

Overcurrent Protector CB1	Overcurrent Protector CB2	Overcurrent Protector CB3	Overcurrent Protector CB4	Overcurrent Protector CB5	Overcurrent Protector CB6
0.0 A / 20A	0.0 A / 20A	0.0 A / 20A	0.0 A / 20A	0.0 A / 20A	0.0 A / 20A
closed L1–NEUTRAL	closed L2–NEUTRAL	closed L3–NEUTRAL	closed L1–NEUTRAL	closed L2–NEUTRAL	closed L3–NEUTRAL

Alerted Sensors (3 Critical, 0 Warned)

Sensors	Value	State ▲
Inlet I1 L1–L2 RMS Voltage	209.4 V	⚠ below lower critical
Inlet I1 L2–L3 RMS Voltage	207.7 V	⚠ below lower critical
Inlet I1 L3–L1 RMS Voltage	207.3 V	⚠ below lower critical

Alarms

No Alarms

Inlet History

Callout	Web Interface Area
1	Main Menu on the left in the navigation pane.
2	Data or setup page of the selected menu item on the right side of the page.

Callout	Web Interface Area
3	Menu bar at the top of the page. ■ Login name. Click the name to view the user account settings. ■ Logout button. ■ Language. Select a language.
4	List beneath the Main Menu on the left in the navigation pane. ■ PDU model. ■ Current firmware version. ■ Date and time of the user account last login. Click Last Login to view the login history. ■ PDU system time, which is converted to the time zone of your computer or mobile device. Click Device Time to open the Date/Time setup page.

▼ Navigating the Web Interface

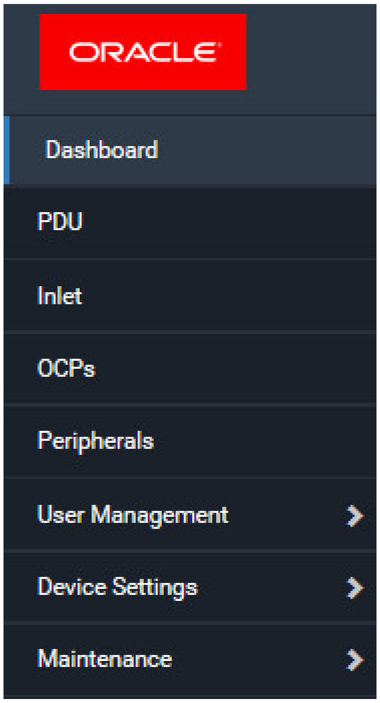
1. **Click any Main Menu or submenu item in the left navigation pane in the Main Menu.**

   That item data or setup page opens on the right side of the page.

2. **View or configure settings on the page.**

3. **To return to the Main Menu and Dashboard page, click Dashboard or Home (Oracle logo).**

Main Menu



Main Menu Item	Description
Dashboard	Summary of the PDU status, including a list of alarms, if any.
PDU	Device data and settings, such as the device name and MAC address.
Inlet	Inlet status and settings, such as inlet thresholds.
OCPs	Displays OCP status and settings, such as OCP thresholds only when there are overcurrent protectors implemented on your model.
Peripherals	Displays peripheral devices connected to the HPDU.
User Management	Data and settings of user accounts and groups, such as password change.
Device Settings	Device settings, including network, security, system time, event rules and more.

Main Menu Item	Description
Maintenance	Device information and maintenance commands, such as firmware upgrade, device backup, and reset.

▼ Using the Main Menu

1. **Click a menu item in the Main Menu.**

   If a Main Menu item contains a submenu, after clicking that item, the submenu appears.

2. **To return to the previous menu, do either of the following:**

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

   - **Click the Oracle logo above the Main Menu to return to the Main Menu.**

▼ Accessing a Frequently Visited Page Quickly

1. **If you frequently visit a page in the HPDU web interface, such as the event log, write down its URL or bookmark it with your web browser.**

2. **Before logging in to the web interface, enter the URL in the address bar of the browser.**

   After login, the HPDU immediately shows the page you want rather than the Dashboard page.

Note - You also can send the URL to other users so that they immediately see that page after login, using their own user credentials.

▼ Sorting a List

If any list displays an Up or Down arrow in one of its column headers, you can resort the list by clicking any column header. The list is resorted in ascending or descending order, based on the selected column. In this procedure, you sort the event log.

1. **To sort the event log in ascending order based on the same column, click the ID header.**

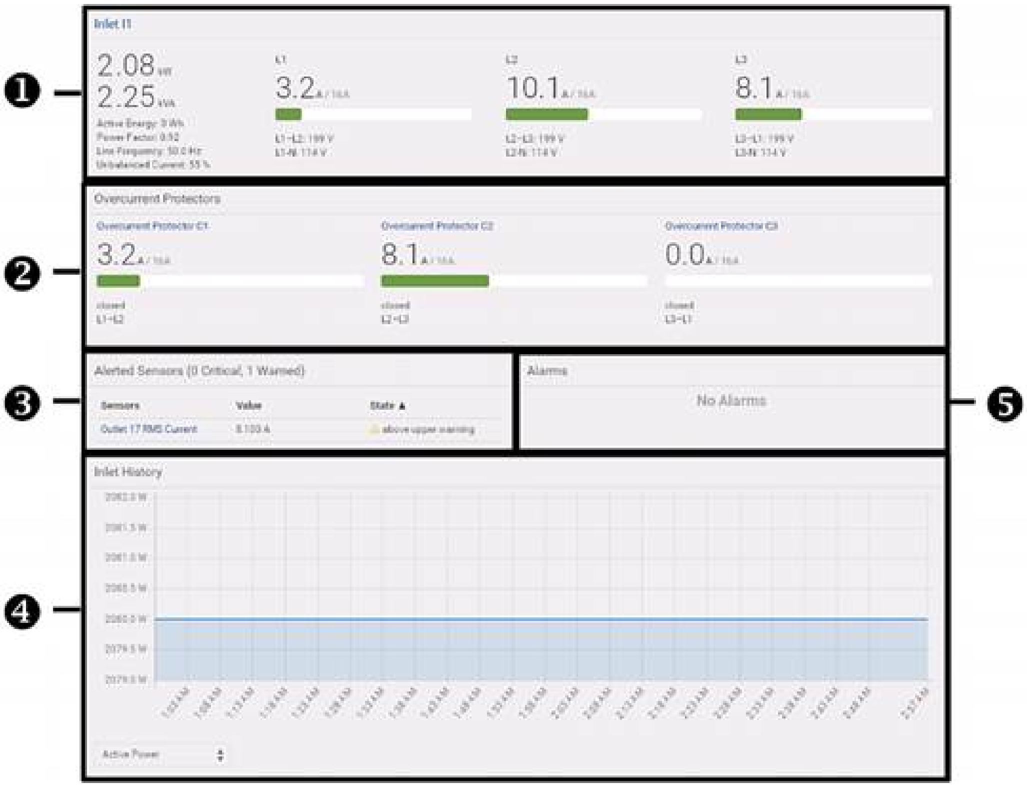
   The Up arrow indicates that the list is sorted in ascending order.

2. **To sort the list based on a different column, click a different column header, such as Event Class column.**

   The arrow now appears next to the selected column, Event Class, indicating the list is sorted in ascending order based on that column.

Dashboard

The Dashboard page contains four to five sections, depending on the HPDU model.



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

Callout	Section	Description
1	Inlet I1	Overview of inlet power data for each phase, represented by a bar that

Callout	Section	Description
		changes colors to indicate the current RMS state. ■ Green: Normal ■ Yellow: Warning ■ Red: Critical
2	Overcurrent Protectors	Displays an overview of each OCP status only when the HPDU contains overcurrent protectors (OCPs). A current bar per OCP changes colors to indicate the current RMS state. ■ Green: Normal ■ Yellow: Warning ■ Red: Critical
3	Alerted Sensors	When any sensor enters the alarmed state, this section lists all alerted sensors. When no sensors enter the alarmed state, this section displays, No Alerted Sensors.
4	Inlet History	The chart of the inlet active power history displays, by default. You also can display a different data type.
5	Alarms	Displays alarm data only after you set event rules requiring users to take the acknowledgment action. When there are unacknowledged events, this section lists all of them. When there are no unacknowledged events, this section shows the message, No Alarms.

▼ Viewing Inlet I1

The number of phases that display in the Inlet section is dependent on the HPDU model.

- **To view more information or configure an inlet, click Inlet I1 to go to the Inlet page.**

  The left side of the Inlet dashboard shows all or some of the following generic inlet power data:

  - Active power (kW or W)
  - Apparent power (kVA or VA)
  - Active energy (kWh or Wh)
  - Power factor
  - Line frequency (Hz)
  - Unbalanced current (%) - Dependent on the HPDU model

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

  The other Inlet data includes:

  - RMS current (A) and rated current
  - Smaller, gray text next to RMS current is the rated current.
  - Bar showing the RMS current level
  - RMS voltage (V)

  The RMS current bars automatically change colors to indicate the current status if the thresholds are enabled.

  - Green – Normal
  - Yellow – Above upper warning
  - Red – Above upper critical

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

Viewing OCP

The availability and total number of OCPs depend on the HPDU model. Each OCP link allows you to view more information or configure individual OCPs.

- **Click the OCP index number (CB1, CB2) to go to the OCP setup page.**

  The power date for each OCP includes:

  - RMS current (A), and rated current

- Smaller gray text adjacent to RMS current is each OCP rated current, such as 16A.
- Bar showing OCP current levels
- OCP status – Open or closed
- Associated line pair

The RMS current bars automatically change colors to indicate the current status if you enabled OCP thresholds.

- Green – Normal
- Yellow – Above upper warning
- Red – Above upper critical

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

▼ Viewing Inlet History

The inlet power chart helps you observe whether there were abnormal events in the past tens of minutes. By default, the inlet active power data displays.

1. **To display the chart for other inlet power data, select a different data type by clicking the selector below the chart. Available data types include:**

   - RMS current
   - RMS voltage
   - Active power
   - Apparent power

2. **To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data display.**

3. **If your HPDU is a multi-inlet model, you can have one or multiple inlets display their power charts by selecting the check box of each inlet you want to display.**

   When multiple inlets display in the chart, their colors are different. You can identify each inlet's data according to the colors of the selected inlet check boxes.

4. **When both inlets display in the chart, hover your mouse over either inlet data line. Both inlet values display simultaneously, marked with corresponding colors.**

Viewing Alarms

If configuring any event rules that require users to take the acknowledgment action, the Alarms section lists any event that no one acknowledges yet since an event occurrence.

1. **Verify that you have Acknowledge Alarms permission so you can manually acknowledge an alarm.**

2. **To acknowledge an alarm, click Acknowledge.**

   That alarm disappears from the Alarms section. The alarms list contains the following settings.

Alarm Setting	Description
Name	Custom name of the Alarm action.
Reason	The first event that triggers the alert.
First Appearance	Date and time when the event indicated in the Reason column occurred for the first time.
Last Appearance	Date and time when the event indicated in the Reason column occurred for the last time. **Note -** The date and time shown on the HPDU web interface are automatically converted to your computer's time zone. To avoid any time confusion, you can apply the same time zone settings as those of HPDU to your computer.
Count	Number of times the event indicated in the Reason column has occurred.
More Alerts	This field appears only when there are more than one types of events triggering this alert. If there are other types of events (that is, other reasons) triggering the same alert, the total number

Alarm Setting	Description
	of additional reasons is displayed. You can click it to view a list of all events.

PDU

The generic HPDU device information and HPDU global settings are available on the PDU page.

▼ Viewing the HPDU Settings

● **To open the PDU page, click PDU in the Main Menu (on page 34).**

The device information includes:

- Firmware version
- Serial number
- MAC address
- Rating

▼ Configuring Global HPDU Settings

1. **Click Edit Settings.**
2. **Click the Up or Down arrow and select an option.**
3. **Select or deselect the check box.**
4. **Adjust the numeric values. For time-related fields, if you do not prefer the option selection using the Up or Down arrow, type a value, which must include a time unit, such as 50 s.**
5. **Click Save.**

▼ Resetting All Active Energy Counters

An active energy reading is a value of total accumulated energy, which is never reset, even if the power fails or the HPDU is rebooted. However, you can manually reset this reading to restart the energy accumulation process.

1. **Verify that you are assigned the Admin role so you can reset active energy readings.**
2. **Click Reset to confirm resetting all active energy readings on the HPDU to zero.**

Note - You can reset the active energy reading of an individual inlet only.

▼ Changing the Time Units

Different fields have different ranges of valid time unit values.

- **Type a new value in the time-related fields, such as Inrush Guard Delay, and add a time unit after the numeric value. For example, type 15 s for 15 seconds.**

Unit	Time
ms	Millisecond
s	Second
min	Minute
h	Hour
d	Day

Inlet

You can view all inlet information, configure inlet-related settings, or reset the inlet active energy on the Inlet page.

▼ Viewing Inlet Information

- **To open the Inlet page, click Inlet in the Main Menu (on page 34).**

Inlet thresholds, once enabled, help you identify whether the inlet enters the warning or critical level. In addition, you can have HPDU automatically generate alert notifications for any warning or critical status.

The generic Inlet information includes:

- Inlet power overview, which is the same as Dashboard - Inlet I1 (on page 40).
- A list of inlet sensors with more details. Number of available inlet sensors depends on the model.

- Sensors show both readings and states.
- Sensors in warning or critical states are highlighted in yellow or red.
- Inlet power chart, which is the same as Dashboard - Inlet History.

▼ Customizing the Inlet Name

1. **Click Edit Settings.**
2. **Type a name for the inlet. For example, you can name it to identify the power source.**
3. **Click Save.**

   The inlet custom name displays on the Inlet or Dashboard page, followed by its label in parentheses.

▼ Resetting the Inlet Active Energy Counter

The energy reset feature per inlet is especially useful when your HPDU has more than one inlet.

1. **Verify that you were assigned the Admin role.**
2. **Click Reset Energy.**
3. **Click Reset to confirm.**

   This inlet active energy reading is reset to zero.

▼ Configuring Inlet Thresholds

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

1. **Click the Thresholds title bar at the bottom of the page to display inlet thresholds.**
2. **Click the sensor and click Edit Thresholds.**
3. **To enable any threshold, select a threshold check box and type a new value in the text box.**

4. **Click Save.**

OCP

The Overcurrent Protectors page displays all breakers with their status. If any breaker trips or its current level enters the alarmed state, it is highlighted in red or yellow.

Overcurrent protector overview:

- OCP status - open (tripped) or closed
- Current drawn and current bar
  - The RMS current bars change colors to indicate the status if the OCP thresholds have been configured and enabled.

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

- Associated lines

▼ Viewing OCP Settings

● **Click any OCP name on the OCPs or Dashboard.**

The OCP data/setup page contains the following information.

OCP Field	Description
Label	OCP physical number.
Status	OCP is open or closed.
Type	OCP type.
Rating	OCP rate current.
Lines	Lines for the OCP.
Inlet	Inlet for the OCP. **Note -** The Inlet information is useful only when the HPDU has multiple inlets.
RMS Current	Current state and readings, including current drawn and current remaining.

▼ Viewing and Sorting OCPs

1. **To open the OCPs page, click OCPs in the Main Menu.**

2. **You can go to each OCP data/setup page by clicking its name on this page.**

3. **To sort the list, click a column header.**

4. **To go to a different OCP data/setup page, click the OCP selector in the top-left corner.**

5. **To go to the Inlet data page, in the Details section, click the Inlet link.**

▼ Configuring Current Thresholds for Multiple Overcurrent Protectors

When you enable OCP thresholds, you can identify the breaker whose RMS current enters the warning or critical level with the yellow or red color. You also can configure the HPDU to generate alert notifications for any warning or critical status.

Note - By default, upper thresholds of a breaker RMS current are configured. You can modify them as needed.

---

1. **Click (three vertical dots name) → Threshold Bulk Setup.**

2. **Select one or multiple OCPs.**

3. **To select all OCPs, click the topmost check box in the header row.**

4. **Click Edit Thresholds.**

5. **Make any changes.**

6. **To enable any threshold, select a threshold check box.**

7. **Type a new value in the text box.**

8. **Click Save.**

▼ Customizing an OCP Name

1. **Click Edit Settings.**

2. **Type a name for the OCP.**
3. **Click Save.**

▼ Viewing an OCP RMS Current Chart

- **in the Overcurrent Protector History section, for the OCP data chart, to retrieve the exact data at a particular time, hover your mouse over the data line in the chart.**

  The threshold data displays on the Y axis and the time displays on the X axis.

▼ Configuring the OCP Threshold Settings

By default, upper thresholds of an OCP RMS current are configured. You can modify them as needed.

Note - The threshold values for an individual OCP override the bulk threshold values stored for the OCP.

---

1. **Click the Thresholds title bar at the bottom of the page to display the threshold data.**
2. **Click the RMS current sensor and click Edit Thresholds.**
3. **Make any changes.**
4. **To enable any threshold, select the threshold check box.**
5. **Type a new value in the text box.**
6. **Click Save.**

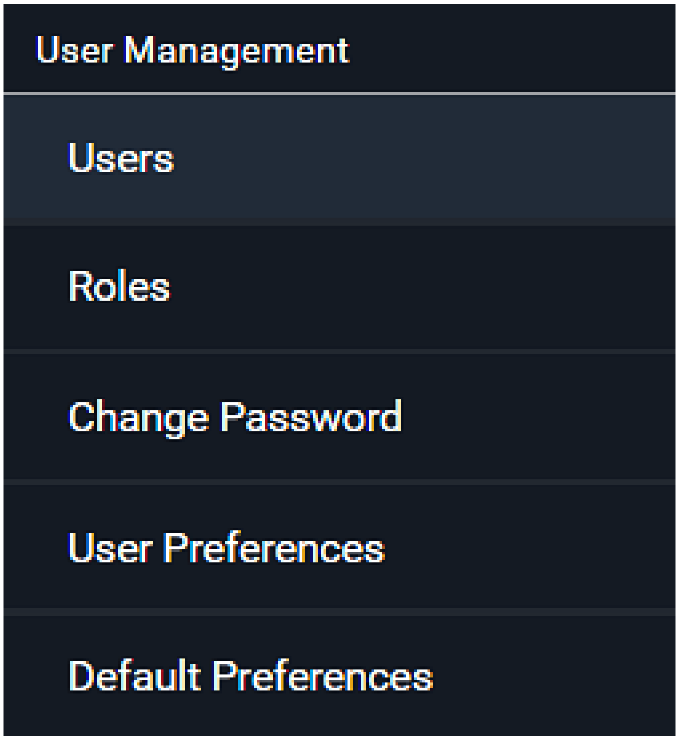
User Management

The User Management menu allows you to manage user accounts, permissions, and preferred measurement units on a per-user basis.

The HPDU is shipped with one built-in administrator account, admin, which is ideal for initial login and system administration. You cannot delete admin or change its permissions. You must change the Admin password.

A role determines the tasks or actions a user is permitted to perform on the HPDU device, and so you must assign one or m roles to each user.

The User Management menu contains the following menu items.



User Management Menu Item	Description
Users	Create users.
Roles	Create roles.
Change Password	Change the password.
User Preferences	Set preferred measurement units.
Default Preferences	Set default measurement units.

Manage Users

You can create, edit, and delete users.

Creating Users

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

1. **Select User Management → Users → Add user button with +.**

2. **Enter information in the Required fields.**

User Information	Description
User Name	The name the user enters to log in to the HPDU. ■ 4 to 32 characters ■ Case sensitive ■ No spaces.
Full Name	The user first and last names.
Password, Confirm Password	■ 4 to 64 characters ■ Case sensitive ■ Spaces
Telephone Number	The user telephone number
eMail Address	The user email address ■ Maximum of 128 characters ■ Case sensitive
Enable	When selected, the user can log in to the HPDU.
Force password change on next login	When selected, a password change request automatically appears the next time the user logs in.

Editing or Deleting Users

1. **Select User Management → Users to open the Users page, which shows users, enabled (check mark) and disabled (X).**

2. **If needed, sort the list by clicking a column header.**
3. **To edit a user:**
   1. **On the Users page, click the user.**
   2. **On the Edit User page, make any changes.**
   3. **To change the password, type a new password in the Password and Confirm Password fields.**

      If the password field is left blank, the password remains unchanged.
4. **To delete one or more users:**
   1. **To delete a user, click Delete (trashcan), and confirm.**
   2. **To delete multiple user accounts, on the Users page, click the check boxes at the beginning of each row or to select all user accounts, except for the admin user, select the first check box next to Enabled in the header row.**
   3. **Click Delete to confirm.**
5. **Click Save.**

Create and Assign Roles

You can use the built-in roles, create new roles, edit and delete roles, and assign the roles to determine the user permissions.

▼ Creating a Role

A role is a combination of permissions. Each user must have at least one role. The HPDU provides two built-in roles. If the two roles are not what you want, add new roles. The HPDU supports up to 64 roles.

1. **Select User Management → Roles → Add role button with +.**
2. **Type a role name.**

   A role name is 1 to 32 characters long, case sensitive, and can include spaces.

3. **Type a description for the role in the Description field.**

4. **Select one or more privileges.**

Privilege	Description
Administrator Privileges	All privileges.
Unrestricted View Privileges	All View privileges.

If any privilege requires the argument setting, a Down arrow symbol displays at the end of that privilege row.

a. **To select a privilege that requires the argument setting, click that privilege in the row to display a list of available arguments for that privilege.**

b. **Select the arguments.**

Note - To select all arguments, select **All (argument name)**.

c. **Click Save.**

▼ Editing or Deleting Roles

1. **Select User Management → Roles to open the Roles page, which lists all roles.**

   The Admin role is not user-configurable and so the lock icon displays, indicating that you are not allowed to configure it.

2. **If needed, sort the list by clicking a column header.**

3. **To edit a role, perform these steps:**

a. **On the Roles page, click the role you want to edit.**

b. **On the Edit Role page, make any changes.**

Note - You cannot change the role name.

4. **To delete one or more roles:**

a. **To delete the role you selected, click Delete (trashcan), and confirm the deletion.**

b. **To delete any roles, on the Roles page, click each check box at the beginning of a row.**

c. **To select all roles, except for the Admin role, select the check box in the header row.**

d. **Click Delete (trashcan) in the top-right corner.**

e. **Click Delete to confirm.**

5. **Click Save.**

▼ Assigning Roles

1. **Select one or multiple roles.**

Note - With multiple roles selected, a user has the union of all roles' permissions.

2. **To select all roles, select the check box in the header row.**

   A user can have a maximum of 32 roles.

3. **If the built-in roles do not satisfy your needs, add new roles by clicking the Add role button with +. The new role is automatically assigned to the user account you created.**

Manage Authentication Settings and Passwords

You can manage the authentication settings, passwords, and password settings.

▼ Entering the SSH Public Key

If the public key authentication for SSH is enabled, you must enter the SSH public key only.

1. **Open the SSH public key with a text editor.**

2. **Copy and paste all SSH public key content in the text editor into the SSH Public Key field.**

▼ Enabling or Disabling SNMPv3

The SNMPv3 access permission is disabled by default. Enable the SNMPv3 protocol for SNMPv3 access.

1. **To permit SNMPv3 access by a user, select Enable SNMPv3.**

2. **Select a Security Level.**

   - **None** – No authentication and no privacy. This is the default.
   - **Authentication** – Authentication and no privacy.
   - **Authentication & Privacy** – Authentication and privacy.

▼ Changing the Authentication Password

The authentication password is configurable only when you select Authentication or Authentication & Privacy.

1. **If the authentication password is identical to the user password, select Same as User Password.**

2. **To specify a different authentication password, clear the Same as User Password check box, and type the authentication password in the Password box.**

   The password must contain 8 to 32 ASCII printable characters.

3. **Type the same authentication password in the Confirm Password box.**

▼ Changing the Privacy Password

The privacy password is configurable only when you select Authentication & Privacy.

1. **If the privacy password is identical to the authentication password, select Same as Authentication Password.**

2. **To specify a different privacy password, clear the Same as Authentication Password check box, and type the privacy password in the Password box.**

The password must contain 8 to 32 ASCII printable characters.

3. **Type the same privacy password in the Confirm Password box.**

▼ Selecting a Protocol

A protocol is configurable only when you select Authentication or Authentication & Privacy.

1. **To select an authentication protocol, click Authentication.**
2. **Select the SHA-1 (default).**
3. **To select a privacy protocol, click Privacy.**
4. **Select DES (default) or AES-128.**

Preferred and Default Measurement Units

You can set preferred and default preferences to specify units of measure for the HPDU. You can change the measurement units in the HPDU user interface according to your own preferences regardless of the permissions you have. Administrators also can change the measurement units for specific users on the Edit User page.

▼ Setting Preferred Measurement Units

Measurement unit changes apply only to the web interface and command line interface. Users can change the measurement units at any time by setting their own preferences. Setting your own preferences does not change the default measurement units.

1. **Select User Management → User Preferences.**
2. **Make any changes.**
    a. **To change the temperature unit of measure, select Celsius or Fahrenheit.**
    b. **To change the length unit for length or height, select Meter or Feet.**
    c. **To change the pressure unit, select Pascal (one newton per square meter) or Psi (pounds per square inch).**

3. **Click Save.**

▼ Setting Default Measurement Units

Default measurement units are applied to all HPDU user interfaces across all users, including users accessing the HPDU through external authentication servers. The front panel display also shows the default measurement units.

Note - The preferred measurement units set by any individual user or by the administrator on a per-user basis overrides the default units in the web interface and command line interface.

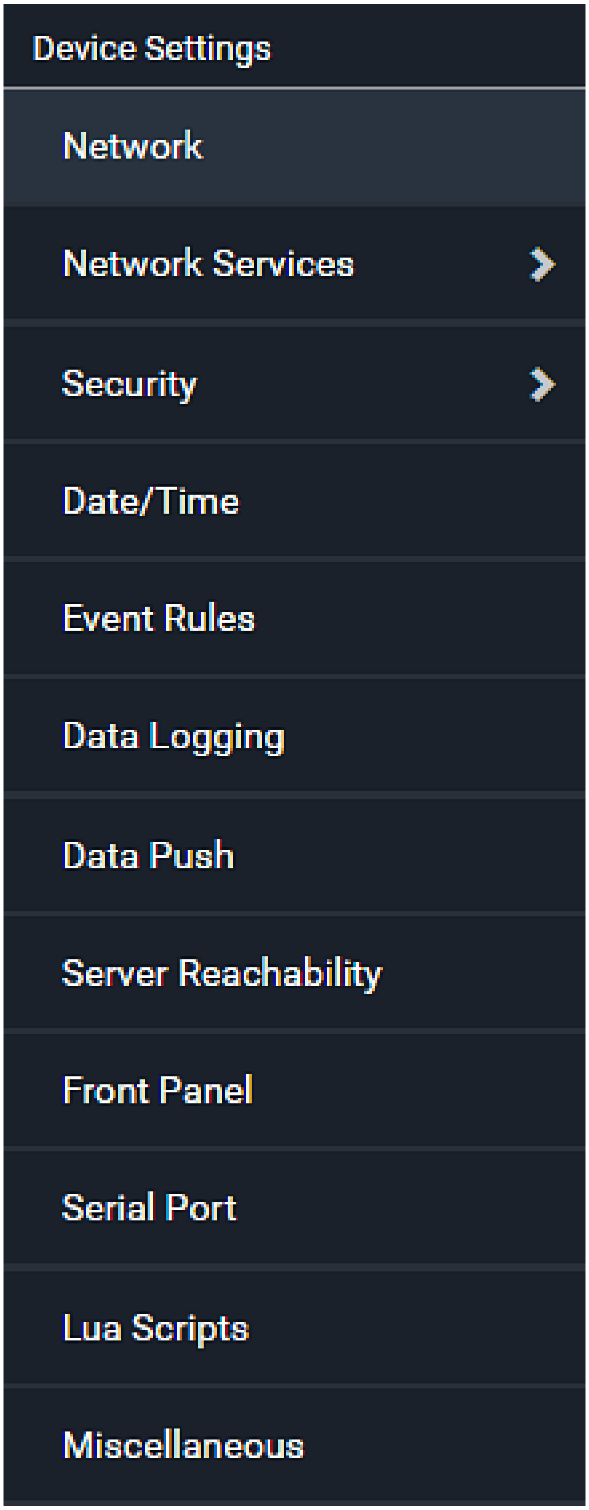
Default measurement units apply to the following user interfaces or data:

- Web interface for new local users when they have not configured their own preferred measurement units.
- Web interface for users who are authenticated through LDAP or Radius servers.
- The sensor report generated by selecting Send Sensor Report.
- Front panel LCD display.

1. **Click User Management → Default Preferences.**
2. **Make any changes.**
   a. **To change the temperature unit of measure, select Celsius or Fahrenheit.**
   b. **To change the length unit for length or height, select Meter or Feet.**
   c. **To change the pressure unit, select Pascal (one newton per square meter) or Psi (pounds per square inch).**
3. **Click Save.**

Device Settings

In the Main Menu, when you select Device Settings, the Device Settings menu displays.


Device Settings
Network
Network Services
Security
Date/Time
Event Rules
Data Logging
Data Push
Server Reachability
Front Panel
Serial Port
Lua Scripts
Miscellaneous

Device Settings Menu Item	Description
Network	Configure network settings.
Network Services	Configure network services, which include: HTTP SNMP SMTP Server SSH Telnet Modbus Server Advertising
Security	IP Access Control Role Based Access Control TLS Certificate Authentication Login Settings Password Policy Service Agreement
Date/Time	Common Network settings. NTP settings.
Event Rules	Create and configure event rules, use built-in event rules, and schedule actions.
Data Logging	Set and configure data logging for Inlet Sensors, OCPs, and Peripheral Device Sensors.
Data Push	Create, modify, or delete data push settings.
Server Reachability	Add, modify, or delete IT devices for ping monitoring, and check server monitoring states and results.
Front Panel	Configure front panel settings.
Serial port	Configure the serial port, analog modem, and GSM modem.

Device Settings Menu Item	Description
Lua Scripts	Write, modify, delete, load, start, and stop Lua scripts, and check the state and settings of each Lua script.
Miscellaneous	Configure Cisco EnergyWise.

Network Settings

Configure wired, wireless, and Internet protocol-related settings on the Network page after connecting the HPDU to your network (on page 5).

You can enable both the wired and wireless networking on the HPDU so that it has multiple IP addresses -- wired and wireless IP. For example, you can obtain one IPv4 and/or IPv6 address by enabling one Ethernet interface, and obtain one more IPv4 and/or IPv6 address by enabling/configuring the wireless interface.

- Wired network settings
- Common network settings
- Ethernet network settings

▼ Configuring Network Settings

1. **Select Device Settings → Network.**

2. **To use DHCP-assigned DNS servers and gateway instead of static ones, go to step 3. To manually specify DNS servers and default gateway, configure the Common Network Settings section.**

3. **Configure the Static routes only when there are local requirements.**

4. **Enable either or both Internet protocols (IPv4 and IPv6).**

   The following protocols are compliant with the Internet protocol(s):

   - LDAP
   - NTP
   - SMTP
   - SSH
   - Telnet

- FTP
- TLS (TLS 1.0, 1.1, and 1.2)
- SNMP
- Syslog

5. **Configure IPv4/IPv6 settings for a wired network in the ETHERNET (or ETH1/ETH2).**

6. **Configure the ETHERNET (or ETH1/ETH2) interface settings.**

▼ Configuring Wired Network Settings

1. **On the Network page, click the ETHERNET (or ETH1/ETH2) section to configure IPv4/IPv6 settings.**

2. **To enable the Interface, ensure the Ethernet interface is enabled, or all networking through this interface fails. This setting is available in the ETHERNET (or ETH1/ETH2) section.**

3. **For IPv4:**

   a. **Enable or disable the IPv4 protocol.**

   b. **To select the method for IP Auto Configuration, select DHCP (automatic) or Static (manual).**

   c. **If you select DHCP, optionally, specify the preferred hostname.**

      The hostname consists of alphanumeric characters and hyphens, cannot begin or end with a hyphen, with a maximum of 63 characters, and no punctuation marks, spaces, and other symbols.

   d. **If you select Static, assign a static IPv4 address, with the syntax IP address/prefix length. For example, 192.168.84.99/24.**

4. **For IPv6:**

   a. **Enable or disable the IPv6 protocol.**

   b. **To select the method for IP Auto Configuration, select Automatic or Static (manual).**

c. **If you select Automatic, optionally, specify the preferred hostname.**

The hostname consists of alphanumeric characters and hyphens, cannot begin or end with a hyphen, with a maximum of 63 characters, and no punctuation marks, spaces, and other symbols.

d. **If you select Static, assign a static IPv6 address, with the syntax IP address/ prefix length. For example, fd07:2fa:6cff:1111::0/128.**

▼ Configuring Common Network Settings

Common Network Settings are optional and you can leave them unchanged if there are no local networking requirements.

● **If you want to change the local networking settings, change any of the following options.**

Common Network Setting	Description
Cascading mode	■ None. ■ Bridging. ■ Port Forwarding.
DNS Resolver Reference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. ■ IPv4 Address: Use the IPv4 addresses. ■ IPv6 Address: Use the IPv6 addresses.
DNS Suffixes (optional)	Specify a DNS suffix name if needed.
First/Second/Third DNS Server	Manually specify static DNS server(s). ■ If you specify any static DNS server, the setting overrides the DHCP-assigned DNS server. ■ If you select DHCP (or Automatic) for IPv4/ IPv6 settings, and you do not specify any static DNS servers, the HPDU

Common Network Setting	Description
	uses DHCP-assigned DNS servers.
IPv4/IPv6 Routes	You need to configure these settings only when your local network contains two subnets, and you want the HPDU to communicate with the other subnet. If so, ensure IP forwarding is enabled in the network, and click Add Route to add static routes.

▼ Configuring Ethernet Interface Settings

The Ethernet Interface setting is available in the ETHERNET (or ETH1/ETH2) section.

1. **Ensure the Ethernet interface is enabled, or all networking through this interface fails.**

2. **Change the Other Ethernet settings, if needed.**

Ethernet Interface Setting	Description
Speed	Select a LAN speed. ■ Auto: System determines the optimum LAN speed through auto-negotiation. ■ 10 MBit/s: Speed is always 10 Mbps. ■ 100 MBit/s: Speed is always 100 Mbps. ■ 1 GBit/s MBit/s: Speed is always 1 Gbps. **Note -** Auto-negotiation is disabled after setting both the speed and duplex settings of the HPDU to NON-Auto values, which might result in a duplex mismatch.
Duplex	Select a duplex mode.

Ethernet Interface Setting	Description
	■ Auto: The HPDU selects the optimum transmission mode through auto-negotiation. ■ Full: Data is transmitted in both directions simultaneously. ■ Half: Data is transmitted in one direction (to or from the HPDU device) at a time. **Note -** Auto-negotiation is disabled after setting both the speed and duplex settings of the HPDU to NON-Auto values, which might result in a duplex mismatch.
Current State	Show the current LAN status, including the current speed and duplex mode.

Static Route Examples

The static route examples are IPv4 and IPv6. Both examples assume that two network interface controllers (NIC) are installed on one network server, with two available subnets, and IP forwarding is enabled. All NICs and HPDU devices in the examples use static IP addresses.

Most local multiple networks are not directly reachable and require the use of a gateway. The Gateway option is selected in the examples.

Note - If your local multiple networks are directly reachable, you would select Interface instead of Gateway. When you select Interface, select an interface name instead of entering an IP address.

Interface Names

When your local multiple networks are directly reachable, select Interface for static routes. Then select an interface where another network is connected.

Network Services

The HPDU supports the following network communication services. All TCP ports for supported services are set to standard ports.

Network Service	Description
HTTP HTTPS	■ Enable or disable access to the HPDU web interface. ■ HTTPS uses Transport Layer Security (TLS) technology to encrypt all traffic to and from the HPDU so it is a more secure protocol than HTTP. The HPDU supports TLS 1.0, 1.1 and 1.2. ■ By default, any access to the HPDU through HTTP is automatically redirected to HTTPS. You can disable this redirection if needed.
SNMP	■ Allows the SNMP manager to retrieve and control the power status of each outlet. ■ Enable or disable SNMP communication between an SNMP manager and the HPDU device.
SMTP Server	■ Sends alerts or event messages to an administrator by email.
SSH	Enable or disable access to the HPDU command line interface (default) or change the TCP port, or set a password or public key for login over the SSH connection.
Telnet	Enable or disable access to the HPDU command line interface or change the TCP port. By default, Telnet is disabled because it

Network Service	Description
	communicates openly and is not secure.
Modbus	Enable or disable the Modbus/TCP access to the HPDU, set it to the read-only mode, or change the TCP port.
Service Advertising	The HPDU advertises all enabled services that are reachable using the IP network. The protocols are MDNS (Multicast DNS) and Link-Local Multicast Name Resolution (LLMNR). The advertised services are discovered by clients that have implemented MDNS and LLMNR. By default,both protocols are enabled. The advertised services include: ■ HTTP ■ HTTPS ■ Telnet ■ SSH ■ Modbus ■ json-rpc ■ SNMP Enables Link-Local Multicast Name Resolution (LLMNR) and MDNS, which are required for resolving APIPA host names. Supports both IPv4 and IPv6 protocols.

▼ Changing HTTP(S) Settings

1. **Select Device Settings → Network Services → HTTP.**

2. **Enable either or both protocols by selecting the Enable check box.**

3. **To use a different port for HTTP or HTTPS, type a new port number.**

Caution - Different network services cannot share the same TCP port.

4. **To redirect the HTTP access to the HPDU to HTTPS, select Redirect HTTP connections to HTTPS.**

   The redirection check box is configurable only when you enable both HTTP and HTTPS.

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

   If you force the HPDU to use a specific AES cipher, for information on configuring AES settings, refer to the client documentation. For example, you can enable a cipher and disable the other in Firefox using the `about:config` command.

▼ Configuring SNMP Settings

1. **Select Device Settings → Network Services → SNMP.**

2. **Enable or disable SNMP v1 / v2c or SNMP v3 by clicking a check box.**

   The SNMP v1/v2c read-only access is enabled by default. The default Read Community String is public.

3. **To enable read-write access, type the Write Community String, where usually the string is private.**

4. **If needed, type the MIB-II system group information.**

   - sysContact – Contact person who manages system
   - sysName – Name assigned to the system
   - sysLocation – Location of the system

5. **Configure SNMP notifications.**

   a. **Select Enable SNMP Notifications.**

b. **Select a notification type: SNMPv2c trap, SNMPv2c inform, SNMPv3 trap, and SNMPv3 inform.**

c. **Specify the Notification type, Timeout, and Number of Retries.**

Note - When you change any SNMP Notifications settings on the SNMP page, the settings in the System SNMP Notification Action are updated. To add more than three SNMP destinations, you can create new SNMP notification actions.

d. **For each SNMP destination, enter the Host, Port, and Community.**

6. **To download the SNMP MIB for the HPDU to use with the SNMP manager, click the Download MIBs down arrow, and click the PDU2-MIB download link.**

Note - If the built-in system SNMP Notification Rule is enabled and the SNMP destination is not set yet, you might need to configure the SNMP destination(s).

7. **Click Save.**

▼ Configuring SMTP Server Settings

1. **Select Device Settings → Network Services → SMTP Server.**

Note - If any email messages fail to be sent successfully, the failure event and reason appear in the event log.

2. **Enter the information, as needed.**

SMTP Server Setting	Description
IP address/hostname	Type the IP address or host name of the mail server.
Port	Type the port number. Default is 25.
Sender Email Address	Type an email address for the sender.
Number of Sending Retries	Type the number of email retries. Default is 2 retries.

SMTP Server Setting	Description
Time Between Sending Retries	Type the interval between email retries in minutes. Default is 2 minutes.
Server Requires Authentication	Select this check box if your SMTP server requires password authentication.
User Name, Password	Type a user name and password for authentication after selecting the above check box. ■ The length of user name and password ranges between 4 and 64. Case sensitive. ■ Spaces are not allowed for the user name, but allowed for the password.
Enable SMTP over TLS (StartTLS)	If your SMTP server supports the Transport Layer Security (TLS), select this option.

3. Select the CA Certificate settings.

CA Certificate Setting	Description
CA certificate	Verifies the validity of the TLS certificate that will be installed. For example, the HPDU verifies the certificate validity period against the system time.
Browse	Imports a certificate file. ■ Click Show to view the certificate content. ■ Click Remove to delete the installed certificate.
Allow expired and not yet valid certificates	■ Forces authentication to succeed regardless of the certificate validity period. ■ If you clear this check box, the authentication fails whenever any certificate in the selected

CA Certificate Setting	Description
	certificate chain is outdated or not valid yet.

4. **To test the SMTP settings, type the recipient email address in the Recipient Email Addresses field, with a comma to separate multiple email addresses.**

5. **Click Send Test Email.**

6. **Verify that the recipient(s) receives the email.**

Note - The TLS and HTTPS protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between the HPDU and the client (such as a web browser), which is impacted by the cipher priority of the HPDU and the client cipher availability and settings.

If you force the HPDU to use a specific AES cipher, for information on configuring AES settings, refer to the client documentation. For example, you can enable a cipher and disable the other in Firefox using the `about:config` command.

---

7. **Click Save.**

▼ Changing SSH Settings

1. **Select Device Settings → Network Services → SSH.**

2. **To enable or disable the SSH access, select or deselect the check box.**

3. **To use a different port, type a port number.**

4. **Select Public key authentication only to enable the public key-based login only**

5. **Click Save.**

▼ Changing Telnet Settings

1. **Select Device Settings → Network Services → Telnet.**

2. **To enable the Telnet access, select the check box.**

3. **To use a different port, type a new port number.**

4. **Click Save.**

▼ Changing Modbus Settings

1. **Select Device Settings → Network Services → Modbus.**
2. **To enable the Modbus/TCP access, select the Modbus/TCP Access check box.**
3. **To use a different port, type a new port number.**
4. **To enable Modbus read-only mode, select Read-only mode or to enable read-write mode, clear the Read-only mode check box .**

▼ Enabling Service Advertising

1. **Select Device Settings → Network Services → Service Advertising.**
2. **To enable the service advertising, select either or both check boxes.**

   Note - If you set a preferred host name for IPv4 and/or IPv6, you can use that host name as the zero configuration .local host name, that is, <preferred_host_name>.local, where <preferred_host_name> is the preferred host name you specified for the HPDU. The IPv4 host name is the first priority. If an IPv4 host name is not available, use the IPv6 host name.

3. **Select where to advertise:**
   - **To advertise through MDNS, select Multicast DNS.**
   - **To advertise through LLMNR, select Link-Local Multicast Name Resolution.**
4. **Click Save.**

TLS Certificate

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

To obtain a CA-signed certificate:

- Create a Certificate Signing Request (CSR) on the HPDU.
- Submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with a certificate.
- Import the CA-signed certificate onto the HPDU.

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

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

▼ Creating a CSR

1. **Select Device Settings → Security → TLS Certificate.**

2. **Enter information in the Required fields.**

Note - If you generate a CSR without values in the required fields, you cannot obtain third-party certificates.

CSR Information	Description
Country	Country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ISO website (`https://www.iso.org/iso-3166-country-codes.html`).
State or Province	Full name of the state or province where your company is located.
Locality	City where your company is located.
Organization	Registered name of your company.
Organizational Unit	Name of your department.
Common Name	Fully qualified domain name (FQDN) of your HPDU device.

CSR Information	Description
Email Address	Email address where you or another administrative user can be reached.

3. **In the Miscellaneous section, enter information for Not valid before, Not valid after, Serial number, and Key length.**

4. **If you want a certificate to secure multiple hosts across different domains or subdomains, click + Add Name to add the DNS host names or IP addresses of the those hosts to this CSR so that a single certificate is valid for all of them.**

   Examples of subject alternative names: support.company.com, help.company.com, help.company.net, and 192.168.77.50.

5. **Select the key creation parameters.**

CSR Option	Description
Key Length	Select an available key length (bits). A larger key length enhances the security, but slows down the HPDU device response. ■ Only 2048 is available now.
Self Sign	For requesting a certificate signed by the CA, ensure this check box is not selected.
Challenge, Confirm Challenge	Type a password. The password protects the certificate or CSR. The value must be 4 to 64 characters long. Case sensitive.

6. **Create a CSR and private key.**

   a. **Click Create New TLS Key.**

      This might take several minutes to complete.

   b. **Click Download Certificate Signing Request to download the CSR to your computer.**

c. **At the prompt, click Save.**

d. **Submit the CSR to a CA to obtain the digital certificate.**

7. **If the CSR contains incorrect data, click Delete Certificate Signing Request to remove it, and then repeat the Steps 1-5 to re-create it.**

8. **To store the newly-created private key on your computer:**

a. **In the Active TLS Certificate section, click Download Key to download the private key of the currently-installed certificate, not the newly-created one.**

b. **In the Subject Alternative Names, enter names.**

9. **When prompted, click Save.**

10. **Install the CA-signed certificate.**

▼ Installing a CA-Signed Certificate

1. **To obtain a certificate from a certificate authority (CA), create a CSR, and send it to the CA.**

2. **After receiving the CA-signed certificate, select Device Settings → Security → TLS Certificate.**

3. **Click Browse to navigate to the CA-signed certificate file.**

4. **Click Upload to install it.**

5. **To verify whether the certificate is installed successfully, verify the data in the Active TLS Certificate section.**

▼ Creating and Installing a Self-Signed Certificate

When the certificate and key files for the HPDU device are unavailable, an alternative (other than submitting a CSR to the CA), is to generate a self-signed certificate.

1. **Select Device Settings → Security → TLS Certificate.**

2. **Enter information in the Required fields.**

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

Self-Signed Certificate Information	Description
Country	Country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ISO website (`https://www.iso.org/iso-3166-country-codes.html`).
State or Province	Full name of the state or province where your company is located.
Locality	City where your company is located.
Organization	Registered name of your company.
Organizational Unit	Name of your department.
Common Name	Fully qualified domain name (FQDN) of your HPDU device.
Email Address	Email address where you or another administrative user can be reached.
Key Length	Select an available key length (bits). A larger key length enhances the security, and slows down the HPDU device response. Only 2,048 is available now.
Self Sign	Ensure this check box is selected, which indicates that you are creating a self-signed certificate.
Validity in Days	This field appears after you select the Self Sign check box. Type the number of days for which the self-signed certificate will be valid.

3. **Click Create New TLS Key to create both the self-signed certificate and private key.**

   This might take several minutes to complete

4. **After the self-signed certificate and private key are completed, verify the data in the New TLS Certificate section.**

   - **If correct, click Install Key and Certificate to install the self-signed certificate and private key.**

   Note - To check whether the certificate is installed successfully, verify the data in the Active TLS Certificate section.

   - **If incorrect, click Delete Key and Certificate to remove the self-signed certificate and private key, and then repeat Steps 1-3 to re-create them.**

5. **(Optional) To download the self-signed certificate or private key, click Download Certificate or Download Key in the New TLS Certificate section.**

6. **When prompted to open or save the file, click Save.**

   Note - The Download Key button in the Active TLS Certificate section is for downloading the private key of the currently-installed certificate, not the newly-created one.

Installing or Downloading an Existing Certificate and Key

You can download the already-installed certificate and private key from any HPDU for backup or file transfer. For example, you can install the files onto a replacement HPDU device, and add the certificate to your browser. If valid certificate and private key files are already available, you can install them on the HPDU without going through the process of creating a CSR or a self-signed certificate.

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

1. **To download active key and certificate files from the HPDU, select Device Settings → Security → TLS Certificate.**

a. **In the Active TLS Certificate section, click Download Key and Download Certificate respectively.**

Note - The Download Key button in the New TLS Certificate section, if it displays, is for downloading the newly-created private key, not the currently-installed certificate.

b. **When prompted to open or save the file, click Save.**

2. **To install available key and certificate files on the HPDU, select Device Settings → Security → TLS Certificate.**
3. **Select the Upload Key and Certificate check box at the bottom of the page.**
4. **In the Key File and Certificate File fields, click Browse, and select the key or certificate file or both.**
5. **Click Upload.**
6. **To check whether the certificate is installed successfully, verify the data in the Active TLS Certificate section.**

External Authentication

Note - The HPDU uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Ensure your network infrastructure, such as LDAP and mail services, uses TLS, not SSL 3.0.

For security purposes, users attempting to log in to the HPDU must be authenticated. The HPDU supports the following authentication mechanisms:

- Local user database on the HPDU
- Lightweight Directory Access Protocol (LDAP)
- Remote Access Dial-In User Service (Radius) protocol

By default, the HPDU is configured for local authentication. If you stay with this method, you only need to create user accounts.

If you prefer external authentication, you must provide the HPDU with information about the external Authentication and Authorization (AA) server. If both local and external authentication is needed, create user accounts on the HPDU in addition to providing the external AA server data.

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

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

Note - Only users who have both the Change Authentication Settings and Change Security Settings permissions can configure or modify the authentication settings.

▼ Enabling External Authentication

1. **Collect the external AA server information.**
2. **Enter the required data for external AA server(s) on the HPDU.**
3. **If both the external and local authentication are needed, or you have to return to the local authentication only, see "Managing External Authentication Settings" on page 111.**

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

If you force the HPDU to use a specific AES cipher, for information on configuring AES settings, refer to the client documentation.

LDAP and Radius Information

You must know the AA server settings to configure the HPDU for external authentication. If you are not familiar with these settings, consult your AA server administrator for help.

Information needed for LDAP authentication:

- IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over TLS) is being used
- If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- Network port used by the LDAP server

- Type of LDAP server, usually one of the following options:
  - OpenLDAP – For the Bind Distinguished Name (DN) and password, consult with the LDAP administrator.
  - Microsoft Active Directory (AD) – For Active Directory Domain name, consult with your AD administrator.

Information needed for Radius authentication:

- IP address or host name of the Radius server
- Authentication protocol used by the Radius server
- Shared secret for a secure communication
- UDP authentication port and accounting port used by the Radius server

▼ Adding LDAP/LDAPS Servers

1. **Select Device Settings → Security → Authentication.**

2. **Click New in the LDAP Servers section.**

3. **Enter the required information.**

LDAP/LDAPS Server Information	Description
IP Address/Hostname	IP address or hostname of your LDAP/LDAPS server. ■ Without encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.
Copy Settings from Existing LDAP Server	Appears only when there are existing AA server settings on the HPDU. To duplicate any existing AA server settings, see "Duplicating LDAP/LDAPS Server Settings" on page 109.
Type of LDAP Server	Select one of the following options: ■ OpenLDAP

LDAP/LDAPS Server Information	Description
	■ Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
Security	Determine whether you want to use Transport Layer Security (TLS) encryption, which allows the HPDU to communicate securely with the LDAPS server. Options: ■ StartTLS ■ TLS ■ None
Port (None/StartTLS)	Default Port is 389. Use the standard LDAP TCP port or specify a different port.
Port (TLS)	Configurable only when TLS is selected in the Security field. The default is 636. Use the default port or specify a different port.
Enable Verification of LDAP Server Certificate	Select this option if it is required to validate the LDAP server certificate by the HPDU before the connection. If the certificate validation fails, the connection is refused.
CA Certificate	Consult with your AA server administrator to get the CA certificate file for the LDAPS server. Click Browse, and select and install the certificate file.

LDAP/LDAPS Server Information	**Description**
	■ Click Show to view the installed certificate content. ■ Click Remove to delete the installed certificate if it is inappropriate.
Allow Expired and Not Yet Valid Certificates	■ Select this option to make the authentication succeed regardless of the certificate validity period. ■ If you deselect this option, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Anonymous Bind	Enables or disables anonymous bind. When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this option.
Bind DN	Required after deselecting the Anonymous Bind option. Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base.
Bind Password, Confirm Bind Password	Required after deselecting the Anonymous Bind option. Enter the Bind password.
Base DN for Search	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search. ■ Example: ou=dev, dc=example,dc=com
Login Name Attribute	Attribute of the LDAP user class which is the login name. Usually it is the uid.

LDAP/LDAPS Server Information	Description
User Entry Object Class	Object class for user entries. Usually it is inetOrgPerson.
User Search Subfilter	Search criteria for finding LDAP user objects in the directory tree.
Active Directory Domain	Active Directory Domain name. Example: testradius. com.

4. **To verify if the authentication configuration is set correctly and the HPDU can connect to the new server successfully, click Test Connection.**

   Note - You also can test the connection on the Authentication page after finishing adding servers.

5. **Click Add Server.**

   The new LDAP server appears on the Authentication page.

6. **To add more servers, repeat Steps 1-5.**

7. **In the Authentication Type field, select LDAP. Otherwise, the LDAP authentication does not work.**

8. **Click Save.**

   The LDAP authentication is now in place.

▼ Duplicating LDAP/LDAPS Server Settings

When you add an LDAP/LDAPS server to the HPDU, and that server shares identical settings with an existing server, you can duplicate that LDAP/LDAPS server settings and modify the IP address and host name.

1. **Select Device Settings → Security → Authentication.**

2. **Click New in the LDAP Servers section.**

3. **Select Copy settings from existing LDAP server.**

4. **Click the Select LDAP Server field to select the LDAP/LDAPS server whose settings you want to copy.**

5. **Modify the IP Address/Hostname information.**

6. **Click Add Server.**

> **Note -** If the HPDU clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, might be expired. To ensure proper synchronization, administrators must configure the HPDU and the LDAP server to use the same NTP server(s).

Adding Radius Servers

1. **Select Device Settings → Security → Authentication.**

2. **Click New in the Radius section.**

3. **Enter the required information.**

Radius Server Setting	Description
IP Address/Hostname	IP address or hostname of your Radius server.
Type of RADIUS Authentication	Select an authentication protocol. ■ PAP (Password Authentication Protocol) ■ CHAP (Challenge Handshake Authentication Protocol) **Note -** CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear. ■ MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol) **Note -** MS-CHAPv2 provides stronger security than the above two. Selecting this option supports both

Radius Server Setting	Description
	MS-CHAPv1 and MS-CHAPv2.
Authentication Port, Accounting Port	Defaults are standard ports -- 1812 and 1813. To use non-standard ports, type a new port number.
Timeout	sets the maximum amount of time to establish contact with the Radius server before timing out. Type the timeout period in seconds.
Retries	Type the number of retries.
Shared Secret, Confirm Shared Secret	Necessary to protect communication with the Radius server.

4. **To verify if the authentication configuration is set correctly and check whether the HPDU can connect to the new server successfully, click Test Connection.**

   Note - You also can test the connection on the Authentication page after you finish adding servers.

5. **Click Add Server.**

   The new Radius server appears on the Authentication page.

6. **To add more servers, repeat Steps 1-5.**

7. **In the Authentication Type field, select Radius. Otherwise, the Radius authentication does not work.**

8. **Click Save.**

▼ Managing External Authentication Settings

1. **Select Device Settings → Security → Authentication to open the Authentication page.**

2. **Select a server in the list.**

3. **Enable both the external and local authentication.**

    a. **In the Authentication Type field, select the external authentication you want: LDAP or Radius.**

    b. **Select Use Local Authentication if Remote Authentication is not available.**

    The HPDU always tries external authentication first. When external authentication fails, the HPDU switches to local authentication.

    c. **Click Save.**

4. **Edit or delete a server:**

    a. **Click Edit, make any changes, and click Modify Server to save the changes.**

    b. **Click Delete to delete the server, and confirm the operation.**

    c. **Click Test Connection to test the connection to the selected server. User credentials might be required.**

    d. **To sort the access order of servers, click the Up arrow or Down arrow, which determines the access priority, and click Save Order.**

5. **Test the connection to a server.**

Note - When the HPDU is successfully connected to one external authentication server, it stops trying to access the remaining servers in the authentication list, regardless of the user authentication result.

6. **To disable external authentication without removing the servers:**

    a. **For the Authentication Type, select Local.**

    b. **Click Save.**

Login Settings

- Configure the user blocking feature, which applies only to local authentication instead of external authentication through AA servers.

- Determine the timeout period for any inactive user.
- Prevent simultaneous logins using the same login name.

▼ Configuring User Blocking

1. **Select Device Settings → Security → Login Settings to open the Login Settings page.**

2. **Select Block user on login failure.**

3. **For the Maximum number of failed logins, type a number.**

4. **To determine how long the user is blocked, for Block timeout, type a value or click the Up arrow or Down arrow and select a time option.**

   Note - If you type a time value, include a time unit, such as 4 min.

   ---

5. **Click Save.**

   Note - If any user blocking event occurs, you can unblock that user manually by using the unblock CLI command over a local connection.

▼ Setting Limitations for Login Timeout and Use of Identical Login Names

1. **To determine how long users are permitted to stay idle before being forced to log out, for the Idle timeout period, type a value, or click the Up arrow or Down arrow and select a time option.**

   Note - If you type a time value, include a time unit, such as 4 min.

   Keep the idle timeout to 20 minutes or less, if possible, to reduce the number of idle sessions connected, and the number of simultaneous commands sent to the HPDU.

   ---

2. **Select Prevent concurrent login with same username, if intending to prevent multiple persons from using the same login name simultaneously.**

3. **Click Save.**

Configuring Password Policy

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the HPDU device.

- Force users to use strong passwords.
- Force users to change passwords at a regular interval -- that is, password aging.

1. **To configure password aging, select Device Settings → Security → Password Policy to open the Password Policy page.**
2. **For Password Aging, select Enabled.**
3. **To determine how often users are requested to change their passwords, for the Password Aging Interval, type a value or click the Up arrow or Down arrow and select a time option.**

   Note - If you type a time value, include a time unit. For example, 10 days is 10 d.

4. **Click Save.**

Forcing Users to Create Strong Passwords

1. **To activate the strong password setting, for Strong Passwords, select Enabled.**

   Default settings:

   - **Minimum length** – 8 characters
   - **Maximum length** – 32 characters

     Note - The maximum password length for strong passwords is 64 characters.

   - **Characters** – At least one lowercase character, uppercase character, numeric character, or special character
   - **Number of forbidden previous passwords** – 5

2. **Make any changes to the default settings.**

3. **Click Save.**

▼ Enabling the Service Agreement

The restricted service agreement forces users to read a security agreement when they log in to the HPDU. Users must accept the agreement, or they cannot log in.

1. **Click Device Settings → Security → Service Agreement.**
2. **Select Enforce Restricted Service Agreement.**
3. **Edit or paste the content (maximum of 10,000 characters).**
4. **Click Save.**
   An event notifying you if a user accepted or declined the agreement can be generated.

▼ Configuring Login Manner after Enabling the Service Agreement

1. **After you enable the is displays on the login screen.**
2. **With the service agreement content onscreen, do one of the following, or the login fails.**

   - **Web interface – Select I understand and accept the Restricted Service Agreement.**

   Note - To select the agreement check box using the keyboard, press Tab to go to the check box and press Enter.

   - **CLI – When the confirmation message, I understand and accept the Restricted Service Agreement displays, type `y`.**

Date and Time

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

▼ Setting the Date and Time

1. **Select Device Settings → Date/Time.**

2. **For the Time Zone, select your time zone.**

3. **If the daylight saving time applies to your time zone, verify that Automatic Daylight Saving Time Adjustment is selected.**
   If the daylight saving time rules do not apply to your time zone, clear the **Automatic Daylight Saving Time Adjustment** check box.

4. **Select the method for setting the date and time.**

5. **To customize the date and time:**

   a. **Select User Specified Time.**

   b. **For the Date, type values using the yyyy-mm-dd format, or click the Up arrow or Down arrow and select a date.**

   c. **For the Time, type values using the hh:mm:ss format, or click the Up arrow or Down arrow to adjust values.**
      The time is measured in a 12-hour format and so you must specify AM or PM by clicking the AM or PM button.

6. **To set the date and time using the NTP server:**

   a. **Select Synchronize with NTP Server.**

   b. **Assign the NTP servers in either of the following ways:**

      - **To use the DHCP-assigned NTP servers, do not enter any NTP servers for the First and Second NTP Server.**
        DHCP-assigned NTP servers are available only when either IPv4 or IPv6 DHCP is enabled.

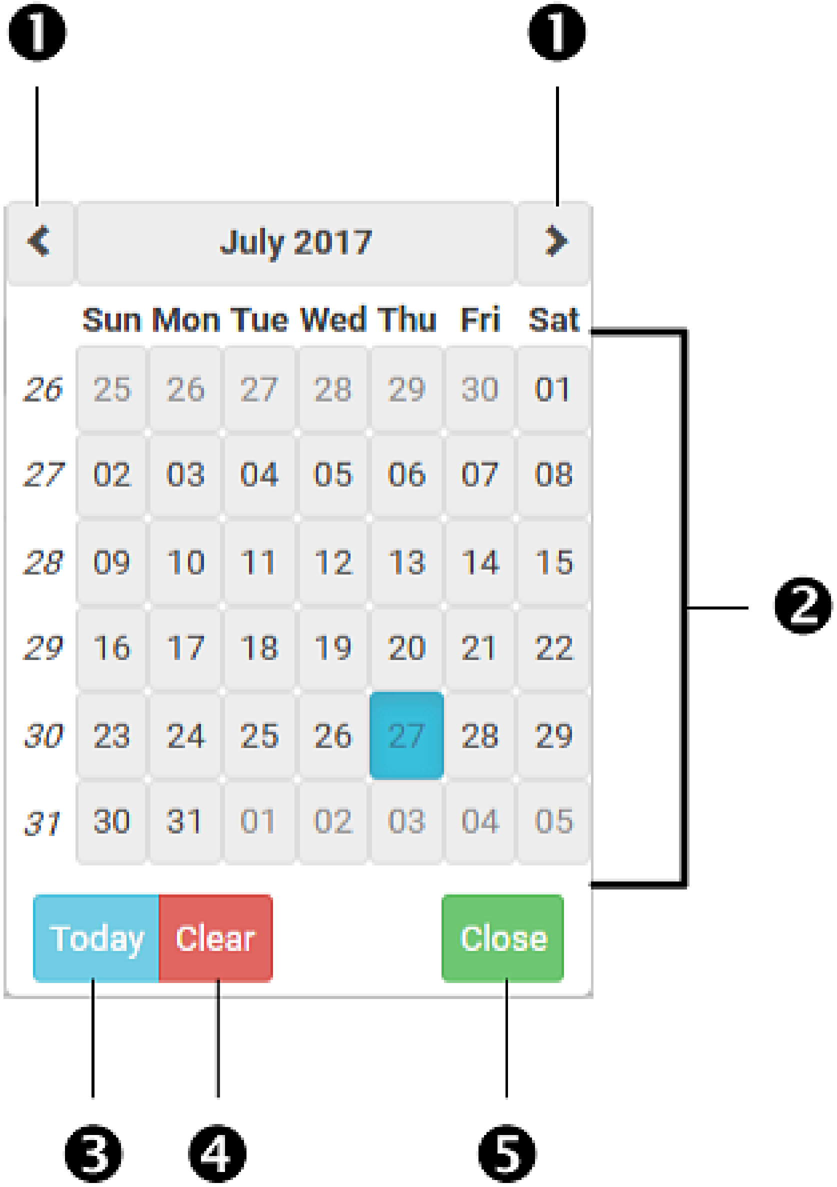
      - **To use the manually-specified NTP servers, specify the primary NTP server in the First Time Server field. A secondary NTP server is optional. Click Check NTP Servers to verify the validity and accessibility of the manually-specified NTP servers.**

7. **Click Save.**

The HPDU follows the NTP server sanity check per the IETF RFC. If the HPDU cannot synchronize with a Windows NTP server, see “Windows NTP Server Synchronization Solution” on page 119.

Viewing the Calendar

The Calendar is a convenient tool to select a custom date. Click the Calendar icon in the Date field to view the calendar.



July 2017

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	25	26	27	28	29	30	01
27	02	03	04	05	06	07	08
28	09	10	11	12	13	14	15
29	16	17	18	19	20	21	22
30	23	24	25	26	27	28	29
31	30	31	01	02	03	04	05

Number	Item	Description
1	Arrows	Switch between months.

Number	Item	Description
2	Dates (01-31)	All dates of the selected month. To select a date, click it.
3	Today	Select today's date.
4	Clear	Clear the entry, if any, in the Date field.
5	Close	Close the calendar.

Windows NTP Server Synchronization Solution

The NTP client on the HPDU follows the NTP RFC and so the HPDU rejects any NTP servers whose root dispersion is more than one second. An NTP server with a dispersion of more than one second is considered an inaccurate NTP server by the HPDU. For information on NTP RFC, visit `https://tools.ietf.org/html/rfc4330`.

Windows NTP servers might have a root dispersion of more than one second, and therefore cannot synchronize with the HPDU. When the NTP synchronization issue occurs, change the dispersion settings to resolve it.

▼ Changing the Windows NTP Root Dispersion Settings

1. **Access the registry settings associated with the root dispersion on the Windows NTP server, `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config`.**

2. **Set AnnounceFlags to either of the following values:**

   - **0x05 = 0x01 (Always time server) and 0x04 (Always reliable time server)**
   - **0x06 = 0x02 (Automatic time server) and 0x04 (Always reliable time server)**

   Note - Do not use 0x08 (Automatic reliable time server) because its dispersion starts at a high value and gradually decreases to one second or lower.

3. **Set LocalClockDispersion to 0.**

Event Rules and Actions

The HPDU can notify you of or react to a change in conditions. This event notification or reaction is an event rule.

An event rule consists of two parts:

- **Event** – HPDU or a device connected to the HPDU meets a certain condition. For example, the inlet voltage reaches the warning level.
- **Action** – Response to the event. For example, the HPDU notifies the system administrator of the event through email. If you want the HPDU to perform one action at a regular interval instead of waiting until an event occurs, you can schedule that action. For example, schedule a recurring action where the HPDU emails the temperature report every hour.

▼ Creating an Event Rule

1. **Verify that you have Administrator Privileges to configure event rules.**

2. **Select Device Settings → Event Rules.**

3. **If needed, to create a new action:**

   a. **Click + New Action.**

   b. **Assign a name to this action.**

   c. **Select the action and configure it as needed.**

   d. **Click Create.**

4. **To create a new rule:**

   a. **Click + New Rule.**

   b. **Assign a name to the rule.**

   c. **Verify that Enabled is selected, or the new event rule does not work.**

   d. **In the Event field, select the event to which you want the HPDU to react.**

e. **In the Available Actions field, select the action(s) to respond to the selected event.**

f. **Click Create.**

▼ Creating a Scheduled Action

1. **If needed, click + New Action to create a new action.**
2. **Click + New Scheduled Action.**
3. **Assign a name to the scheduled action.**
4. **Ensure Enabled is selected, or the HPDU does not perform this scheduled action.**
5. **Set the interval time, which ranges from every minute to yearly.**
6. **In the Available Actions field, select the action(s).**
7. **Click Create.**

Built-in Event Rules and Rule Configuration

The HPDU ships with four built-in event rules, which you cannot delete. If the built-in event rules are not what you need, create new rules.

Built-In Event Rule	**Description**
System Event Log	Causes any event that occurred on the HPDU to be recorded in the internal log (enabled by default).
System SNMP Notification	Causes SNMP traps or informs to be sent to specified IP addresses or hosts when any event occurs on the HPDU (disabled by default).

Built-In Event Rule	Description
System Tamper Detection Alarmed	Causes the HPDU to send alarm notifications if a DX tamper sensor is connected and the HPDU detects that the tamper sensor enters the alarmed state (enabled by default).
System Tamper Detection Unavailable	Causes the HPDU to send alarm notifications if a DX tamper sensor was once connected or remains connected but the HPDU does not detect the presence of the tamper sensor (enabled by default).

Selecting a Trigger Condition for an Event

Depending on the event you select, the Trigger conditions might be available.

Event Type	Trigger Condition
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	■ **Asserted** – The HPDU takes the action only when the selected event occurs. The status of the event transits from false to true. ■ **Deasserted** – The HPDU takes the action only when the selected event disappears or stops. The status of the selected event transits from true to false. ■ **Both** – The HPDU takes the action both when the event occurs (asserts) and when the event stops or disappears (deasserts).
State sensor state change	■ **Alarmed/Open/On** – The HPDU takes the action only when the selected sensor enters the alarmed, open, or on state. ■ **No longer alarmed/Closed/Off** – The HPDU takes the action only when the selected sensor returns to the normal, closed, or off state. ■ **Both** – The HPDU takes the action whenever the selected sensor switches its state.
Sensor availability	■ **Unavailable**: – The HPDU takes the action only when the selected sensor is not detected and becomes unavailable. ■ **Available**: – The HPDU takes the action only when the selected sensor is detected and becomes available. ■ **Both**: – The HPDU takes the action both when the selected sensor becomes unavailable or available.

Event Type	Trigger Condition
Network interface link state	■ **Link state is up**: – The HPDU takes the action only when the network link state changes from down to up. ■ **Link state is down**: – The HPDU takes the action only when the network link state changes from up to down. ■ **Both**: – The HPDU takes the action whenever the network link state changes.
Function enabled or disabled	■ **Enabled**: – The HPDU takes the action only when the selected function is enabled. ■ **Disabled**: – The HPDU takes the action only when the selected function is disabled. ■ **Both**: – The HPDU takes the action when the selected function is either enabled or disabled.
Restricted service agreement	■ **Accepted**: – The HPDU takes the action only when the specified user accepts the restricted service agreement. ■ **Declined**: – The HPDU takes the action only when the specified user rejects the restricted service agreement. ■ **Both**: – The HPDU takes the action both when the specified user accepts or rejects the restricted service agreement.
Server monitoring event	■ **Monitoring started**: – The HPDU takes the action only when the monitoring of any specified server starts. ■ **Monitoring stopped**: – The HPDU takes the action only when the monitoring of any specified server stops. ■ **Both**: – The HPDU takes the action when the monitoring of any specified server starts or stops.
Server reachability	■ **Unreachable**: – The HPDU takes the action only when any specified server becomes inaccessible. ■ **Reachable**: – The HPDU takes the action only when any specified server becomes accessible. ■ **Both**: – The HPDU takes the action when any specified server becomes either inaccessible or accessible.

Default Log Messages

The default log messages are recorded internally and emailed to specified recipients when HPDU events occur (are true) or, in some cases, stop or become unavailable (are false).

Available Actions

The HPDU comes with three built-in actions, which you cannot delete. You can create additional actions for responding to different events.

- **System Event Log** – Records the selected event in the internal log when the event occurs.
- **System SNMP Notification Action** – Sends SNMP notifications to one or multiple IP addresses after the selected event occurs.

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

- **System Tamper Alarm** – Causes the HPDU to show the alarm for the DX tamper sensor, if any, on the Dashboard page until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules.

▼ Creating an Action

1. **Select Device Settings → Event Rules → + New Action.**

2. **Click Action and select an action type.**

   The following table contains the available actions with their functions.

Action	Function
Alarm	Requires the user to acknowledge the alert after it is generated. If needed, you can have the alert notifications regularly generated until a person takes the acknowledgment action.
Execute an action group	Creates a group of actions comprising existing actions.
Log event message	Records the selected events in the internal log.
Push out sensor readings	Sends internal sensor log, environmental sensor log or asset management strip data to a remote server using HTTP POST requests.
Send email	Emails a textual message.
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors.
Send SMS message	Sends a message to a mobile phone.

Action	Function
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations.
Start/stop Lua script	If you are a developer who can create a Lua script, you can upload it to the HPDU, and have the HPDU automatically perform or stop the script in response to an event.
Syslog message	Makes the HPDU automatically forward event messages to the specified syslog server.

3. **Enter the information as needed and click Create.**

4. **Assign the newly-created action to an event rule or schedule it.**

Alarm

The Alarm is an action that requires users to acknowledge an alert. This helps ensure that the user is aware of the alert.

If the Alarm action has been included in a specific event rule and no one acknowledges that alert after it occurs, the HPDU resends or regenerates an alert notification regularly until the alert is acknowledged or the maximum number of alert notifications is sent.

▼ Setting an Alarm

1. **Select Device Settings → Event Rules → + New Action.**

2. **For the Action type, select Alarm.**

3. **Specify one or more methods to issue the alert notifications.**

   - **In the Alarm Notifications, select each method in the Available field.**

     Available methods vary, depending on how many notification-based actions were created. Notification-based action types include:

     - Syslog message
     - Send email
     - Send SMS message

   - **If no appropriate actions are available, create them first.**

4. **To select methods:**

   - **To select a method, select each one in the Available field.**
   - **To select all available methods, click Select All.**

5. **To delete methods:**

   - **To delete a method, click the X for the method in the Selected field.**
   - **To delete all methods, click Deselect All.**

6. **To enable notification-resending, select Enable Re-scheduling of Alarm Notifications.**

   a. **For Re-scheduling Period, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly.**

   b. **For Re-scheduling Limit, specify the maximum number of times the alert notification is resent (1 to infinite).**

7. **(Optional) Configure the HPDU to send the acknowledgment notification after the alarm is acknowledged in the Acknowledgment Notifications field.**

   Available methods are identical to those for generating alarm notifications.

   a. **In the Available field, select each methods, or click Select All.**

   b. **In the Selected field, click the X for each method to remove unnecessary ones, or click Deselect All.**

Action Group

You can create an action group that performs up to 32 actions, and assign the set of actions to any event rule rather than selecting all needed actions one by one per rule.

If the needed action is not available yet, create it first.

▼ Creating an Action Group

1. **Select Device Settings → Event Rules → + New Action.**

2. **Select Execute an action group from the Action list.**
3. **To select any action(s), select each one in the Available Actions list, or click Select All.**
4. **To remove any action(s) from the Selected Actions field, click the X for the action, or to remove all actions, click Deselect All.**

Log an Event Message

The Log event message option records the selected events in the internal log.

The default log message generated for each type of event is available in the Default Log Messages section (on page 94).

▼ Pushing Out Sensor Readings

You can configure the HPDU to push sensor log to a remote server after a certain event occurs, including logs of internal sensors. Before creating this action, ensure you defined the destination servers and the data to be sent on the Data Push page.

1. **Select Device Settings → Event Rules → + New Action.**
2. **For Action, select Push out sensor readings.**
3. **For Destination, select a server or host that receives the asset strip data or sensor log. If the destination is not available, specify the destination on the Data Push page.**

Note - To send the data at a regular interval, schedule this action.

▼ Sending Email

1. **Select Device Settings→ Event Rules → + New Action.**
2. **For Action, select Send email.**
3. **In the Recipient Email Addresses field, specify the email address(es) of the recipient(s), with a comma to separate multiple email addresses.**

4. **To specify an SMPT server: .**

   - **To use the SMTP server specified on the SMTP Server page, select Use default settings.**
   - **To use a different SMTP server, select Use custom settings.**

     The fields for customized SMTP settings appear.

   Default messages are sent based on the event.

5. **If needed, create a custom message:**

   a. **Select Use Custom Log Message.**

   b. **Type a custom message up to 1024 characters.**

   c. **Click anywhere inside the text box.**

      The Event Context Information displays, showing a list of placeholders and their definitions.

   d. **Scroll down and select a placeholder.**

   e. **To start a new line in the text box, press Enter.**

Note - To type square brackets [ ] in the custom message for non-placeholder words, add a backslash in front of the square bracket, \[or \], such as \[and]. Otherwise, the message sent does display the square brackets.

Sending a Sensor Report

You can set the HPDU so that it automatically reports the latest readings or states of one or more sensors by sending a message or email or recording the report in a log. The sensor report can contain the following information.

- Inlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor and active energy.
- Overcurrent protector sensors, including RMS current and tripping state.

1. **Select Device Settings → Event Rules → + New Action.**
2. **For Action, select Send sensor report.**

3. **In the Destination Actions section, select the method(s) to report sensor readings or states. The number of available methods varies, depending on how many messaging actions have been created.**

   The messaging action types include:

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

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

5. **To select a method, select each one in the Available field, or to add all available methods, click Select All.**

6. **To delete any method, click the X for a method in the Selected field, or to delete all methods, click Deselect All.**

7. **In the Available Sensors list, select a sensor for the target:**

   a. **Click the first Up or Down arrow (far left) and select a target component.**

   b. **Click the second Up or Down arrow (middle) and select the sensor for the target.**

      For example, to monitor the current reading of the Inlet 1, select Inlet 1 from the left field, and select RMS Current from the right field.

   c. **To report additional sensors simultaneously, repeat the Step 7b to add more sensors.**

   d. **Click + to add the selected sensor to the Report Sensors list.**

8. **To remove any sensor from the Report Sensors list:**

   a. **Select the sensor and click the - (Minus button).**

   b. **To select multiple sensors, press Ctrl+click or Shift+click to highlight the sensors.**

9. **To send the sensor report, click Send Report Now.**

Note - When intending to send a sensor report using custom messages, use the placeholder [SENSORREPORT] to report sensor readings.

▼ Sending an SMS Message

You can configure SMS messages to be sent when an event occurs and can customize the message.

Only the 7-bit ASCII charset is supported for SMS messages. Messages consist of a combination of free text and HPDU placeholders. The placeholders represent information that is pulled from the HPDU and inserted into the message.

A supported modem, such as the Cinterion GSM MC52i modem, must be plugged into the HPDU to send SMS messages.

Note - The HPDU cannot receive SMS messages.

1. **Select Device Settings → Event Rules → + New Action.**
2. **Select Send SMS message in the Action list.**
3. **In the Recipient Phone Number field, specify the phone number of the recipient.**
4. **Create a custom message:**
   a. **Select Use Custom Log Message.**

   b. **Type a custom message up to 1024 characters.**

      For example:

      - [USERNAME] logged into the device on [TIMESTAMP]

        translates to
      - Mary logged into the device on 2012-January-30 21:00

   c. **Click anywhere inside the text box.**

      The Event Context Information displays, showing a list of placeholders and their definitions.

   d. **Scroll down and select a placeholder.**

e. **To start a new line in the text box, press Enter.**

Note - To type square brackets [ ] in the custom message for non-placeholder words, add a backslash in front of the square bracket, \[or \], such as \[and]. Otherwise, the message sent does display the square brackets.

▼ Sending an SNMP Notification

You can send an SNMP notification to one or multiple SNMP destinations.

1. **Select Device Settings → Event Rules → + New Action.**
2. **Select Send SNMP notification in the Action list.**
3. **Select the type of SNMP notification: SNMP v2c or SNMP v3.**
4. **To send SNMP v2c notifications:**

   a. **In the Notification Type field, select SNMPv2c Trap or SNMPv2c Inform.**

   b. **For SNMP INFORM communications, leave the resend settings at their default or continue with Step 4c.**

   c. **In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.**

   d. **In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.**

   e. **In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.**

   f. **In the Port fields, enter the port number used to access the device(s).**

g. **In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the HPDU and all SNMP management stations.**

Note - An SNMP v2c notification action permits only a maximum of three SNMP destinations. To assign more than three SNMP destinations to a specific rule, first create several SNMP v2c notification actions, each of which contains completely different SNMP destinations, and then add all of these SNMP v2c notification actions to the same rule.

---

5. **To send SNMP v3 notifications:**

a. **In the Notification Type field, select SNMPv3 Trap or SNMPv3 Inform.**

b. **For SNMP TRAPs, the engine ID is prepopulated.**

c. **For SNMP INFORM communications, leave the resend settings at their default or continue with Step 5d.**

d. **In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.**

e. **In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.**

f. **For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings.**

- Host name
- Port number
- User ID for accessing the host – Ensure the User ID has the SNMPv3 permission.
- Host security level – For host security levels and next steps, see the following table.

Host Security Level	Description/Next Steps
noAuthNoPriv	No authorization or privacy protocols are needed.
authNoPriv	Authorization is required but no privacy protocols are required.

Host Security Level	Description/Next Steps
	1. Select the authentication protocol: MD5 or SHA. 2. Enter the authentication passphrase and then confirm the authentication passphrase.
authPriv	Authentication and privacy protocols are required. 1. Select the authentication protocol: MD5 or SHA. 2. Enter the authentication passphrase and confirm the authentication passphrase. 3. Select the Privacy Protocol: DES or AES. 4. Enter the privacy passphrase and then confirm the privacy passphrase.

▼ Sending a Syslog Message

You can automatically forward event messages to the specified syslog server. The HPDU might not detect the syslog message transmission failure. If the HPDU detects it, the syslog failure and the reason appear in the event log.

1. **Select Device Settings → Event Rules → + New Action.**

2. **Select Syslog message from the Action list.**

3. **In the Syslog Server field, specify the IP address to which the syslog is forwarded.**

4. **In the Transport Protocol field, select a syslog protocol: TCP, UDP (default) or TCP+TLS and perform the steps in the following table.**

Transport Protocol	Next Steps
UDP	1. In the UDP Port field, type a port number (default is 514). 2. Select Legacy BSD Syslog Protocol, if applicable.
TCP	NO TLS certificate is required. Type a port number in the TCP Port field.
TCP+TLS	A TLS certificate is required. Do the following: 1. Type a port number in the TCP Port field (default is 6514). 2. In the CA Certificate field, click Browse, and select a TLS certificate.

Transport Protocol	Next Steps
	3. Click Show to view the content. 4. Click Remove to delete it if it is not what you want. 5. Determine whether to select Allow expired and not yet valid certificates. 6. To always send the event message to the specified syslog server as long as a TLS certificate is available, select this option. 7. To prevent the event message from being sent to the specified syslog server when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect this option.

▼ Scheduling an Action

An action can be regularly performed at a preset time interval instead of being triggered by a specific event. For example, you can make the HPDU report the reading or state of a specific sensor regularly by scheduling the Send Sensor Report action.

When scheduling an action, ensure you have a minimum of a 1-minute buffer between the action creation and first execution time. Otherwise, the scheduled action is not performed at the specified time when the buffer time is too short. For example, if you want an action to be performed at 11:00 am, finish scheduling it at 10:59 am or earlier.

If the needed action is not available yet, create it first.

An example of the scheduled action is available in the section titled Send Sensor Report Example (on page 94).

1. **Select Device Settings → Event Rules → + New Action.**

2. **To select any action(s), select each one in the Available Actions list, or select all available actions by clicking Select All.**

3. **To remove any action(s) from the Selected Actions field, click the X for that action, or to remove all actions, click Deselect All.**

4. **Select the frequency in the Execution Time field, and specify the time interval or a specific date and time using the frequency settings in the following table.**

Action Execution Time	Frequency Setting
Minutes	Click the Frequency field and select an option.

Action Execution Time	Frequency Setting
	The frequency ranges from every minute, every 5 minutes, every 10 minutes, and continues in 5 minute increments to a maximum of every 30 minutes.
Hourly	Type a value in the Minute field, which is set to either of the following: ■ 0 (zero) value – For example, the action is performed on the hour at 1:00 AM, 2:00 AM, or 3:00 AM. ■ Non-zero value – For example, if it is set to 30, the action is performed on the half hour at 1:30 AM, 2:30 AM, 3:30 AM.
Daily	Type the values or click the Up or Down arrow. The time is measured in 12-hour format and so you must correctly specify AM or PM by clicking the AM/PM button. For example, if you specify 01:30 PM, the action is performed at 13:30 pm every day.
Weekly	Both the day and time must be specified for the weekly option. ■ Days range from Sunday to Saturday. ■ The time is measured in 12-hour format and so you must correctly specify AM or PM by clicking the AM/PM button.
Monthly	Both the date and time must be specified for the monthly option. ■ The dates range from 1 to 31. **Note -** Not every month has the date 31, and February does not have the date 30 or 29. Carefully check the calendar when selecting 29, 30, or 31. ■ The time is measured in 12-hour format and so you must correctly specify AM or PM by clicking the AM/PM button.
Yearly	■ Month – January through December. ■ Day of month – 1 to 31. ■ Time – Uses 12-hour format and so you must correctly specify AM or PM by clicking the AM/PM button.

▼ Placeholders for Custom Messages

The Actions of Send email and Send SMS message allow you to customize event messages.

1. **Click anywhere inside the text box.**

   The Event Context Information displays, showing a list of placeholders and their definitions.

2. **Scroll down and select a placeholder or type a keyword in the search box to find the placeholder.**

3. **If wanted, sort the list by clicking a column header.**

4. **To start a new line in the text box, press Enter.**

   Note - To type square brackets [ ] in the custom message for non-placeholder words, add a backslash in front of the square bracket, \[or \], such as \[and]. Otherwise, the message sent does display the square brackets.

5. **To close the Event Context Information, click anywhere inside the browser window.**

▼ Editing or Deleting a Rule or Action

You can change the settings of an event rule, action, or scheduled action, or delete them.

Note - You cannot configure some settings for built-in event rules or actions. You cannot delete built-in rules and actions.

1. **Select Device Settings → Event Rules.**

2. **Click a rule in the list of rules, actions, or scheduled actions.**

3. **On the setup page, edit or delete the rule or action:**

   - **To modify settings, make any changes and click Save.**

   - **To delete the rule or action, click Delete in the top-right corner, and click Delete to confirm.**

Untriggered Rules

In some cases, a measurement exceeds a threshold causing the HPDU to generate an alert. The measurement then returns to a value within the threshold, but the HPDU does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the HPDU uses.

▼ Configuring Data Logging

The HPDU can store 120 measurements for each sensor in a memory buffer. This memory buffer is known as the data log. Sensor readings in the data log can be retrieved using SNMP.

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field. Since the HPDU internal sensors are measured every second, specifying a value of 60, for example, would cause measurements to be written to the data log once every minute. Since there are 120 measurements of storage per sensor, specifying a value of 60 means the log can store the last two hours of measurements before the oldest one in the log is overwritten.

When measurements are written to the log, three values for each sensor are written: the average, minimum and maximum values. For example, if measurements are written every minute, the average of all measurements that occurred during the preceding 60 seconds along with the minimum and maximum measurement values are written to the log.

Note - The SNMP agent for the HPDU device must be enabled for this feature to work. Using an NTP time server ensures accurately time-stamped measurements.

---

1. **Select Device Settings → Data Logging.**

   Note - By default, data logging is enabled. You must have the Administrator Privileges or Change PDU, Inlet, and Overcurrent Protector Configuration permissions to change the setting.

   ---

2. **To enable the data logging feature, select Enable in the General Settings section.**

3. **Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.**

4. **Verify that all sensor logging is enabled.**

   ⚠ **Caution -** Although it is possible to selectively enable or disable logging for individual sensors on the HPDU, it is not recommended.

   - **To enable all sensors, click Enable All at the bottom of the page.**

- **To select all sensors of the same type, click Logging Enabled in the header row of each section.**

  If the number of sensors exceeds 35 in any section, the remaining sensors appear on next page(s). If so, a pagination bar displays in this section, on which you can click any button to navigate the pages.

5. **Click Save at the bottom of the page.**

Configuring Data Push Settings

You can push the sensor or asset strip data to a remote server for data synchronization. The data is sent in JSON format using HTTP POST requests. You need to set up the destination and authentication for data push on the HPDU.

After configuring the destination and authentication settings, do either, or both of the following:

- To perform the data push after the occurrence of a certain event, create the data push action and assign it to an event rule.
- To push the data at a regular interval, schedule the data push action.

1. **Select Device Settings → Data Push.**
2. **To specify a destination, click + New Destination.**
3. **Set up the URL field.**
   a. **Click the Up or Down arrow and select http or https.**
   b. **Type the URL or host name.**
   c. **If you selected https, click the CA certificate to install it.**
4. **If the destination server requires authentication, select Use Authentication, and enter the User name and password.**
5. **In the Entry Type field, determine the data that will be transmitted.**

Data Push Entry Type	Description
Asset management tag list	Transmit the information of the specified asset strip(s),

Data Push Entry Type	Description
	including the general status of the specified strip(s) and a list of asset tags. The asset tags list also includes the tags on blade extension strips, if any.
Asset management log	Transmit the log of all asset strips, which is generated when there are changes made to asset tags and asset strips, including asset tag connection or disconnection events.
Sensor log	Transmit the record of all logged sensors, including their sensor readings and/or status. Logged sensors refer to all internal and/or environmental sensors/actuators that you have selected on the Data Logging page.

6. **Click Create.**
7. **Repeat Steps 1-6 for additional destinations.**

▼ Modifying or Deleting Data Push Settings

1. **On the Data Push page, click the one you want in the list.**
2. **Perform either of the following actions:**
   - **To modify settings, make any changes, and click Save.**
   - **To delete a data push setting, click Delete, and confirm it.**

Monitor Server Accessibility

You can monitor whether specific IT devices are alive by having the HPDU device continuously ping them. An IT device's successful response to the ping commands indicates that the IT device is still alive and can be remotely accessed. This function is especially useful when you are not located in an area with Internet connectivity.

The HPDU can monitor the accessibility of any IT device, such as database servers, remote authentication servers, and power distribution units (HPDUs), and supports monitoring a maximum of 8 devices.

The default ping settings might not be suitable for monitoring devices that require high connection reliability and so it is recommended that you adjust the ping settings for optimal results.

Note - To make the HPDU automatically log, send notifications or perform other actions for any server monitoring events, you can create event rules.

▼ Adding IT Equipment for Ping Monitoring

1. **Select Device Settings → Server Reachability.**
2. **Click Monitor New Server.**
3. **Verify that Enable ping monitoring for this server (default) is selected.**
4. **Configure the following settings:**

Ping Monitoring Setting	Description
IP address/hostname	IP address or host name of the IT equipment that you want to monitor.
Number of successful pings to enable feature	Number of successful pings required to declare that the monitored equipment is Reachable. Valid range is 0 to 200.
Wait time after successful ping	Wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait time after unsuccessful ping	Wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of consecutive unsuccessful pings for failure	Number of consecutive pings without any response before the monitored equipment is declared Unreachable. Valid range is 1 to 100.
Wait time before resuming pinging after failure	The wait time before the HPDU resumes pinging after the monitored equipment is declared Unreachable. Valid range is 1 to 1200 (seconds).
Number of consecutive failures before disabling feature (0 = unlimited)	Number of times the monitored equipment is declared Unreachable consecutively before the HPDU disables the ping monitoring feature for it and shows Waiting for reliable connection. Valid range is 0 to 100.

5. **Click Create.**

6. **To add more IT devices, repeat Steps 1-5.**

Note - At the beginning of ping monitoring the server, the status of the added IT equipment shows Waiting for reliable connection, which means the requested number of consecutive successful or unsuccessful pings is not reached before the HPDU can declare that the monitored device is reachable or unreachable.

Server Monitoring States and Results

After adding IT equipment for monitoring, all IT devices appear on the Server Reachability page. The Ping Enabled column indicates whether the monitoring for the corresponding IT device is activated or not. The Status column indicates the accessibility of each monitored equipment.

Server Monitoring Status	Description
Reachable	Monitored equipment is accessible.
Unreachable	Monitored equipment is inaccessible.
Waiting for reliable connection	Connection between the HPDU device and the monitored equipment is not reliably established yet.

▼ Editing or Deleting Ping Monitoring Settings

You can edit the ping monitoring settings of any IT device or delete it if no longer needed.

1. **Select Device Settings → Server Reachability.**

2. **Click a monitored IT device in the list.**

3. **Modify or delete the ping monitoring settings.**

   a. **To modify settings, make necessary changes and then click Save.**

   b. **To delete a setting, click the Delete icon in the top-right corner.**

▼ Configuring the Front Panel Settings

1. **Select Device Settings → Front Panel.**

2. **To configure the default view of the LCD display, select one of the following modes.**

Front Panel Mode	Data Entered
Automatic mode (default)	LCD display cycles through both the inlet and overcurrent protector information. **Note -** Overcurrent protector information is available only when you HPDU has overcurrent protectors.
Inlet overview	LCD display cycles through only the inlet information.

▼ Configuring the Serial Port

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

The HPDU supports the following devices through the serial interface:

- Computer or KVM product for console management.
- Analog modem for remote dial-in and access to the CLI.
- GSM modem for sending out SMS messages to a cellular phone.

Bit-rate adjustment may be necessary. Change the bit rate before connecting the supported device to the HPDU through the serial port, or there are communication problems.

You can set diverse bit-rate settings for console and modem operations. Usually the HPDU can detect the device type, and automatically apply the preset bit rate.

The HPDU indicates the detected device in the Port State section of the Serial Port page.

1. **To configure serial port or modem settings, select Device Settings → Serial Port.**

2. **To change the serial port baud rate settings, click Connected device, and select any of the following settings to make the serial port enter an appropriate state.**

Serial Port Setting	Description
Automatic detection	HPDU automatically detects the type of the device connected to the serial port. Select this option unless your HPDU cannot correctly detect the device type.
Force console	HPDU attempts to recognize that the connected device is set for the console mode.

Serial Port Setting	Description
Force analog modem	HPDU attempts to recognize that the connected device is an analog modem.
Force GSM modem	HPDU attempts to recognize that the connected device is a GSM modem.

3. **Click Console Baud Rate and select the baud rate for console management.**

   Note - For a serial RS-232 or USB connection between a computer and the HPDU, leave it at the default, 115200 bps.

4. **Click Modem Baud Rate and select the baud rate for the modem connected to the HPDU.**

   After the HPDU detects the connection of an analog or GSM modem, the modem settings appear in the web interface.

5. **To configure the analog modem:**

   a. **Select Answer incoming calls to enable the remote access through a modem. Otherwise, deselect it.**

   b. **Type a value in the Number of rings before answering field to determine the number of rings the HPDU must wait before answering the call.**

6. **To configure the GSM modem:**

   a. **Enter the SIM PIN code.**

   b. **Select Use custom SMS center number if a custom SMS center is used.**

   c. **Enter the SMS center number in the SMS center field.**

7. **If needed, click Advanced Information to view detailed information about the modem, SIM, and mobile network.**

8. **To test whether the HPDU can successfully send out SMS messages with the modem settings:**

   a. **Enter the phone number of the recipient in the Recipient Phone field.**

   b. **Click Send SMS Test to send a test SMS message.**

Lua Scripts

If you can write or obtain any Lua scripts, you can create or load them into the HPDU to control its behaviors.

You must have Administrator Privileges to manage Lua scripts.

▼ Writing or Loading a Lua Script

You can enter or load up to 4 scripts to the HPDU.

Note - If you can no longer enter or load a new script after reaching the upper limit, you can either delete any script or modify or replace script codes.

1. **Select Device Settings → Lua Scripts → + Create New Script.**

2. **Type a name for this script. Its length ranges between 1 to 63 characters.**

   The name must contain only alphanumeric characters, underscore (_), and minus (-), with no spaces.

3. **Determine whether and when to automatically execute the loaded script.**

Lua Script Setting	Description
Start automatically at system boot	When the HPDU reboots, the script is automatically executed.
Restart after termination	Script is automatically executed each time after 10 seconds since the script execution finishes.

4. **(Optional) Determine the arguments that will be executed by default.**

   a. **Click + Add argument.**

   b. **Type the key and value.**

   c. **Repeat Steps 4a and 4b to enter more arguments as needed.**

   d. **To remove an argument, click - (Minus button) next to it.**

Note - Default arguments are overridden by the new arguments specified with the Start with Arguments command or with any Lua-script-related event rule.

5. **In the Source Code section, do one of the following. It is recommended to leave the Enable Syntax Highlighting check box selected unless you do not need different text colors to identify diverse code syntaxes.**

   - **To write a Lua script, type the codes in the Source Code section.**
   - **To load an existing Lua script file, click Load Local File.**
   - **To use one of the Lua script examples, click Load Example.**

Caution - The new script overwrites all codes in the Source Code section. Therefore, do not load a new script if the current script meets your needs.

6. **Click Create.**
7. **To execute the newly-added script immediately, click Start or the three vertical dots → Start with Arguments.**
8. **To add more scripts, return to the scripts list by clicking Lua Scripts at the top of the page or in the Menu, and repeat Steps 1-7.**

Automatically Starting or Stopping a Lua Script

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

1. **Select Device Settings → Event Rules → + New Action.**
2. **Select Start/stop Lua script from the Action list.**
3. **In the Operation field, select Start Script or Stop Script.**
4. **In the Script field, select the script that you want it to be started or stopped when an event occurs.**

Note - If you did not create or load a script into the HPDU, a script does not appear in the Script list.

---

5. **To apply different arguments other than the default, perform these steps.**

   a. **Click + Add argument**

   b. **Type the key and value.**

   c. **If you need to enter additional arguments, repeat Steps 6a-6b.**

Note - The new arguments override the Lua script default arguments.

---

6. **To remove an argument, click the - (Minus button) next to the argument.**

▼ Manually Starting or Stopping a Lua Script

You can manually start or stop an existing Lua script at any time.

When starting a script, you can select to start it either with its default arguments or with new arguments.

Note - To have the HPDU automatically start or stop a script in response to an event, create an event rule.

---

1. **Select Device Settings → Lua Scripts.**
2. **In the Lua scripts list, click the script whose state is either Terminated or New.**
3. **To start the script using arguments, do either of the following:**

   - **To start with default arguments, click Start.**
   - **To start with new arguments, click the three vertical dots → Start with Arguments, and enter the key and value. If needed, click + Add Argument to add more arguments.**

Note - Newly-assigned arguments override default ones.

---

4. **Click Start.**

   The script output appears in the Script Output section.

5. **If needed, click Clear to delete the existing output data.**

6. **To manually stop a script:**

   a. **Select Device Settings → Lua Scripts.**

   b. **Click the script whose state is either Running or Restarting.**

   c. **Click Stop in the top-right corner.**

   d. **Click Stop to confirm.**

7. **To return to the scripts list, click Lua Scripts at the top of the page or in the Menu.**

▼ Checking Lua Scripts States

1. **Select Device Settings → Lua Scripts to show the scripts list, which indicates the current state and settings of each script.**

   Four script states are available.

State	Description
New	Script is never executed since the device boot.
Running	Script is being executed.
Terminated	Script was executed, but stops now.
Restarting	Script is executed. Only the scripts with the Restart column set to Yes show this state.

2. **Verify the following settings:**

   - **Autostart** – Indicates whether the Start automatically at system boot option is enabled.
   - **Restart** – Indicates whether the Restart after termination option is enabled.

▼ Modifying or Deleting a Lua Script

You can edit the codes in a Lua script, replace the script with a new one, or delete a script you no longer need.

1. **To modify or replace a script:**

   a. **Select Device Settings → Lua Scripts.**

   b. **Click the script you want to modify or replace.**

   c. **Click ? → Edit Script.**

   d. **Make changes to the information, except for the script name, which you cannot change.**

   e. **To replace the script, click Load Local File or Load Example, and select a new script.**

2. **To delete a script:**

   a. **Select Device Settings → Lua Scripts.**

   b. **Click the script you want to delete.**

   c. **Click ? → Delete.**

   d. **Click Delete to confirm.**

3. **To return to the scripts list, click Lua Scripts at the top of the page or in the Menu.**

Cisco EnergyWise

If Cisco EnergyWise energy management architecture is implemented, you can enable the Cisco EnergyWise endpoint implemented on the HPDU so that this HPDU becomes part of the Cisco EnergyWise domain.

▼ Enabling Cisco EnergyWise

1. **To enable Cisco EnergyWise:**

   a. **Select Device Settings → Miscellaneous.**

   b. **Select Enable EnergyWise.**

2. **To configure Cisco EnergyWise, change any of the following settings, and click Save in the EnergyWise section.**

Cisco EnergyWise Setting	Description
Domain name	Type the name of a Cisco EnergyWise domain where the HPDU belongs. ■ Up to 127 printable ASCII characters. ■ No spaces or asterisks.
Domain password	Type the authentication password (secret) for entering the Cisco EnergyWise domain ■ Up to 127 printable ASCII characters. ■ No spaces or asterisks.
Port	Type a User Datagram Protocol (UDP) port number for communications in the Cisco EnergyWise domain. ■ Range from 1 to 65535. ■ Default is 43440.
Polling interval	Type a polling interval to determine how often the HPDU is queried in the Cisco EnergyWise domain. ■ Range from 30 to 600 ms. ■ Default is 180 ms.

Maintenance

In the Maintenance Menu, you can view the device information, connected users, event log, and firmware history. You also can update the HPDU firmware.

Viewing Device Information

1. **To view hardware and software information of components or peripheral devices connected to your HPDU, select Maintenance → Device Information.**

2. **Click the title bar of the device information section to display the information. For example, click the Network section.**

Note - The number of available sections is HPDU model dependent. If the information on the page does not match the latest status, press F5 to reload it.

Device Information Section	Description
Information	General device information, such as model name, serial number, firmware version, hardware revision, and MIB download link(s).
Network	Current networking mode, IPv4 and/or IPv6 addresses.
Overcurrent Protectors	Each overcurrent protector type, rated current, and the outlets that it protects.
Controllers	Each inlet or outlet controller serial number, board ID, firmware version and hardware version.
Inlets	Each inlet plug type, rated voltage, and current.

Viewing and Managing Connected Users

You can check which users logged in to the HPDU device and their status. If you have administrator privileges, you can terminate any user connection to the HPDU.

1. **Select Maintenance → Connected Users.**
   A list of logged-in users displays.

Column	Description
User name	Login name of each connected user.
IP Address	IP address of each user host. For the login through a local connection (serial RS), <local> displays instead of an IP address.
Client Type	Web GUI or CLI interface through which the user is being connected to the HPDU. The CLI client type

Column	Description
	shows how the user is connected to the CLI: Serial local connection, such as the serial RS-232 connection, SSH connection, or Telnet connection.
Idle Time	Length of time for which a user remains idle.

2. **If needed, sort the list by clicking a column header.**

3. **To disconnect any user, click the corresponding ?.**

4. **Click Disconnect to confirm.**

   The disconnected user is forced to log out.

Viewing or Clearing the Local Event Log

By default, the HPDU captures certain system events and saves them in a local (internal) event log. You can view over 2,000 historical events that occurred on the HPDU in the local event log. When the log size exceeds 256KB, each new entry overwrites the oldest one.

1. **Select Maintenance → Event Log.**

   Each event entry consists of the following information:

   - ID number of the event
   - Date and time of the event

   Note - The date and time that appears in the HPDU web interface are automatically converted to your computer time zone. To avoid any time confusion, you can apply the same time zone settings as those of the HPDU to your computer.

   - Event type
   - Description of the event

2. **To view a specific type of events only, select the event type in the Filter Event Class field.**

   The event log is refreshed in real time whenever new events occur.

3. **To avoid any interruption during data browsing, you can suspend the real-time update by clicking ?.**

4. **To restore real-time update, click ?.**

Those events that are not listed yet due to suspension are displayed in the log now.

5. **To navigate the log:**

   a. **To go to other pages in the log, click the pagination bar at the bottom of the page.**

   b. **When there are more than 5 pages and the page numbers listed do not show the page you want, click the ellipsis button (…) to display the next or previous five page numbers in the bar, if available.**

6. **If wanted, sort the list by clicking a column header.**

7. **To clear the local log:**

   a. **Click ? in the top-right corner.**

   b. **Click Clear Log in the confirmation message.**

▼ Updating the HPDU Firmware

When performing a firmware upgrade, the HPDU keeps the power status of each outlet unchanged so that no server operation is interrupted. During and after the firmware upgrade, outlets that were powered before the firmware upgrade remain powered on and outlets that were powered off remain powered off. You must be the administrator or a user with the Firmware Update permission to update the HPDU firmware.

The HPDU web-interface-based firmware upgrade time varies from unit to unit, depending on various external and internal factors. Upgrades through other management systems, such as Sunbird Power IQ, may take additional time beyond the control of the HPDU itself.

External factors include, but are not limited to: network throughput, firmware file size, and speed at which the firmware is retrieved from the storage location. Internal factors include: the necessity of upgrading the firmware on the microcontroller and the number of microcontrollers that require an upgrade (depending on the number of outlets). The microcontroller is upgraded only when required. The length of firmware upgrade time ranges from approximately 3 minutes (without any microcontroller updated) to almost 7 minutes (with all microcontrollers for 48 outlets updated). Take the above factors into account when estimating the HPDU firmware upgrade time.

1. **Select Maintenance → Update Firmware.**

2. **Click ? and select a firmware file.**

3. **Click Upload.**

   When the progress bar indicates that the upload is complete, information of both installed and uploaded firmware versions and compatibility and signature-checking results display.

4. **If anything is incorrect, click Discard Upload.**

5. **To proceed with the update, click Update Firmware.**

⚠ **Caution -** Warning: Do not power off the HPDU during the update.

During the firmware update process, the following actions occur:

- Progress bar appears in the web interface, indicating the update status.
- Front panel display shows the firmware upgrade message.
- Outlet LEDs blink if the relay boards are being updated. If the firmware update does not include the update of the relay board firmware, outlet LEDs do not blink.
- No users can successfully log in to the HPDU.
- Other user operations, if any, are forced to suspend.
- When the update is complete, the HPDU resets, and the Login page appears.
- Other logged-in users are logged out when the firmware update is complete.

Note - If you are using the HPDU with an SNMP manager, download its MIB again after the firmware update to ensure your SNMP manager has the correct MIB for the latest release you are using.

To use a different method to update the firmware, see "Firmware Update through SCP" on page 259 or "Bulk Configuration or Firmware Upgrade through DHCP/TFTP" on page 159.

▼ View Firmware Update History

The firmware upgrade history is permanently stored on the HPDU. It remains available even though you perform a device reboot or any firmware update.

1. **Select Maintenance → Firmware History.**

   Each firmware update event includes:

- Update date and time
- Previous firmware version
- Update firmware version
- Update result

2. **If wanted, sort the list by clicking a column header.**

Bulk Configuration

The Bulk Configuration feature allows you save generic settings of a configured HPDU device to your computer. You can use this configuration file to copy common settings to other HPDU devices of the same model and firmware version.

A source device is the HPDU device where the configuration file is downloaded/saved. A target device is the HPDU device that loads the configuration file.

By default, the configuration file downloaded from the source device contains settings based on the built-in bulk profile. The built-in bulk profile defines that all settings must be saved except for device settings. The device settings, such as the device IP address or environmental sensor settings, are not included into any profile and so they are not downloaded from any source device.

You can decide which settings are downloaded and which are not by creating your own bulk configuration profile.

When the date and time settings are included in the bulk configuration file, exercise caution when distributing that file to target devices located in a different time zone than the source device.

Note - To back up or restore all settings, including device settings, use Backup/Restore feature instead.

Bulk Configuration Methods

If you must set up multiple HHPDU devices, use one of the following configuration methods to save time.

Bulk configuration file downloaded from one HHPDU

- Requirement: All HHPDU devices to configure are of the same model and firmware.

- Procedure: First finish configuring one HHPDU. Then download the bulk configuration file from it and copy the file to all other HHPDU devices.

TFTP server

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

▼ Configuring Main Bulk

1. **If you prefer customizing the bulk configuration file, create your own bulk configuration profile(s) first.**
2. **Perform the bulk configuration operation, which includes the following steps.**
3. **Make sure the desired bulk configuration profile has been selected on the source device.**
4. **Save a bulk configuration file from the source device.**
5. **Perform bulk configuration on one or multiple target devices.**

Note - On startup, the HPDU performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the Bulk configuration copied event is logged only when the new configuration file contains the Bulk configuration copied event rule.

If you copied any bulk configuration or device backup file to the HPDU, the last record displays at the bottom of both the Bulk Configuration and Backup/Restore pages.

Note - The date and time shown on the HPDU web interface are automatically converted to your time zone that you set on your computer. To avoid any time confusion, you can apply the same time zone settings as those of the HPDU to your computer.

Bulk Configuration Restrictions

Before performing bulk configuration, ensure your source and target devices are compatible devices for sharing general settings.

Restrictions for bulk configuration:

- Target device must be running the same firmware version as the source device.
- Target device must be the same model type as the source device.
- Bulk configuration is permitted if the differences between the target and source devices are only mechanical designs that are indicated in the model name suffix. For example, you can perform bulk configuration between PX2-4724-E2N1K2 and PX2-4724-E2N1K9 because the only difference between the two models is their chassis colors represented by K2 (blue) and K9 (gray).

▼ Creating or Customizing Bulk Configuration Profiles

A bulk profile defines which settings are downloaded or saved from the source device and which are not. The default is to apply the built-in bulk profile, which downloads all settings from the source device except for device data.

If the built-in profile does not meet your needs, you can create your own profile(s), and apply the wanted profile before downloading or saving any settings from the source device.

1. **Log in to the source HPDU device, whose settings you want to download.**
2. **Select Maintenance → Bulk Configuration.**
3. **To add a bulk configuration profile:**
   a. **In the Bulk Profiles section, click the Profile + button.**
   b. **In the Profile Name and Description fields, enter information for identifying the new profile.**
4. **Click Save.**
5. **If you want to create more bulk profiles, repeat Steps 1-4.**

▼ Performing a Bulk Configuration

1. **On the source device, ensure the wanted profile is selected as the default. If not, start from Step 2. If yes, go to Step 3.**
2. **(Optional) Select the desired bulk configuration profile.**
   a. **Log in to the source HPDU, whose settings you want to copy.**
   b. **Select Maintenance → Bulk Configuration.**

   c. **Click the row of the wanted profile to open the Edit Bulk Profile page.**

   d. **For the Default Profile option, click Select.**

   e. **Click Save.**

3. **Save a bulk configuration file.**

   a. **Verify that you have the Administrator Privileges or Unrestricted View Privileges to download the configuration.**

   b. **Log in to the source HPDU if you did not log in yet.**

   c. **Select Maintenance → Bulk Configuration.**

   d. **If the selected Bulk Format value (see the following table) does not match your need, you can change it.**

Bulk Format Value	Description
Encrypted	■ Partial content is base64 encoded. ■ Its content is encrypted using the AES-128 encryption algorithm. ■ File is saved to the TXT format
Cleartext	■ Content is displayed in clear text. ■ File is saved to the TXT format.

   e. **Change any bulk configuration settings.**

   f. **Click Download Bulk Configuration.**

   g. **When prompted to open or save the configuration file, click Save.**

4. **Perform a bulk configuration.**

   a. **Verify that you have the Administrator Privileges to upload the configuration.**

   b. **Log in to the target HPDU, which is the same model and runs the same firmware as the source HPDU.**

c. **Select Maintenance → Bulk Configuration.**

d. **Click Browse and select the configuration file.**

e. **Click Upload & Restore Bulk Configuration to copy it.**

f. **When prompted, type the admin password, and click Restore.**

g. **Wait until the HPDU device resets and the login page re-appears.**

▼ Modifying or Removing Bulk Profiles

You can modify or remove any bulk profile except for the built-in one.

1. **Select Maintenance → Bulk Configuration to display a list of profiles.**
2. **To modify an existing profile:**
   a. **Click the row of the profile you want to modify.**

   b. **Change any settings.**

   c. **Click Save.**
3. **To remove a profile, except the default profile:**
   a. **Click the row of the profile you want to remove.**

   b. **Click the trash can icon in the top-right corner.**

   c. **Click Delete to confirm.**
4. **To remove one or multiple profiles:**
   a. **Select one or multiple profiles.**

   b. **To select all profiles, select the first check box in the header row.**

   c. **Click the trash can icon in the top-right corner.**

d. **Click Delete to confirm.**

Bulk Configuration or Firmware Upgrade through DHCP/TFTP

If a TFTP server is available, you can use it and appropriate configuration files to perform any or all of the following tasks for a large number of HPDU devices in the same network.

- Initial deployment
- Configuration changes
- Firmware upgrade
- Downloading diagnostic data

This feature is useful if you have hundreds or even thousands of HPDU devices to configure or upgrade.

Note - Bulk configuration or firmware upgrade through DHCP/TFTP works only on standalone HPDU devices directly connected to the network, and does not work for slave devices in the USB-cascading configuration.

Bulk Configuration and Upgrade

The DHCP/TFTP feature is supported as of release 3.1.0. Ensure that all HPDU devices you want to configure or upgrade are running firmware version 3.1.0 or later.

Bulk Configuration or Firmware Upgrade through DHCP/TFTP

If a TFTP server is available, you can use the server and configuration files to perform any or all of the following tasks for a large number of HPDU devices in the same network.

- Initial deployment
- Configuration changes
- Firmware upgrade
- Downloading diagnostic data

Note - Bulk configuration or firmware upgrade through DHCP/TFTP works only on standalone HPDU devices directly connected to the network, and not on slave devices in the USB-cascading configuration.

Bulk Configuration or Upgrade

The DHCP/TFTP feature is supported as of release 3.1.0. Ensure that all HPDU devices that you want to configure or upgrade are running firmware version 3.1.0 or later.

▼ Using DHCP/TFTP for Bulk Configuration Upgrade

1. **Create configuration files specific to your HPDU models and firmware versions.**

   To prepare some or all of the following files, contact Oracle Support at `https://support.oracle.com`.

   - `fwupdate.cfg` (always required)
   - `config.txt`
   - `devices.csv`

   Note - Supported syntax of `fwupdate.cfg` and `config.txt` might vary, based on different firmware versions. If you have existing configuration files, verify with Oracle Technical Support for the correctness of these files before using this feature.

   ---

2. **Configure your TFTP server properly.**

3. **Copy all required configuration files (and firmware binary file, if a firmware upgrade is needed) into the TFTP root directory.**

4. **Configure your DHCP server so that it refers to the file `fwupdate.cfg` on the TFTP server for your HPDU.**

5. **Configure DHCP, based on the operating system and IP address type.**

6. **Ensure that the HPDU devices use DHCP as the IP configuration method and are connected to the network.**

7. **Re-boot the HPDU devices.**

   The DHCP server executes the commands in the `fwupdate.cfg` file on the TFTP server to configure or upgrade those HPDU devices supporting DHCP in the same network.

   DHCP executes the `fwupdate.cfg` commands once for IPv4 and once for IPv6 respectively if both IPv4 and IPv6 settings are configured properly in DHCP.

TFTP Requirements

To perform bulk configuration or a firmware upgrade successfully, your TFTP server must meet the following requirements:

- The server is able to work with both IPv4 and IPv6.
- In Linux, remove any IPv4 or IPv6 flags from `/etc/xinetd.d/tftp`.
- All required configuration files are available in the TFTP root directory.
- If you are going to upload any HPDU diagnostic file or create a log file in the TFTP server, the server supports the write operation, including file creation and upload. In Linux, provide the option "-c" for write support.

  For uploading the diagnostic file only, the timeout for file upload is set to one minute or longer.

Note - DHCP executes the `fwupdate.cfg` commands once for IPv4 and once for IPv6 respectively if both IPv4 and IPv6 settings are configured properly in DHCP.

▼ Configuring DHCP for IPv4 in Windows

You can configure the DHCP server for HPDU devices using IPv4 addresses. This procedure is based on Microsoft Windows Server 2012.

1. **Add a new vendor class for the HPDU under IPv4.**

   a. **Right-click the IPv4 node in DHCP to select Define Vendor Classes.**

   b. **Click Add to add a new vendor class.**

   c. **In the New Class dialog box, type a unique name for this vendor class and the binary codes of the HPDU.**

   d. **Define one DHCP standard option, Vendor Class Identifier.**

      i. **Right-click the IPv4 node in DHCP and select Set Predefined Options.**

      ii. **Select DHCP Standard Options in the Option class field, and Vendor Class Identifier in the Option name field. Leave the String field blank.**

   e. **Add three options to the new vendor class for the HPDU.**

i. **Select the HPDU in the Option class field.**

ii. **Click Add to add the first option. Type `pdu-tftp-server` in the Name field, select IP Address as the data type, and type 1 in the Code field.**

iii. **Click Add to add the second option. Type `pdu-update-control-file` in the Name field, select String as the data type, and type 2 in the Code field.**

iv. **Click Add to add the third one. Type `pdu-update-magic` in the Name field, select String as the data type, and type 3 in the Code field.**

2. **Create a new policy associated with the vendor class.**

   a. **Right-click the Policies node under IPv4 and select New Policy.**

   b. **Specify a policy name, and click Next.**

   c. **Click Add to add a new condition.**

   d. **Select the vendor class for the HPDU in the Value field, click Add, and click OK.**

   e. **Click Next.**

3. **Select DHCP Standard Options in the Vendor class field, select 060 Vendor Class Identifier from the Available Options list, and type the HPDU name in the String value field.**

4. **Select the HPDU name in the Vendor class field, select 001 pdu-tftp-server from the Available Options list, and type the TFTP server IPv4 address in the IP address field.**

5. **Select 002 pdu-update-control-file from the Available Options list, and type the file name `fwupdate.cfg` in the String value field.**

6. **Select 003 pdu-update-magic from the Available Options list, and type any string in the String value field.**

   The third option/code is the magic cookie to prevent the `fwupdate.cfg` commands from being executed repeatedly. It does not matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. For example, you can use a combination of a date and a serial number.

Note - The magic cookie is transmitted to and stored in HPDU at the time of executing the `fwupdate.cfg` commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in the HPDU. Modify the magic cookie value in DHCP when intending to execute the `fwupdate.cfg` commands the next time.

▼ Configuring DHCP for IPv6 in Windows

You can configure the DHCP server for HPDU devices using IPv6 addresses. The following procedure is based on Microsoft Windows Server 2012.

1. **Add a new vendor class for HPDU under IPv6.**

   a. **Right-click the IPv6 node in DHCP to select Define Vendor Classes.**

   b. **Click Add to add a new vendor class.**

   c. **In the New Class dialog box, type a unique name for the vendor class, type `13742` in the Vendor ID (IANA) field, and type the binary codes of the HPDU.**

2. **Add three options to the vendor class.**

   a. **Right-click the IPv6 node in DHCP to select Set Predefined Options.**

   b. **Select PDU 1.0 in the Option class field.**

   c. **Click Add to add the first option. Type `pdu-tftp-server` in the Name field, select IP Address as the data type, and type 1 in the Code field.**

   d. **Click Add to add the second option. Type `pdu-update-control-file` in the Name field, select String as the data type, and type 2 in the Code field.**

   e. **Click Add to add the third one. Type `pdu-update-magic` in the Name field, select String as the data type, and type 3 in the Code field.**

3. **Configure the server options associated with the vendor class.**

a. **Right-click the Server Options node under IPv6 to select Configure Options.**

b. **Click the Advanced tab.**

c. **Select the HPDU in the Vendor class field, select 00001 pdu-tftp-server from the Available Options list, and type the TFTP server IPv6 address in the IPv6 address field.**

d. **Select 00002 pdu-update-control-file from the Available Options list, and type the file name `fwupdate.cfg` in the String value field.**

e. **Select 00003 pdu-update-magic from the Available Options list, and type any string in the String value field.**

   The third option/code is the magic cookie to prevent the `fwupdate.cfg` commands from being executed repeatedly. It does not matter whether the IPv6 magic cookie is identical to or different from the IPv4 magic cookie.

   The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Note - The magic cookie is transmitted to and stored in HPDU at the time of executing the `fwupdate.cfg` commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in HPDU. Modify the magic cookies value in DHCP when intending to execute the `fwupdate.cfg` commands next time.

▼ Configuring DHCP for IPv4 in Linux

Modify the `dhcpd.conf` file for IPv4 settings when the DHCP server is running Linux.

1. **Locate and open the `dhcpd.conf` file of the DHCP server.**

   The HPDU provides the value of the vendor-class-identifier option (option 60). The vendor-class-identifier is the HPDU name.

2. **Configure the same option in DHCP.**

   The HPDU accepts the configuration or firmware upgrade only when this value in DHCP matches.

3. **Set the following three sub-options in the vendor-encapsulated-options (option 43).**

- code 1 (pdu-tftp-server) = TFTP server IPv4 address
- code 2 (pdu-update-control-file) = Control file name `fwupdate.cfg`
- code 3 (pdu-update-magic) = Any string

This third option/code is the magic cookie to prevent the `fwupdate.cfg` commands from being executed repeatedly. It does not matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Note - The magic cookie is transmitted to and stored in the HPDU at the time of executing the `fwupdate.cfg` commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in the HHPDU. Modify the magic cookies value in DHCP when intending to execute the `fwupdate.cfg` commands the next time.

▼ Configuring DHCP for IPv6 in Linux

Modify the `dhcpd6.conf` file for IPv6 settings when your DHCP server is running Linux.

1. **Locate and open the `dhcpd6.conf` file of the DHCP server.**

   The HPDU provides the following values to the vendor-class option (option 16).

   - 13742 (IANA number)
   - HPDU name
   - 15 (length of the string)

2. **Configure related settings in DHCP.**

3. **Set the following three sub-options in the vendor-opts (option 17).**

   - code 1 (pdu-tftp-server) = the TFTP server's IPv6 address
   - code 2 (pdu-update-control-file) = the name of the control file "fwupdate.cfg"
   - code 3 (pdu-update-magic) = any string

   The third option/code is the magic cookie to prevent the `fwupdate.cfg` commands from being executed repeatedly. It does not matter whether the IPv6 magic cookie is identical to or different from the IPv4 magic cookie.

   The magic cookie is a string comprising numerical and/or alphabetical digits in any format. For example, use a combination of a date and a serial number.

Note - The magic cookie is transmitted to and stored in the HPDU at the time of executing the `fwupdate.cfg` commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in the HPDU. Modify the magic cookies value in DHCP when intending to execute the `fwupdate.cfg` commands the next time.

▼ Backing Up and Restoring Device Settings

Unlike the bulk configuration file, the backup file contains all device settings, including device data such as device names and all network settings. To back up or restore HPDU device settings, perform the Backup/Restore feature.

All HPDU information is captured in the plain-TEXT-formatted backup file except for the device logs and TLS certificate.

1. **To download a backup HPDU file:**

   a. **Verify that you have the Administrator Privileges or Unrestricted View Privileges to download a backup file.**

   b. **Select Maintenance → Backup/Restore.**

   c. **Select Backup Format. If the selected value does not match your need, you can change it.**

   d. **If the selected value (see the following table) does not match your need, you can change it.**

Option	Description
Encrypted	■ Partial content is base64 encoded. ■ Its content is encrypted using the AES-128 encryption algorithm. ■ File is saved to the TXT format.
Cleartext	■ Content is displayed in clear text. ■ File is saved to the TXT format.

   e. **Click Download Device Settings.**

f. **Save the file on your computer.**

2. **To restore the HPDU using a backup file:**

a. **Verify that you have the Administrator Privileges to restore the device settings.**

b. **Select Maintenance → Backup/Restore.**

c. **Click Browse and select the backup file.**

d. **Click Upload & Restore Device Settings to upload the file.**

e. **When prompted, type the admin password, and click Restore.**

f. **Wait until the HPDU device resets and the Login page appears, indicating that the restore is complete.**

Note - On startup, the HPDU performs all of its functions, including event rules and logs, based on the new configuration you copied instead of the previous configuration prior to the device reset. For example, the Bulk configuration copied event is logged only when the new configuration file contains the Bulk configuration copied event rule.

If you copied any bulk configuration or device backup file to the HPDU, the last record displays at the bottom of both the Bulk Configuration and Backup/Restore pages.

To use a different bulk configuration method, see “Bulk Configuration through SCP” on page 260 Bulk Configuration via SCP (on page 94).

Network Diagnostics

The HPDU provides the following tools in the web interface for diagnosing potential networking issues. These network diagnostic tools are also available through CLI.

- Ping – Verifies whether a host is accessible through the network or Internet.
- Trace Route – Allows you to find out the route over the network between two hosts or systems.
- List TCP Connections – Displays a list of TCP connections.

▼ Running Network Diagnostics

1. **Select Maintenance → Network Diagnostics.**
2. **To use the Ping diagnostic tool:**

   a. **Type values in the following fields.**

Field	Description
Network Host	The name or IP address of the host that you want to check.
Number of Requests	A number up to 20. This determines how many packets are sent for pinging the host.

   b. **Click Run Ping to ping the host and view the results.**

3. **To run the Trace Route diagnostic tool:**

   a. **Type values in the following fields.**

Field/setting	Description
Host Name	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation.
Use ICMP Packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this check box.

   b. **Click Run to use the Trace Route diagnostics and view the results.**

4. **To use the List TCP Connections diagnostics tool, click the List TCP Connections title bar to show the list.**

▼ Downloading Diagnostic Information

You can download the diagnostic file from the HPDU to a client machine. The file is compressed into a .tgz file and must be sent to Technical Support for interpretation.

1. **Verify that you have Administrative Privileges or Unrestricted View Privileges.**

2. **To retrieve a diagnostic file, select Maintenance → Download Diagnostic → Download Diagnostic.**

3. **When prompted, click Save to save the file.**

4. **Email the diagnostic file, as instructed by Oracle Technical Support. To access My Oracle Support, go to `https://support.oracle.com`.**

▼ Rebooting the HPDU Device

You can remotely reboot the HPDU device through the web interface.

Resetting the HPDU does not interrupt the operation of connected servers because there is no loss of power to outlets. During and after the reboot, outlets that were powered on prior to the reboot remain powered on, and outlets that were powered off remain powered off.

1. **Select Maintenance → Unit Reset.**

2. **Click Reboot Unit to confirm and restart the HPDU.**

   A message appears, with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.

3. **When the restart is complete, the login page opens.**

Note - If you are not redirected to the login page after the restart is complete, click the link,**this link**, in the countdown message.

▼ Resetting All Settings to Factory Defaults

Caution - Exercise caution before you reset all settings to its factory defaults because this feature erases information and customized settings, such as user profiles and threshold values. Only active energy data and firmware upgrade history are retained.

1. **Verify that you have the Administrator Privileges to reset all settings of the HPDU to factory defaults.**

2. **Select Maintenance → Unit Reset → Reset to Factory Defaults.**

3. **Click Factory Reset to confirm and reset the HPDU to factory defaults.**

   A message appears, with a countdown timer showing the remaining time of the operation. It takes about two minutes to complete.

   When the reset is complete, the login page opens.

Note - If you are not redirected to the login page after the restart is complete, click the link,**this link**, in the countdown message.

---

4. **Alternatively, use any of the following methods to reset the device to factory defaults.**

   - **Use the mechanical reset button.**

     An RS-232 serial connection to a computer is required for using the reset button.

     a. **Connect a computer to the HPDU device.**

     b. **Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the HPDU.**

     c. **Press (and release) the Reset button of the HPDU device while pressing the Esc key of the keyboard several times in rapid succession.**

     d. **At the => prompt, type `defaults` to reset the HPDU to its factory defaults.**

     e. **Wait until the Username prompt appears, indicating the reset is complete.**

        The reset button on Zero U HPDU models are located to the right of the Ethernet ports. Port locations might differ on HPDU models.

Note - HyperTerminal is available on Windows operating systems prior to Windows Vista. For Windows Vista or later versions, you may use PuTTY, which is a free program you can download from the Internet. For details on configuration, refer to the PuTTY documentation .

   - **Perform the CLI command with logging in to the CLI.**

     a. **Connect to the HPDU device.**

     b. **Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the HPDU.**

c. **Log in to the CLI by typing the user name "admin" and its password.**

d. **After the # system prompt appears, type `reset factorydefaults` or `reset factorydefaults/y`either of the following commands and press Enter.**

   If you entered the command without "/y" in Step 4, a message appears prompting you to confirm the operation. Type y to confirm the reset.

e. **Wait until the Username prompt appears, indicating the reset is complete.**

- **Perform the CLI command without logging in to the CLI.**

  a. **Connect to the HPDU and launch a terminal emulation program.**

  b. **At the Username prompt in the CLI, type `factorydefaults`, and press Enter.**

  c. **Type y in the confirmation message to perform the reset.**

▼ Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the HPDU device through the web interface.

1. **Select Maintenance → PDU.**

2. **In the open source packages list, click any link to access related information or download any software package.**

Command Line Interface

This section explains how to use the command line interface (CLI) to administer a HPDU device.

- “Serial Port Configuration Commands” on page 246
- “Multi-Command Syntax” on page 247
- “Using Diagnostic Commands” on page 250

About the Interface

The HPDU provides a command line interface that allows data center administrators to perform the following basic management tasks.

- Reset the HPDU device
- Display the HPDU and network information, such as the device name, firmware version, and IP address
- Configure the HPDU and network settings
- Troubleshoot network problems

You can access the interface over a local connection using a terminal emulation program such as HyperTerminal, or through a Telnet or SSH client such as PuTTY.

▼ Log In to CLI with HyperTerminal

HyperTerminal is part of the Windows operating systems before Windows Vista. If a security login agreement is enabled, you must accept the agreement to complete the login. Users are authenticated first and the security banner is verified afterward. You can use any terminal emulation programs for local access to the command line interface.

1. **Connect your computer to the HPDU through a local (USB or RS-232) connection.**

2. **Launch HyperTerminal on your computer and open a console window. When the window first opens, it is blank.**

3. **Verify that the COM port settings use the following configuration:**

   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None

Note - For a USB connection, you can determine the COM port by choosing Control Panel → System → Hardware → Device Manager, and locating Dominion PX2 Serial Console in the Ports group.

4. **In the communications program, press Enter to send a carriage return to the HPDU.**

5. **When prompted, type a name (case sensitive) and press Enter.**

6. **When prompted, type a password (case sensitive) and press Enter.**

   The # or > system prompt appears. You are now logged in to the command line interface and can begin administering the HPDU.

Note - The Last Login information, including the date and time, also displays if the same user account was used to log in to this HPDU web interface or CLI.

▼ Log In to CLI with SSH or Telnet

You can remotely log in to the command line interface (CLI) using an SSH or Telnet client, such as PuTTY, which is a free program you can download from the Internet. For details on configuration, refer to the PuTTY documentation.

Note - Telnet access is disabled by default because it communicates openly and is thus insecure. To enable Telnet, see “Changing the Telnet Configuration” on page 201.

1. **Verify that SSH or Telnet is enabled.**

2. **Launch an SSH or Telnet client and open a console window. A login prompt appears.**

3. **When prompted, type a name (case sensitive) and press Enter.**

   Note: If using the SSH client, the name must NOT exceed 25 characters. Otherwise, the login fails.

4. **When prompted, type a password (case sensitive) and press Enter.**

   The # or > system prompt appears. You are now logged in to the command line interface and can begin administering the HPDU.

Note - The Last Login information, including the date and time, also displays if the same user account was used to log in to this HPDU web interface or CLI.

▼ Log In to CLI with an Analog Modem

The HPDU supports remote access to the CLI through a connected analog modem, which is useful when LAN access is not available.

1. **Ensure that the HPDU has an analog modem connected.**
2. **Ensure that the computer you are using has an appropriate modem connected.**
3. **Launch a terminal emulation program, and configure its baud rate settings according to the baud rate set for the analog modem connected to the HPDU.**
4. **Type `ATD< modem phone number>` to make a connection with the HPDU.**
5. **At the CLI login prompt, type the user name and password to log in to the CLI.**
6. **To disconnect from the HPDU:**
   a. **Return to the modem command mode using the escape code +++.**
   b. **After the OK prompt appears, type `ATH` to disconnect from the HPDU.**

Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies.

CLI Mode	Prompt
User Mode	When you log in as a user, who might not have full permissions to configure the HPDU device, the > prompt appears.
Administrator Mode	When you log in as an administrator, who has full

CLI Mode	Prompt
	permissions to configure the HPDU device, the # prompt appears.
Configuration Mode	You can enter configuration mode from the administrator or user mode. The prompt changes to config:# or config:> and you can change HPDU device and network configurations.
Diagnostic Mode	You can enter diagnostic mode from the administrator or user mode. The prompt changes to diag:# or diag:> and you can use the network troubleshooting commands, such as the ping command.

▼ Closing a Local Connection

- **Close the window or terminal emulation program when you finish accessing a HPDU device over a local connection.**

Note - When accessing or upgrading multiple HPDU devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

▼ The Help (?) Command for Showing Available Commands

When you are not familiar with CLI commands, you can press the Help (?) key at any time for one of the following purposes.

- Show a list of main CLI commands available in the current mode.
- Show a list of available commands or parameters for the command you type.

1. **Type any of the following commands:**

Mode	Command	Parameter
Administrator	#	?

Mode	Command	Parameter
Configuration	`config:#`	`?`
Diagnostic	`diag:#`	`?`

2. **Press Enter after pressing the ? command.**

   A list of main commands for the current mode displays.

   Note - To automatically complete a command after typing part of the full command, see "Automatically Completing a Command" on page 251.

3. **To re-execute a previous command, see "Retrieving Previous Commands" on page 251.**

Querying Available Parameters for a Command

1. **If you are not sure what commands or parameters are available for a particular type of CLI command or its syntax, type a space after the help command (?) or list command (ls).**

   Here are a few query examples.

Command	Query
Show	`# show ?`
Show User	`# show user ?`
Role Configuration	`config:# role ?`
Role Create	`config:# role create ?`

2. **A list of available parameters and their descriptions displays.**

   Note - To automatically complete a command after typing part of the full command, see "Automatically Completing a Command" on page 251.

3. **To re-execute a previous command, see "Retrieving Previous Commands" on page 251.**

Show Information

You can use the show commands to view current settings or the status of the HPDU device or part of it, such as the IP address, networking mode, firmware version, states or readings of internal or external sensors, and user profiles.

Some "show" commands have two formats: one with the parameter details that displays in-depth information, and the other without details that displays a shortened version of information.

At the # prompt, type the `show` command and press Enter.

Note - CLI commands are case sensitive.

Depending on your login name, the # prompt may be replaced by the > prompt.

▼ Showing Network Configuration Information

- **To show all network configuration and all network interface information, such as the IP address, MAC address, the Ethernet interface's duplex mode, and the wireless interface status and settings, type `show network`, and press Enter.**

▼ Showing IP Information

1. **To show the IP settings shared by all network interfaces (including both IPv4 and IPv6 configuration), such as DNS and routes, type `show network ip common`, and press Enter.**

2. **To show the IP settings of a specific network interface, type `show network ip interface <ETH>`, and press Enter.**

   <ETH> is one of the network interfaces: Ethernet (or ETH1/ETH2), wireless, or bridge. For details, see the following table.

   Note - If your HPDU is set to the bridging mode, select and configure the bridge interface. In bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET (or ETH1/ETH2) and WIRELESS interfaces do not function.

Interface	Description
ethernet (PDU)	Show the IP-related configuration of the ETHERNET interface.
eth1 (PDU -iX7)	Show the IP-related configuration of the ETH1 interface.
eth2 (PDU -iX7)	Show the IP-related configuration of the ETH2 interface.
bridge	Show the IP-related configuration of the BRIDGE interface.
all	Show the IP-related configuration of all interfaces. **Note -** You also can type the command without the `all` option to get the same data. For example, `show network ip interface`.

▼ Showing the IPv4 or IPv6 Configuration

1. **To show IPv4 settings shared by all network interfaces, such as DNS and routes, type `show network ipv4 common`, and press Enter.**

2. **To show the IPv4 configuration of a specific network interface, type `show network ipv4 interface <ETH>`, and press Enter.**

3. **To show IPv6 settings shared by all network interfaces, such as DNS and routes, type `show network ipv6 common`, and press Enter.**

   <ETH> is one of the network interfaces: ethernet (or ETH1/ETH2) or bridge. For details, see the following table.

   Note - Select and configure the bridge interface if your HPDU is set to the bridging mode.

Network Interface for IPv4/ IPv6	Description
ethernet (PDU)	Show the IPv4 or IPv6 configuration of the ETHERNET interface.
eth1 (PDU -iX7)	Show the IPv4 or IPv6 configuration of the ETH1 interface.
eth2 (PDU -iX7)	Show the IPv4 or IPv6 configuration of the ETH2 interface.
bridge	Show the IPv4 or IPv6 configuration of the BRIDGE interface.
all	Show the IPv4 or IPv6 configuration of all interfaces. **Note -** You also can type the command without the `all` option to get the same data. For example, `show network ip interface`.

▼ Showing the Network Interface Settings

- **To show the specified network interface information that is not related to IP configuration, for example, the Ethernet port LAN interface speed and duplex mode, or the wireless interface SSID parameter and authentication protocol, type `show network interface <ETH>`, and press Enter.**

  <ETH> is one of the network interfaces: ethernet (or ETH1/ETH2), wireless, or bridge. For details, see the following table.

Note - If the HPDU is set to the bridging mode, select and configure the bridge interface.

Interface	Description
ethernet (PDU)	Show the ETHERNET interface non-IP settings.
eth1	Show the ETH1 interface non-IP settings.

Interface	Description
(PDU -iX7)	
eth2 (PDU -iX7)	Show the ETH2 interface non-IP settings.
bridge	Show the BRIDGE interface non-IP settings.
all	Show the non-IP settings of all interfaces. You also can type the command without the `all` option to get the same data. For example, `show network ip interface`.

▼ Show the Network Service Settings

- **To show the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS, SSH and Modbus/TCP services, and SNMP settings, type `show network services <option>`, and press Enter.**

  <option> is one of the options.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP. You also can type the command without the `all` option to get the same data.
http	Only displays the TCP port for the HTTP service.
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.
modbus	Only displays the settings of the Modbus/TCP service.
zeroconfig	Only displays the settings of the zero configuration advertising.

▼ Show the HPDU Configuration

1. **To show the HPDU configuration, such as the device name, firmware version and model type, type `show pdu`, and press Enter.**

2. **To show detailed information, type `pdu details`, and press Enter.**

▼ Show the Inlet Configuration

1. **To show the inlet configuration, type `show inlets <n>`, and press Enter.**

   The inlet name and RMS current display.

2. **To show detailed information, type `show inlets <n> details`, and press Enter.**

   <n> is one of the following options.

Option	Description
all	Displays the information for all inlets. You also can type the command without the `all` option to get the same data. For example, `show network ip interface`.
Specific inlet number	Displays the information for the specified inlet only. An inlet number needs to be specified only when there is more than 1 inlet on your HPDU.

▼ Show the Date and Time Settings

1. **To show the current date and time settings on the HPDU device, type `show time`, and press Enter.**

2. **To show detailed information, type `show time details`, and press Enter.**

Show the Default Measurement Units

- **To show the default measurement units applied to the HPDU web and CLI interfaces across all users, especially those users authenticated through remote authentication servers, type `show user defaultPreferences`, and press Enter.**

Note - If a user sets preferred measurement units or the administrator changes any preferred units for a user, the web and CLI interfaces show the preferred measurement units for that user instead of the default ones after that user logs in to the HPDU.

Show the Inlet Sensor Threshold Information

1. **To show the specified inlet sensor threshold information, type `show sensor inlet <n> <sensor type>`, and press Enter.**

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

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

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

2. **To show detailed information, type `show sensor inlet <n> <sensor type> details`, and press Enter.**

Show the Inlet Pole Sensor Threshold Information

1. **To show the specified inlet pole sensor threshold information, type `show sensor inletpole <n> <p> <sensor type>`, and press Enter.**

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

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

<sensor type> is one of the following inlet pole sensor types:

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

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

2. **To show detailed information, type `show sensor inletpole <n> <p> <sensor type> details`, and press Enter.**

Show the Security Settings

1. **To show the security settings of the HPDU, type `show security`, and press Enter.**
   - Without the parameter "details," the information including IP access control, role-based access control, password policy, and HTTPS encryption is displayed.
   - With the parameter "details," more security information is displayed, such as user blocking time, user idle timeout and front panel permissions (if supported by your model).
2. **To show detailed information, type `show security details`, and press Enter.**

Show the Authentication Settings

1. **To show the authentication settings, including both LDAP and Radius settings, type `show authentication`, and press Enter.**
   - <server_num> is the sequential number of the specified authentication server on the LDAP or Radius server list.
   - Without specifying any server, HPDU shows the authentication type and a list of both LDAP and Radius servers that have been configured.
   - When specifying a server, only that server's basic configuration is displayed, such as IP address and port number.
   - With the parameter "details" added, detailed information of the specified server is displayed, such as an LDAP server's bind DN and the login name attribute, or a Radius server's timeout and retries values.
2. **To show the configuration of a specific LDAP server, assign the desired LDAP server with its sequential number in the command, and type `show authentication ldapServer <server_num>`, and press Enter.**
3. **To show detailed information of a specific LDAP server, type `show authentication ldapServer <server_num> details`, and press Enter.**
4. **To show the configuration of a specific Radius server, assign the desired Radius server with its sequential number in the command, type `show authentication radiusServer <server_num>`, and press Enter.**

5. **To show detailed information of a specific Radius server, type `show authentication radiusServer <server_num> details`, and press Enter.**

▼ Show Existing User Profiles

1. **To show the data of one or all existing user profiles, type `show user <user_name>`, and press Enter.**

   <user_name> is the name of the user whose profile you want to query. The variable can be one of the options: all shows all existing user profiles or a user's name to show the profile of the specified user only.

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

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

2. **To show detailed information of a user profile, type `show user <user_name> details`, and press Enter.**

▼ Show Existing Roles

- **To show the data of one or all existing roles, including the role description and privileges, type `show roles <role_name>`, and press Enter.**

  <role_name> is the name of the role whose permissions you want to query. The variable can be one of the options: *all* shows all existing roles or a *role name* to show the data of the specified role only.

  Note - You can type the `show roles` command without adding the *all* option to get the same data.

▼ Show Serial Port Settings

- **To show the baud rate setting of the serial port labeled CONSOLE / MODEM on the HPDU device, type `show serial`, and press Enter.**

▼ Show EnergyWise Settings

- **To show the current configuration for Cisco EnergyWise of the HPDU device, type `show energywise`, and press Enter.**

▼ Show the Event Log

1. **To show the last 30 entries in the event log, type `show eventlog`, and press Enter.**

2. **To show a specific number of last entries in the event log, type `show eventlog limit <n>`, and press Enter.**

3. **To show a specific type of events only, type `show eventlog class <event_type>`, and press Enter.**

Event Type	Description
all	All events.
device	Device-related events, such as system starting or firmware upgrade event.
userAdministration	User management events, such as a new user profile or a new role.
userActivity	User activities, such as login or logout.
pdu	Displays PDU-related events, such as entry or exit of the load shedding mode.
sensor	Internal or external sensor events, such as state changes of any sensors.
serverMonitor	Server-monitoring records, such as a server being declared reachable or unreachable.
modem	Modem-related events.
timerEvent	Scheduled action events.
energywise	Cisco EnergyWise-related events, such as enabling support for the Cisco EnergyWise function.

4. **To show a specific number of last entries associated with a specific type of events only, type `show eventlog limit <n> class <event_type>`, and press Enter.**

   <n> is one of the options. Type *all* to display all entries in the event log or an integer number between 1 to 10,000 to display the specified number of last entries in the event log.

▼ Show Server Reachability Information

1. **To show all server reachability information with a list of monitored servers and status, type `show serverReachability`, and press Enter.**

   The device IP address, monitoring enabled or disabled state, and current status display.

2. **To show the server reachability information for a certain IT device only, type `show serverReachabilityserver <n>`, and press Enter.**

   <n> is a number representing the sequence of the IT device in the monitored server list.

   You can find each IT device's sequence number using the CLI command of show serverReachability as illustrated below.

3. **To show detailed server reachability information, type `show serverReachabilityserver <n> details`, and press Enter.**

   The number of pings and wait time before the next ping display.

▼ Show the Command History

- **To show a list of commands that were previously entered in the current connection session, type `show history`, and press Enter.**

▼ Show the Reliability Data

- **To show the reliability data, type `show reliability data`, and press Enter.**

▼ Show the Reliability Error Log

- **To show the reliability error log, type `show reliability errorlog <n>`, and press Enter.**

  <n> is one of the options. Type *0* (zero) to display all entries in the reliability error log or any other integer number to display the specified number of last entries in the reliability error log. You also can type the command without adding the *0* option to get all data.

▼ Clear Event Log

- **To remove all data from the event log, do one of the following:**
  - **At the # or > prompt, type `clear eventlog` and type y to confirm.**
  - **At the # or > prompt, type `clear eventlog/y`. After all data in the event log is deleted, the message Event log was cleared successfully displays.**

▼ Configure the HPDU Device and Network

1. **Log in as the administrator so that you have full permissions.**
2. **At the # prompt, to enter configuration mode, type `config`, and press Enter.**

   Note - Configuration commands are case sensitive. Be sure to capitalize them correctly.

   Configuration commands function in configuration mode only.

   Note - If you enter Configuration mode from User mode, you might have limited permissions to make configuration changes.

3. **At the config:# prompt, type any configuration command, and press Enter to change the settings.**

   Note - To apply new configuration settings, you must type the `apply` command before closing the terminal emulation program. Closing the program does not save any configuration changes.

4. **To save the changes and quit Configuration mode, at the config:# prompt, type `apply`, and press Enter.**
   - `apply` command – Saves all changes you made and quits Configuration mode.
   - `cancel` command – Allows you to abort the changes you made and quit Configuration mode.

   The # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode.

Using HPDU Configuration Commands

You can use the HPDU configuration commands to change the settings that apply to the entire HPDU device.

▼ Change the HPDU Name

- **To change the HPDU device name, at the config:# prompt, type `pdu name "<name>"`, and press Enter.**

  <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

▼ Enable or Disable Data Logging

- **To enable or disable the data logging feature, at the config:# prompt, type `pdu dataRetrieval <option>`, and press Enter.**

  <option> is one of the options: Enable to enable the data logging feature or Disable to disable the data logging feature.

▼ Set Data Logging Measurements Per Entry

- **To define the number of measurements accumulated per log entry, at the config:# prompt, type `pdu measurementsPerLogEntry <number>`, and press Enter.**

  <number> is an integer between 1 and 600. The default is 60 samples per log entry.

▼ Specify the Device Altitude

- **To specify your HPDU device altitude above sea level (in meters), at the config:# prompt, type `pdu deviceAltitude <altitude>`, and press Enter.**

  - <altitude> is an integer between -425 and 3000 meters.
  - The lower limit of -425 is a negative value because some locations are below sea level.

▼ Set the Z Coordinate Format for Environmental Sensors

- **To enable or disable the use of rack units for specifying the height (Z coordinate) of environmental sensors, at the config:# prompt, type `pdu externalSensorsZCoordinateFormat <option>`, and press Enter.**

  <option> is one of the options:

  rackUnits – The height of the Z coordinate is measured in standard rack units. Type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors or actuators.

  freeForm – Any alphanumeric string can be used for specifying the Z coordinate. After determining the format for the Z coordinate, you can set a value for it.

Using Network Configuration Commands

A network configuration command begins with the command `network`. You can change the IP address, transmission speed, and duplex mode.

▼ Configure IPv4 and IPv 6 Parameters

1. **To determine the IP configuration mode, at the config:# prompt, type `network ipv4 interface <ETH> configMethod <mode>` or `network ipv6 interface <ETH> configMethod <mode>`, and press Enter.**

Interface	Description
ethernet (PDU)	Determine the IPv4 or IPv6 configuration of the ETHERNET interface (wired networking).
eth1 (PDU -iX7)	Determine the IPv4 or IPv6 configuration mode of the ETH1 interface (wired networking).
eth2 (PDU -iX7)	Determine the IPv4 or IPv6 configuration mode of the ETH2 interface (wired networking).

Interface	Description
bridge	Determine the IPv4 or IPv6 configuration mode of the Bridge interface (Bridging mode). **Note -** Be sure to configure the bridge.

<mode> is one of the following modes:

dhcp – IPv4 configuration mode is set to DHCP.

automatic – IPv6 configuration mode is set to automatic.

static – IPv4 or IPv6 configuration mode is set to the static IP address.

2. **To enable the wired networking mode, at the config:# prompt, type `network mode wired`, and press Enter.**

3. **To enable the Static IP configuration mode, at the config:# prompt, type `network ipv4 ipConfigurationMode static`, and press Enter.**

4. **To enable both IPv4 and IPv6 protocols, at the config:# prompt, type `network ip proto both`, and press Enter.**

▼ Set the IPv4 and IPv6 Preferred Host Name

- **After selecting DHCP as the IPv4 configuration mode, optionally, to specify the preferred host name, at the config:# prompt, type `network ipv4 interface <ETH> preferredHostName <name>` or `network ipv6 interface <ETH> preferredHostName <name>`, and press Enter.**

  <name> is a host name which:

  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

IPv4 Network Interface	Description
ethernet	Determine the IPv4 or IPv6 preferred host name of

IPv4 Network Interface	Description
(PDU)	the ETHERNET interface (wired networking).
eth1 (PDU -iX7)	Determine the IPv4 or IPv6 preferred host name of the ETH1 interface (wired networking).
eth2 (PDU -iX7)	Determine the IPv4 or IPv6 preferred host name of the ETH2 interface (wired networking).
bridge	Determine the IPv4 or IPv6 preferred host name of the Bridge interface (Bridging mode). **Note -** Be sure to configure the bridge. In Bridging mode, only the IP parameters of the Bridge interface function. The IP parameters of the ETHERNET (or ETH1/ ETH2) and WIRELESS interfaces do not function.

Set the IPv4 and IPv6 Address

- **After selecting the static IP configuration mode, to assign a permanent IP address to the HPDU device, at the config:# prompt, type `network ipv4 interface <ETH> address <ip address>` or `network ipv6 interface <ETH> address <ip address>/xx`, and press Enter.**

  <ip address> is the IP address being assigned to your HPDU device. The IP address format is IP address/prefix. For example, 192.168.84.99/24.

  /xx indicates a prefix length of bits such as /64 for IPv6 only.

Interface	Description
ethernet (PDU)	Determine the IPv4 or IPv6 address of the ETHERNET interface (wired networking).
eth1 (PDU -iX7)	Determine the IPv4 or IPv6 address of the

Interface	Description
	ETH1 interface (wired networking).
eth2 (PDU -iX7)	Determine the IPv4 or IPv6 address of the ETH2 interface (wired networking).
bridge	Determine the IPv4 or IPv6 address of the Bridge interface (Bridging mode). **Note -** Be sure to configure the bridge.

▼ Set the IPv4 and IPv6 Gateway

- **After selecting the static IP configuration mode, to specify the gateway, at the config:# prompt, type `network ipv4 gateway <ip address>` or `network ipv6 gateway <ip address>`, and press Enter.**

  <ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

▼ Set the IPv4 and IPv6 Static Routes

If the IPv4 or IPv6 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the HPDU and devices in the other subnet.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route. For further information, see "Static Route Examples" on page 91.

1. **Use of the one following methods to set the IPv4 and IPv6 static routes.**

   - **After selecting the static IP configuration mode, to add a static route when the other network is NOT directly reachable, at the config:# prompt, type `network ipv4 staticRoutes add <dest-1> <hop>` or `network ipv6 staticRoutes add <dest-1> <hop>`, and press Enter.**

   - **After selecting the static IP configuration mode, to add a static route when the other network is directly reachable, at the config:# prompt, type `network`**

`ipv4 staticRoutes add <dest-1> interface <ETH>` or `network ipv6 staticRoutes add <dest-1> interface <ETH>`, and press Enter.

<dest-1> for IPv4 is a combination of the IP address and subnet mask of the other subnet. The format is IP address/subnet mask.

<dest-1> for IPv6 is the IP address and prefix length of the subnet where the HPDU belongs. The format is IP address/prefix length.

<hop> is the IP address of the next hop router.

<ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

<ETH> is one of the interfaces: ethernet (or ETH1/ETH2), wireless, and bridge. Type "bridge" only when your HPDU is in the bridging mode.

2. **To delete an existing static route, at the config:# prompt, type `network ipv4 staticRoutes delete <route_ID>` or `network ipv6 staticRoutes delete <route_ID>`, and press Enter.**

3. **To modify an existing static route, at the config:# prompt, enter one of the following commands:**

   - **At the config:# prompt, type `network ipv4 staticRoutes modify <route_ID> <dest-2> <hop>` or `network ipv6 staticRoutes modify <route_ID> <dest-2> <hop>`, and press Enter.**

   - **At the config:# prompt, type `network ipv4 staticRoutes modify <route_ID> <dest-2> interface <ETH>` or `network ipv6 staticRoutes modify <route_ID> <dest-2> interface <ETH>`, and press Enter.**

     <route_ID> is the ID number of the route setting which you want to delete or modify.

     <dest-2> for IPv4 is a modified route setting that will replace the original route setting. Its format is IP address/subnet mask. You can modify either the IP address or the subnet mask or both.

     <dest-2> for IPv6 is a modified route setting that will replace the original route setting. Its format is IP address/prefix length. You can modify either the IP address or the prefix length or both.

Configuring DNS Parameters

You can configure the parameters for one or more DNS servers.

▼ Configure DNS Parameters

1. **To specify the primary DNS server, at the config:# prompt, type `network dns firstServer <ip address>`, and press Enter.**

2. **To specify the secondary DNS server, at the config:# prompt, type `network dns secondServer <ip address>`, and press Enter.**

3. **To specify the third DNS server, at the config:# prompt, type `network dns thirdServer <ip address>`, and press Enter.**

4. **To specify one or multiple optional DNS search suffixes, at the config:# prompt, type `network dns searchSuffixes <suffix1>` or `network dns searchSuffixes <suffix1>,<suffix2>,<suffix3>,...,<suffix6>`, and press Enter.**

5. **To determine which IP address is used when the DNS server returns both IPv4 and IPv6 addresses, at the config:# prompt, type `network dns resolverPreference <resolver>`, and press Enter.**

   <ip address> is the IP address of the DNS server.

   <suffix1>, <suffix2>, and so on are the DNS suffixes that automatically apply when searching for any device through the HPDU. For example, <suffix1> can be `company.com` and <suffix2> can be `parent.com`. You can specify up to 6 suffixes by separating them with commas.

   <resolver> is one of the options:

   preferV4 - Use the IPv4 addresses returned by the DNS server.

   preferV6 - Use the IPv6 addresses returned by the DNS server.

Setting the LAN Interface Parameters

You can enable or disable the LAN interface and change the LAN settings.

▼ Enable or Disable the LAN Interface

- **To enable or disable the LAN interface, at the config:# prompt, type `network ethernet <ETH> enabled <option>`, and press Enter.**

Interface	Description
ethernet (PDU)	ETHERNET port of the PDU model.
eth1 (PDU -iX7)	ETH1 port of the iX7 model.
eth2 (PDU -iX7)	ETH2 port of the iX7 model.

<option> is one of the options:

- true – Network interface is enabled.
- false – Network interface is disabled.

Change the LAN Interface Speed

- **To change the LAN interface speed, at the config:# prompt, type `network ethernet <ETH> speed <option>`, and press Enter.**

Interface	Description
ethernet (PDU)	ETHERNET port of the HPDU model.
eth1 (PDU -iX7)	ETH1 port of the iX7 model.
eth2 (PDU -iX7)	ETH2 port of the iX7 model.

<option> is one of the options:

LAN Speed	Description
auto	System determines the optimum LAN speed through auto-negotiation.

LAN Speed	Description
10Mbps	LAN speed is always 10 Mbps.
100Mbps	LAN speed is always 100 Mbps.
1000Mbps	Available only on PDU-iX7 models or PDU models with the suffix, -G1. LAN speed is 1,000 Mbps.

Change the LAN Duplex Mode

- **To change the LAN duplex mode, at the config:# prompt, type `network ethernet <ETH> duplexMode <mode>`, and press Enter.**

Network Interface	Description
ethernet (PDU)	ETHERNET port of the HPDU model.
eth1 (PDU -iX7)	ETH1 port of the iX7 model.
eth2 (PDU -iX7)	ETH2 port of the iX7 model.

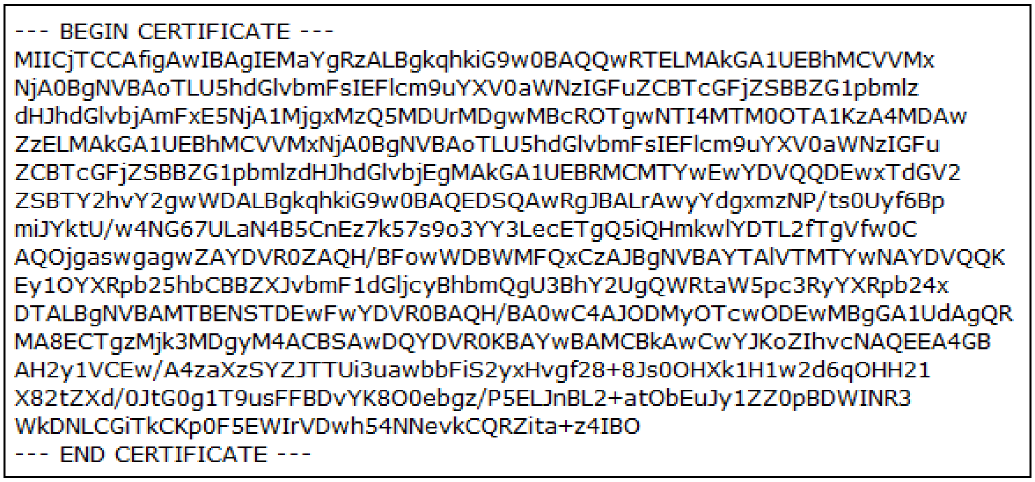
<mode> is one of the modes:

Option	Description
auto	HPDU selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the HPDU device) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Create an EAP CA Certificate

1. **Enter configuration mode.**
2. **At the config:# prompt, type `network wireless eapCACertificate`, and press Enter.**
3. **When prompted, open a CA certificate using a text editor.**

   Your CA certificate contents is different from the contents displayed in the following example.



```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

4. **Select and copy the contents, excluding the starting line BEGIN CERTIFICATE and the ending line END CERTIFICATE.**
5. **Paste the contents in the terminal and press Enter.**
6. **Verify whether the system shows the config:# command prompt, indicating the provided CA certificate is valid.**

Set the BSSID

- **To set the BSSID, at the config:# prompt, type `network wireless BSSID <bssid>`, and press Enter.**

  <bssid> is either the MAC address of the wireless access point or `none` for automatic selection.

Setting the Network Service Parameters

You can set the HTTP and HTTPS ports.

▼ Set the HTTP Port

1. **To change the HTTP port, at the config:# prompt, type `network services http port <n>`, and press Enter.**

   <n> is a TCP port number between 1 and 65535. The default HTTP port is 80.

2. **To enable or disable the HTTP port, at the config:# prompt, type `network services http enabled <option>`, and press Enter.**

   <option> is one of the options: true - Enable the HTTP port or false - disable the HTTP port.

▼ Set the HTTPS Port

1. **To change the HTTPS port, at the config:# prompt, type `network services https port <n>`, and press Enter.**

   <n> is a TCP port number between 1 and 65535. The default HTTP port is 443.

2. **To enable or disable the HTTPS port, at the config:# prompt, type `network services https enabled <option>`, and press Enter.**

   <option> is one of the options: true - Forces any access to the HPDU through HTTP to be redirected to HTTPS or false - No HTTP access is redirected to HTTPS.

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

▼ Enable or Disable Telnet

- **To enable or disable the Telnet service, at the config:# prompt, type `network services telnet enabled <option>`, and press Enter.**

<option> is one of the options: true - Enable the Telnet service or false - disable the Telnet service.

▼ Change the Telnet Port

- **To change the Telnet port, at the config:# prompt, type `network services telnet port <n>`, and press Enter.**

  <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

▼ Enable or Disable SSH

- **To enable or disable SSH, at the config:# prompt, type `network services sshenabled <option>`, and press Enter.**

  <option> is one of the options:

  - true – Enable SSH.
  - false – Disable SSH.

▼ Change the SSH Port

- **To change the SSH port, at the config:# prompt, type `network services ssh port <n>`, and press Enter.**

  <n> is a TCP port number between 1 and 65535. The default SSH port is 22.

▼ Determine the SSH Authentication Method

1. **To determine the SSH authentication method, at the config:# prompt, type `network services ssh authentication <auth_method>`, and press Enter.**

<n> is a TCP port number between 1 and 65535. The default SSH port is 22.

<option> is one of the following SSH authentication methods.

SSH Authentication Method	Description
passwordOnly	Enables the password-based login only.
publicKeyOnly	Enables the public key-based login only.
passwordOrPublicKey	Enables both the password- and public key-based login. This is the default.

2. **If you select a public key authentication, enter a valid SSH public key for each user profile to log in over the SSH connection.**

3. **To set the wireless authentication method to PSK, at the config:# prompt, type `network wireless authMethod PSK`, and press Enter.**

Setting the SNMP Configuration

You can enable or disable the SNMP v1/v2c or v3 agent, configure the read and write community strings, or set the MIB-II parameters, such as sysContact, using the CLI commands.

▼ Enable or Disable SNMP v1/v2c

● **To enable or disable the SNMP v1/v2c protocol, at the config:# prompt, type `network services snmp v1/v2c <option>`, and press Enter.**

<n> is a TCP port number between 1 and 65535. The default SSH port is 22.

<option> is one of the options:

- Enable the SNMP v1/v2c protocol.
- Disable the SNMP v1/v2c protocol.

▼ Enable or Disable SNMP v3

● **To enable or disable the SNMP v3 protocol, at the config:# prompt, type `network services snmp v3 <option>`, and press Enter.**

<n> is a TCP port number between 1 and 65535. The default SSH port is 22.

<option> is one of the options:

- Enable the SNMP v3 protocol.
- Disable the SNMP v3 protocol.

▼ Set the SNMP Read Community

- **To set the SNMP read-only community string, at the config:# prompt, type `network services snmp readCommunity <string>`, and press Enter.**

  <string> is a string comprising 4 to 64 ASCII printable characters, with no spaces.

▼ Set the SNMP Write Community

- **To set the SNMP read/write community string, at the config:# prompt, type `network services snmp writeCommunity <string>`, and press Enter.**

  <string> is a string comprising 4 to 64 ASCII printable characters, with no spaces.

▼ Set the sysContact Value

- **To set the SNMP MIB-II sysContact value, at the config:# prompt, type `network services snmp sysContact <value>`, and press Enter.**

  <value> is a string comprising 0 to 255 alphanumeric characters.

▼ Set the sysName Value

- **To set the SNMP MIB-II sysName value, at the config:# prompt, type `network services snmp sysName <value>`, and press Enter.**

  <value> is a string comprising 0 to 255 alphanumeric characters.

▼ Set the sysLocation Value

- **To set the SNMP MIB-II sysLocation value, at the config:# prompt, type `network services snmp sysLocation <value>`, and press Enter.**
  <value> is a string comprising 0 to 255 alphanumeric characters.

Changing the Modbus Configuration

You can enable or disable the Modbus agent, configure its read-only capability, or change its TCP port.

▼ Enable or Disable Modbus

- **To enable or disable the Modbus protocol, at the config:# prompt, type `network services modbus enabled <option>`, and press Enter.**
  <option> is one of the options:
  - True enables the Modbus agent.
  - False disables the Modbus agent.

▼ Enable or Disable the Read-Only Mode for the Modbus Agent

- **To enable or disable the Read-Only mode for the Modbus agent, at the config:# prompt, type `network services modbus readonly <option>`, and press Enter.**
  <option> is one of the options:
  - True enables the Read-Only mode for the Modbus agent.
  - False disables the Read-Only mode for the Modbus agent.

▼ Change the Modbus Port

- **To change the Modbus port, at the config:# prompt, type `network services modbus port <n>`, and press Enter.**

<n> is a TCP port number between 1 and 65535. The default Modbus port is 502.

Enabling or Disabling Service Advertising

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services.

▼ Enable or Disable Service Advertising

- **To enable or disable service advertising, at the config:# prompt, type `network services zeroconfig enabled <option>`, and press Enter.**

  <option> is one of the options:

  - True enables the zero configuration protocol.
  - False disables the zero configuration protocol.

Configuring the System Date and Time

You can configure the system date and time manually or by using NTP servers.

▼ Configure the Time Setup Method

1. **To set the date and time settings manually, at the config:# prompt, type `time method manual`, and press Enter.**

2. **To set the date and time settings by using the NTP servers, at the config:# prompt, type `time method ntp`, and press Enter.**

   <method> is one of the time setup options:

   - manual – Allows you to customize the date and time settings.
   - ntp – Allows you to synchronize the date and time settings with an NTP server.

Set NTP Parameters

1. **To specify the primary time server, at the config:# prompt, type `time ntp firstServer <first_server>`, and press Enter. For example, type `time ntp firstServer 192.168.80.66`.**

2. **To specify the secondary time server, at the config:# prompt, type `time ntp secondServer <second_server>`, and press Enter.**

3. **To delete the primary time server, at the config:# prompt, type `time ntp firstServer ""`, and press Enter.**

4. **To delete the primary time server, at the config:# prompt, type `time ntp secondServer ""`, and press Enter.**

   - <first_server> – IP address or host name of the primary NTP server.
   - <second_server> – IP address or host name of the secondary NTP server.

   <option> is one of these options:

   - true – Customized NTP server settings override the DHCP-specified NTP servers.
   - false – Customized NTP server settings do not override the DHCP-specified NTP servers.

Customize the Date and Time

1. **Set the time configuration method to manual.**

2. **To assign the date manually, at the config:# prompt, type `time set date` <yyyy-mm-dd>, and press Enter.**

3. **To assign the time manually, at the config:# prompt, type `time set time <hh:mm:ss>`, and press Enter.**

Date/Time	Description
<yyyy-mm-dd>	Type the date in the format of yyyy-mm-dd. For example, type 2015-11-30 for November 30, 2015.
<hh:mm:ss>	Type the time in the format of hh:mm:ss in the 24-hour format. For example, type 13:50:20 for 1:50:20 pm.

Set the Time Zone

1. **To set the time zone, at the config:# prompt, type `time zone`, and press Enter.**
2. **After a list of time zones is displayed, type the index number of the time zone, and press Enter.**
3. **Type `apply` for the selected time zone to take effect.**

Set the Automatic Daylight Saving Time

- **To determine whether the daylight saving time is applied to the time settings, at the config:# prompt, type `time autoDST <option>`, and press Enter.**

  <option> is one of the options:

  - true – Enables daylight saving time.
  - false – Disables daylight saving time.

Check the Accessibility of NTP Servers

1. **Verify that you own the Change Date/Time Settings permission.**
2. **Customize NTP servers.**

   The check command is available either in the administrator/user mode or configuration mode.
3. **In administrator/user mode at the # prompt, or in configuration mode at the config:# prompt, type `check ntp`.**

Configuring Security

You can manage firewall control features through the CLI. The firewall control lets you set up rules that permit or disallow access to the HPDU device from a specific or a range of IP addresses.

▼ Manage Firewall Control Parameters

1. **To enable or disable the IPv4 firewall control feature, at the config:# prompt, type `security ipAccessControl ipv4 enabled <option>`, and press Enter.**

2. **To enable or disable the IPv6 firewall control feature, at the config:# prompt, type `security ipAccessControl ipv6 enabled <option>`, and press Enter.**

   <option> is one of the options:

   - true – Enables the IP access control feature.
   - false – Disables the IP access control feature.

3. **To determine the default IPv4 firewall control policy for inbound traffic, at the config:# prompt, type `security ipAccessControl ipv4 defaultPolicyIn <policy>`, and press Enter.**

4. **To determine the default IPv6 firewall control policy for inbound traffic, at the config:# prompt, type `security ipAccessControl ipv6 defaultPolicyIn <policy>`, and press Enter.**

5. **To determine the default IPv4 firewall control policy for outbound traffic, at the config:# prompt, type `security ipAccessControl ipv4 defaultPolicyOut <policy>`, and press Enter.**

6. **To determine the default IPv6 firewall control policy for outbound traffic, at the config:# prompt, type `security ipAccessControl ipv6 defaultPolicyOut <policy>`, and press Enter.**

   <policy> is one of the options:

Policy	Description
accept	Accepts traffic from all IP addresses.
drop	Discards traffic from all IP addresses, without sending any failure notification to the source host.
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

7. **For example, to combine both commands to modify all firewall control parameters at a time, config:# prompt, type `security ipAccessControl ipv4 enabled true defaultPolicyIn accept defaultPolicyOut accept`, and press Enter.**

   - IPv4 access control feature is enabled.
   - Default policy for inbound traffic is set to *accept*.

- Default policy for outbound traffic is set to *accept*.

Managing Firewall Rules

You can add, delete, or modify firewall rules using the CLI commands.

▼ Add a Firewall Rule

1. **To add a new IPv4 rule at the bottom of the IPv4 rules list, at the config:# prompt, type `security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy>`, and press Enter.**

2. **To add a new IPv6 rule at the bottom of the IPv6 rules list, at the config:# prompt, type `security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy>`, and press Enter.**

3. **To add a new IPv4 rule by inserting it above or below a specific rule, at the config:# prompt, type `security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy> <insert> <rule_number>`, and press Enter.**
   For example, to add an IPv4 rule to accept all packets sent from the IPv4 address 192.168.84.123 by inserting it above the fifth rule, at the config:# prompt, type `security ipAccessControl ipv4 rule add 192.168.84.123/24 accept insertAbove 5`, and press Enter. The original 5th rule becomes the 6th rule.

4. **To add a new IPv6 rule by inserting it above or below a specific rule, at the config:# prompt, type `security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy> <insert> <rule_number>`, and press Enter.**
   <direction> is one of the options:

   - in – Inbound traffic.
   - out – Outbound traffic.

   <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, 192.168.94.222/24.

Policy	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.

Policy	Description
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

<rule_number> is the number of the existing rule which you want to insert the new rule above or below.

<insert> is one of the options:

Insert	Description
insertAbove	Inserts the new rule above the specified rule number. Then: new rule number = the specified rule number
insertBelow	Inserts the new rule below the specified rule number. Then: new rule number = the specified rule number + 1

▼ Modify a Firewall Rule

1. **To modify an IPv4 rule IP address and subnet mask, at the config:# prompt, type `security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask <ip_mask>`, and press Enter.**

2. **To modify an IPv6 rule IP address and prefix length, at the config:# prompt, type `security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask <ip_mask>`, and press Enter.**

3. **To modify an IPv4 rule policy, at the config:# prompt, type `security ipAccessControl ipv4 rule modify <direction> <rule_number> policy <policy>`, and press Enter.**

4. **To add an IPv6 rule policy, at the config:# prompt, type `security ipAccessControl ipv6 rule modify <direction> <rule_number> policy <policy>`, and press Enter.**

5. **To modify all contents of an existing IPv4 rule, at the config:# prompt, type `security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask <ip_mask> policy <policy>`, and press Enter.**

6. **To modify all contents of an existing IPv6 rule, at the config:# prompt, type `security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask <ip_mask> policy <policy>`, and press Enter.**

   <direction> is one of the options:

   - in – Inbound traffic.
   - out – Outbound traffic.

   <rule_number> is the number of the existing rule that you want to modify.

   <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, 192.168.94.222/24.

Policy	Description
accept	Accepts traffic from or to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

▼ Delete a Firewall Rule

1. **To delete a IPv4 firewall rule in the list, at the config:# prompt, type `security ipAccessControl ipv4 rule delete <direction> <rule_number>`, and press Enter.**

2. **To delete a IPv6 firewall rule in the list, at the config:# prompt, type `security ipAccessControl ipv6 rule delete <direction> <rule_number>`, and press Enter.**

   <direction> is one of the options:

   - in – Inbound traffic.
   - out – Outbound traffic.

   <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, 192.168.94.222/24.

   <rule_number> is the number of the existing rule you want to delete.

Restricted Service Agreement

You can enable or disable the Restricted Service Agreement feature.

▼ Enable or Disable the Restricted Service Agreement

1. **To enable or disable the Restricted Service Agreement, at the config:# prompt, type `security restrictedServiceAgreement enabled <option>`, and press Enter.**

   <option> is one of the options:

   - true – Enables the Restricted Service Agreement feature.
   - false – Disables the Restricted Service Agreement feature.

2. **After you enable the Restricted Service Agreement, do either of the following or the login fails:**

   - **In the web interface, press Tab, select `I understand and accept the Restricted Service Agreement`, and press Enter.**
   - **In the CLI, when the confirmation message `I understand and accept the Restricted Service Agreement` displays, type `y`.**

▼ Specify the Agreement Content

1. **To create or modify the agreement content, at the config:# prompt, type `security restrictedServiceAgreement bannerContent`, and press Enter.**

2. **When the CLI prompts you to enter the content, type the text comprising of up to 10,000 ASCII characters.**

Caution - You are accessing a HPDU. If you are not the system administrator, do not make changes without the permission of the system administrator.

3. **To end the content, press Enter, type `--END--` to indicate the end of the content, and press Enter.**

   If the content is successfully entered, the CLI displays the message `Successfully entered Restricted Service Agreement`, followed by the total number of entered characters in parentheses.

4. **Type the `apply` command to save the new content of the Restricted Service Agreement.**

Login Limitation

The login limitation feature controls login-related limitations, such as password aging, simultaneous logins using the same user name, and the idle time permitted before forcing a user to log out.

You can combine multiple commands to modify various login limitation parameters at a time.

▼ Specify the Single Login Limitation

- **To enable or disable the single login limitation, which controls whether multiple logins using the same login name simultaneously is permitted, at the config:# prompt, type `security loginLimits singleLogin <option>`, and press Enter.**

  <option> is one of the options:

  - enable – Enables single login.
  - disable – Disables single login.

▼ Set Password Aging

- **To enable or disable password aging, which controls whether the password must be changed at a regular interval, at the config:# prompt, type `security loginLimits passwordAging <option>`, and press Enter.**

  <option> is one of these options:

  - enable – Enables password aging.
  - disable – Disables password aging.

▼ Set Password Aging Interval

- **To determine how often the password must be changed, at the config:# prompt, type `security loginLimits passwordAgingInterval <value>`, and press Enter.**

  <value> is a numeric value ranging from 7 to 365 days for the password aging interval.

▼ Set Idle Timeout

- **To determine how long a user can remain idle before that user is forced to log out of the HPDU web interface or CLI, at the config:# prompt, type `security loginLimits idleTimeout <value>`, and press Enter.**

  <value> is a numeric value from 1 to 1440 minutes (24 hours) for the idle timeout.

▼ User Blocking

1. **To determine the maximum number of failed logins before blocking a user, at the config:# prompt, type `security userBlocking maximumNumberOfFailedLogins <value1>`, and press Enter.**

   <value1> is an integer between 3 and 10, or unlimited, which sets no limit on the maximum number of failed logins and thus disables the user blocking function.

2. **To determine how long a user is blocked, at the config:# prompt, type `security userBlocking blockTime <value2>`, and press Enter.**

   <value2> is a numeric value ranging from 1 to 1440 minutes (one day), or infinite, which blocks the user all the time until the user is unblocked manually.

   For example, to set the maximum number of failed logins to 5 and the user blocking time to 30 minutes, at the config:# prompt, type `security userBlocking maximumNumberOfFailedLogins 5 blockTime 30`, and press Enter.

Strong Passwords

The strong password commands determine whether a strong password is required for login, and what a strong password should contain at the least.

You can combine multiple strong password commands to modify different parameters at a time.

▼ Enable or Disable the Strong Password Option

- **To enable or disable the strong password option, at the config:# prompt, type `security strongPasswords enabled <option>`, and press Enter.**

  <options> is one of these options:

- enable – Enables the strong password option.
- disable – Disables the strong password option.

▼ Set the Minimum Password Length

- **To determine the minimum length of the password, at the config:# prompt, type `security strongPasswords minimumLength <value>`, and press Enter.**

  <value> is an integer between 8 and 32.

▼ Set the Maximum Password Length

- **To determine the maximum length of the password, at the config:# prompt, type `security strongPasswords maximumLength <value>`, and press Enter.**

  <value> is an integer between 16 and 64.

▼ Set the Lowercase Character Requirement

- **To determine whether a strong password includes at least a lowercase character, at the config:# prompt, type `security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>`, and press Enter.**

  <options> is one of these options:

  - enable – At least one lowercase character is required.
  - disable – No lowercase character is required.

▼ Set the Uppercase Character Requirement

- **To determine whether a strong password includes at least an uppercase character, at the config:# prompt, type `security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>`, and press Enter.**

  <options> is one of these options:

  - enable – At least one uppercase character is required.
  - disable – No uppercase character is required.

▼ Set the Numeric Character Requirement

- **To determine whether a strong password includes at least a numeric character, at the config:# prompt, type `security strongPasswords enforceAtLeastOneNumericCharacter <option>`, and press Enter.**

  <options> is one of these options:

  - enable – At least one numeric character is required.
  - disable – No numeric character is required.

▼ Set the Special Character Requirement

- **To determine whether a strong password includes at least a special character, at the config:# prompt, type `security strongPasswords enforceAtLeastOneSpecialCharacter <option>`, and press Enter.**

  <options> is one of these options:

  - enable – At least one special character is required.
  - disable – No special character is required.

▼ Set the Maximum Password History

- **To determine the number of previous passwords that cannot be repeated when changing the password, at the config:# prompt, type `security strongPasswords passwordHistoryDepth <value>`, and press Enter.**

  <value> is an integer between 1 and 12.

Setting Role-Based Access Control

In addition to firewall access control based on IP addresses, you can configure other access control rules that are based on both IP addresses and user roles.

▼ Modify Role-Based Access Control Parameters

1. **To enable or disable the IPv4 role-based access control feature, at the config:# prompt, type `security roleBasedAccessControl ipv4 enabled <option>`, and press Enter.**

2. **To enable or disable the IPv6 role-based access control feature, at the config:# prompt, type `security roleBasedAccessControl ipv6 enabled <option>`, and press Enter.**

   <options> is one of these options:

   - true – Enables role-based access control.
   - false – Disables role-based access control.

3. **To determine the IPv4 role-based access control policy, at the config:# prompt, type `security roleBasedAccessControl ipv4 defaultPolicy <policy>`, and press Enter.**

4. **To determine the IPv6 role-based access control policy, at the config:# prompt, type `security roleBasedAccessControl ipv6 defaultPolicy <policy>`, and press Enter.**

   <policy> is one of these options:

   - allow – Accepts traffic from all IP addresses regardless of the user role.
   - deny – Drops traffic from all IP addresses regardless of the user role.

Note - You can combine both commands to modify all role-based access control parameters at a time.

Managing Role-Based Access Control Rules

You can add, delete or modify role-based access control rules.

▼ Add a Role-Based Access Control Rule

1. **To add a new IPv4 role-based access control rule at the bottom of the IPv4 rules list, at the config:# prompt, type `security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy>`, and press Enter.**

   For example, to add a new IPv4 role-based access control rule, dropping all packets from any IPv4 address between 192.168.78.50 and 192.168.90.100 when the user is a member of the role "admin," and insert the rule above the 3rd rule, at the config:# prompt, type `security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100 admin deny insertAbove 3`, and press Enter. The original 3rd rule becomes the 4th rule.

2. **To add a new IPv6 role-based access control rule at the bottom of the IPv4 rules list, at the config:# prompt, type `security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role> <policy>`, and press Enter.**

3. **To add a new IPv4 role-based access control rule by inserting it above or below a specific rule, at the config:# prompt, type `security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy> <insert> <rule_number>`, and press Enter.**

4. **To add a new IPv6 role-based access control rule by inserting it above or below a specific rule, at the config:# prompt, type `security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role> <policy> <insert> <rule_number>`, and press Enter.**

- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is the role for which you want to create an access control rule.

<policy> is one of these options:

- allow – Accepts traffic from the specified IP address range when the user is a member of the specified role.
- deny – Drops traffic from the specified IP address range when the user is a member of the specified role.

<insert> is one of the options:

Insert	Description
insertAbove	Inserts the new rule above the specified rule number. Then: new rule number = the specified rule number <rule_number> is the number of the existing rule which you want to insert the new rule above.
insertBelow	Inserts the new rule below the specified rule number. Then: new rule number = the specified rule number + 1 <rule_number> is the number of the existing rule which you want to insert the new rule below.

▼ Modify a Role-Based Access Control Rule

1. **To modify the IP address range an IPv4 role-based access control rule, at the config:# prompt, type `security roleBasedAccessControl ipv4 rule modify <rule_number> startIpAddress <start_ip> endIpAddress <end_ip>`, and press Enter.**

2. **To modify the IP address range an IPv4 role-based access control rule, at the config:# prompt, type `security roleBasedAccessControl ipv6 rule modify <rule_number> startIpAddress <start_ip> endIpAddress <end_ip>`, and press Enter.**

3. **To modify the rule role of an IPv4 role-based access control rule, at the config:# prompt, type `security roleBasedAccessControl ipv4 rule modify <rule_number> role <role>`, and press Enter.**

4. **To modify the rule role of an IPv6 role-based access control rule, at the config:# prompt, type `security roleBasedAccessControl ipv6 rule modify <rule_number> role <role>`, and press Enter.**

5. **To modify the policy of an IPv4 role-based access control rule, at the config:# prompt, type `security roleBasedAccessControl ipv4 rule modify <rule_number> policy <policy>`, and press Enter.**

6. **To modify the policy of an IPv6 role-based access control rule, at the config:# prompt, type `security roleBasedAccessControl ipv6 rule modify <rule_number> policy <policy>`, and press Enter.**

7. **To modify all contents of an existing IPv4 role-based access control rule, at the config:# prompt, type `security roleBasedAccessControl ipv4 rule modify <rule_number> startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>`, and press Enter.**

8. **To modify all contents of an existing IPv6 role-based access control rule, at the config:# prompt, type security roleBasedAccessControl ipv6 rule modify <rule_number> startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>, and press Enter.**

   - <rule_number> is the number of the existing rule that you want to modify.
   - <start_ip> is the starting IP address.
   - <end_ip> is the ending IP address.
   - <role> is the role for which you want to modify an access control rule.

   <policy> is one of these options:

- allow – Accepts traffic from the specified IP address range when the user is a member of the specified role.
- deny – Drops traffic from the specified IP address range when the user is a member of the specified role.

▼ Delete a Role-Based Access Control Rule

1. **To delete an IPv4 role-based access control in the list, at the config:# prompt, type `security roleBasedAccessControl ipv4 rule delete <rule_number>`, and press Enter.**

2. **To delete a IPv6 role-based access control rule in the list, at the config:# prompt, type `security roleBasedAccessControl ipv6 rule delete <rule_number>`, and press Enter.**

   <rule_number> is the number of the existing rule you want to delete.

▼ Enable or Disable Front Panel Actuator Control

1. **To enable the front panel actuator control by operating the front panel LCD display, at the config:# prompt, type `security frontPanelPermissions add switchActuator`, and press Enter.**

2. **To disable the front panel actuator control, at the config:# prompt, type `security frontPanelPermissions remove switchActuator`, and press Enter.**

   Note - If your HPDU supports multiple front panel permissions, you can combine them into one command by adding a semicolon (;) between different permissions.

Inlet Configuration Commands

You can change an inlet name and enable or disable an inlet.

▼ Change the Inlet Name

- **To change an inlet name, at the config:# prompt, type `inlet <n> name "<name>"`, and press Enter.**

  <n> is the number of the inlet that you want to configure. For a single-inlet HPDU, <n> is always 1. The value is an integer between 1 and 50.

  <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

▼ Enable or Disable an Inlet (for Multi-Inlet HPDUs)

- **To enable or disable an inlet for only multi-inlet HPDUs, at the config:# prompt, type `inlet <n> enabled <option>`, and press Enter.**

  Note - If running this command causes all inlets to be disabled, a warning message appears, prompting you to confirm. When this occurs, type **`y`** to confirm or **`n`** to cancel the operation.

  <n> is the number of the inlet that you want to configure. For a single-inlet HPDU, <n> is always 1. The value is an integer between 1 and 50.

  <option> is one of these options:

  - true – Enables the specified inlet.
  - false – Disables the specified inlet.

  For example, to assign the name "AC source" to inlet 1, at the config:# prompt, type `inlet 1 name "AC source"`, and press Enter. If your HPDU device contains multiple inlets, this command names the 1st inlet.

Overcurrent Protector Configuration Commands

An overcurrent protector configuration command configures an individual circuit breaker or fuse which protects outlets.

▼ Change the Overcurrent Protector Name

- **To create a name for a circuit breaker or a fuse which protects outlets on your HPDU, at the config:# prompt, type `ocp <n> name "<name>"`, and press Enter.**

  <n> is the number of the overcurrent protector that you want to configure. The value is an integer between 1 and 50.

  <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

  For example, to assign the name "Email servers CB" to the overcurrent protector labeled 2, at the config:# prompt, type `ocp 2 name "Email servers CB"`, and press Enter..

User Configuration Commands

Use the user configuration commands to change create, change, and delete user profile settings.

▼ Create a User Profile

1. **To create a new user profile, at the config:# prompt, type `user create <name> <option> <roles>`, and press Enter.**

   <name> is a string comprising up to 32 ASCII printable characters. The <name> variable CANNOT contain spaces.

   <option> is one of the options:

   - enable – Enables the newly-created user profile.
   - disable – Disables the newly-created user profile.

   <roles> is a role or a list of comma-separated roles assigned to the specified user profile. For example, to create a new user profile named May, enable the profile, and assign the Admin role to the user profile, at the config:# prompt, type `user create May enable admin`, and press Enter.

2. **When prompted to assign a password to the newly-created user, type the password, and press Enter.**

3. **Re-type the same password for confirmation and press Enter.**

Modifying a User Profile

You can change a user password, user personal data, enable or disable a user profile, force a password change, and change SNMPv3 settings, roles, measurement units, and SSH public key settings.

Tip: You can combine all commands to modify the parameters of a specific user profile at a time.

▼ Change a User Password

1. **Ensure that you have the Administrator Privileges and the HPDU is in configuration mode.**
2. **To change a user password, at the config:# prompt, type `user modify <name> password`, and press Enter.**

   <name> is the name of the user whose settings you want to change. For example, to change the password of the user "May," at the config:# prompt, type `user modify May password`, and press Enter.
3. **When prompted, type the password, and press Enter.**
4. **Re-type the same password for confirmation and press Enter.**

   If the password change is successful, the config:# prompt appears.

▼ Modify a User's Personal Data

You can change the full name, telephone number, and email address for a user.

Various commands can be combined to modify the parameters of a specific user profile at a time.

1. **Ensure that you have the Administrator Privileges and the HPDU is in configuration mode.**
2. **To change a user name, at the config:# prompt, type `user modify <name> fullName "<full_name>"`, and press Enter.**

<name> is the name of the user whose settings you want to change.

<full_name> is a string comprising up to 64 ASCII printable characters. The <full_name> variable must be enclosed in quotes when it contains spaces.

3. **To change a user's telephone number, at the config:# prompt, type `user modify <name> telephoneNumber "<phone_number>"`, and press Enter.**

   <phone_number> is the phone number that can reach the specified user. The <phone_number> variable must be enclosed in quotes when it contains spaces.

4. **To change a user's email address, at the config:# prompt, type `user modify <name> eMailAddress <email_address>`, and press Enter.**

   <email_address> is the email address of the specified user.

Enable or Disable a User Profile

- **To enable or disable a user profile, at the config:# prompt, type `user modify <name> enabled <option>`, and press Enter.**

  A user can log in to the HPDU device only after that user's user profile is enabled.

  <name> is the name of the user whose settings you want to change.

  <option> is one of the options:

  - true – Enables the specified user profile.
  - false – Disables the specified user profile.

Force a Password Change

- **To determine whether the password change is forced when a user logs in to the specified user profile next time, at the config:# prompt, type `user modify <name> forcePasswordChangeOnNextLogin <option>`, and press Enter.**

  <name> is the name of the user whose settings you want to change.

  <option> is one of the options:

  - true – Forces the user to change the password change on the next login.
  - false – Does not force the user to change the password change on the next login.

▼ Modify SNMPv3 Settings

You can combine all of the following commands to modify the SNMPv3 parameters at a time.

1. **To enable or disable the SNMP v3 access to HPDU for the specified user, at the config:# prompt, type `user modify <name> snmpV3Access <option1>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <option> is one of the options:

   - true – Enables the SNMP v3 access permission for the specified user.
   - false – Disables the SNMP v3 access permission for the specified user.

2. **To determine the security level, at the config:# prompt, type `user modify <name> securityLevel <option2>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

Security	Description
noAuthNoPriv	No authentication and no privacy.
authNoPriv	Authentication and no privacy.
authPriv	Authentication and privacy.

3. **To determine whether the authentication passphrase is identical to the password, at the config:# prompt, type `user modify <name> userPasswordAsAuthenticationPassphrase <option3>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <option3> is one of the options:

   - true – Authentication passphrase is identical to the password.
   - false – Authentication passphrase is different from the password.

4. **To determine the authentication passphrase, at the config:# prompt, type `user modify <name> authenticationPassPhrase <authentication_passphrase>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <authentication_passphrase> is a string used as an authentication passphrase, comprising 8 to 32 ASCII printable characters.

5. **To determine whether the privacy passphrase is identical to the authentication passphrase, at the config:# prompt, type `user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <option4> is one of the options:

   - true – Privacy passphrase is identical to the authentication passphrase.
   - false – Privacy passphrase is different from the authentication password.

6. **To determine the privacy passphrase, at the config:# prompt, type `user modify <name> privacyPassPhrase <privacy_passphrase>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <privacy_passphrase> is a string used as a privacy passphrase, comprising 8 to 32 ASCII printable characters.

7. **To determine the authentication protocol, at the config:# prompt, type `user modify <name> authenticationProtocol <option5>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <option5> is one of the options:

   - true – Privacy passphrase is identical to the authentication passphrase.
   - false – Privacy passphrase is different from the authentication password.

   MD5 - Applies the MD5 authentication protocol.

   SHA-1 - Applies the SHA-1 authentication protocol.

8. **To determine the privacy protocol, at the config:# prompt, type `user modify <name> privacyProtocol <option6>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <option6> is one of the options:

   - DES – Applies the DES privacy protocol.
   - AES-128 – Applies the AES-128 privacy protocol.

▼ Change the Role(s)

- **To change the role(s) of a specific user, at the config:# prompt, type `user modify <name> roles <roles>`, and press Enter.**

<name> is the name of the user whose settings you want to change.

<roles> is a role or a list of comma-separated roles assigned to the specified user profile.

For example, to assign two roles to the user May, admin and tester, at the config:# prompt, type `user modify May roles admin,tester`, and press Enter.

▼ Change Measurement Units

You can change the measurement units displayed for temperatures, length, and pressure for a user profile. Different measurement unit commands can be combined so that you can set all measurement units at a time.

1. **To set the preferred temperature unit, at the config:# prompt, type `user modify <name> preferredTemperatureUnit <option1>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <option1> is one of the options:

   - C – Displays the temperature in Celsius.
   - F – Displays the temperature in Fahrenheit.

2. **To set the preferred length unit, at the config:# prompt, type `user modify <name> preferredLengthUnit <option2>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <option2> is one of the options:

   - meter – Displays the length or height in meters.
   - feet – Displays the length or height in feet.

3. **To set the preferred pressure unit, at the config:# prompt, type `user modify <name> preferredPressureUnit <option3>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <option3> is one of the options:

   - pascal – Displays the pressure value in Pascals (Pa).
   - psi – Displays the pressure value in psi.

▼ Specify the SSH Public Key

If SSH key-based authentication is enabled, you can specify the SSH public key for each user profile.

1. **To specify or change the SSH public key for a specific user, at the config:# prompt, type `user modify <name> sshPublicKey`, and press Enter.**
   For example, to change the SSH public key for the user "assistant," at the config:# prompt, type `user modify assistant sshPublicKey`, and press Enter.
2. **When prompted to enter the content, perform the following steps:**
   a. **Open your SSH public key with a text editor.**
   b. **Copy all content in the text editor.**
   c. **Paste the content into the terminal.**
   d. **Press Enter.**
3. **To remove an existing SSH public key:**
   a. **At the config:# prompt, type `user modify <name> sshPublicKey`, and press Enter.**
   b. **When prompted to enter the content, press Enter without typing or pasting anything.**

▼ Delete a User Profile

- **At the config:# prompt, type `user delete <name>`, and press Enter.**

▼ Change Your Own Password

Every user can change their own password with this command if they have the Change Own Password privilege.

1. **At the config:# prompt, type `password`, and press Enter.**

2. **When prompted, type the current password, and press Enter.**

3. **When prompted, type the new password, and press Enter.**

4. **Re-type the new password for confirmation and press Enter.**

Note - After you change the password successfully, the new password is effective immediately no matter whether you type the `apply` command or not to save the changes.

▼ Set Default Measurement Units

Default measurement units, including temperature, length, and pressure units, apply to the HPDU user interfaces across all users except for those whose preferred measurement units are set differently by themselves or the administrator. Diverse measurement unit commands can be combined so that you can set all default measurement units at a time.

1. **To set the default temperature unit, at the config:# prompt, type `user defaultpreferences preferredTemperatureUnit <option1>`, and press Enter.**

   <option1> is one of the options:

   - C – Displays the temperature in Celsius.
   - F – Displays the temperature in Fahrenheit.

2. **To set the default length unit, at the config:# prompt, type `user defaultpreferences preferredLengthUnit <option2>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <option2> is one of the options:

   - meter – Displays the length or height in meters.
   - feet – Displays the length or height in feet.

3. **To set the default pressure unit, at the config:# prompt, type `user modify <name> preferredPressureUnit <option3>`, and press Enter.**

   <name> is the name of the user whose settings you want to change.

   <option3> is one of the options:

   - pascal – Displays the pressure value in Pascals (Pa).
   - psi – Displays the pressure value in psi.

For example, to set all default measurement units at a time, type `user defaultpreferences preferredTemperatureUnit F preferredLengthUnit feet preferredPressureUnit psi`, and press Enter.

- Default temperature unit is set to Fahrenheit.
- Default length unit is set to feet.
- Default pressure unit is set to psi.

Role Configuration Commands

You can create, modify, and delete one or more roles.

▼ Create a Role

- **To create a new role with privileges assigned to the role, at the config:# prompt, type `role create <name> <privilege1>;<privilege2>;<privilege3>...`, and press Enter.**

If a privilege contains any arguments, after the privilege, type a colon and the argument(s).

role create <name> <privilege1>:<argument1>,<argument2>...;

<privilege2>:<argument1>,<argument2>...;

<privilege3>:<argument1>,<argument2>...;

...

<name> is a string comprising up to 32 ASCII printable characters.

<privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon.

<argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

For example, to create a new role and assigns privileges to the role, at the config:# prompt, type `role create tester firmwareUpdate;viewEventSetup`, and press Enter.

A new role "tester" is created.

Two privileges are assigned to the role: firmwareUpdate (Firmware Update) and viewEventSetup (View Event Settings).

The following tables lists all privileges.

Privilege	Description
acknowledgeAlarms	Acknowledge Alarms
adminPrivilege	Administrator Privileges
changeAuthSettings	Change Authentication Settings
changeDataTimeSettings	Change Date/Time Settings
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePduConfiguration	Change Pdu, Inlet, & Overcurrent Protector Configuration
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings
changeUserSettings	Change Local User Management
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
viewEventSetup	View Event Settings
viewEverything	Unrestricted View Privileges
viewLog	View Local Event Log
viewSecuritySettings	View Security Settings
viewSnmpSettings	View SNMP Settings
viewUserSettings	View Local User Management

▼ Modify a Role

1. **To modify a role description, at the config:# prompt, type `role modify <name> description "<description>"`, and press Enter.**

   <name> is a string comprising up to 32 ASCII printable characters.

   <description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.

2. **To add more privileges to a role, at the config:# prompt, type `role modify <name> addPrivileges <privilege1>;<privilege2>;<privilege3>...`, and press Enter.**

If a privilege contains any arguments, add a colon and the argument(s) after that privilege. For example, type:

role modify <name> addPrivileges <privilege1>:<argument1>,<argument2>...;

<privilege2>:<argument1>,<argument2>...;

<privilege3>:<argument1>,<argument2>...;

...

<name> is a string comprising up to 32 ASCII printable characters.

<privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon.

<argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

3. **To remove privileges from a role, at the config:# prompt, type `role modify <name> removePrivileges <privilege1>;<privilege2>;<privilege3>...`, and press Enter.**

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege. For example, type:

role modify <name> removePrivileges <privilege1>:<argument1>,<argument2>...;

<privilege2>:<argument1>,<argument2>...;

<privilege3>:<argument1>,<argument2>...;

...

Note - When removing privileges from a role, ensure the specified privileges and arguments (if any) exactly match those assigned to the role. Otherwise, the command fails to remove specified privileges that are not available.

<name> is a string comprising up to 32 ASCII printable characters.

<privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon.

<argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

▼ Delete a Role

- **To delete a role, at the config:# prompt, type `role delete <name>`, and press Enter.**

Authentication Commands

You can set the authentication type only, or set the authentication type and determine whether to switch to local authentication in case the remote authentication is not available.

▼ Determine the Authentication Method

1. **To determine the authentication type only, at the config:# prompt, type `authentication type <option1>`, and press Enter.**

   Note - You cannot enable or disable the option of switching to local authentication without determining the authentication type in the CLI. Always type "authentication type <option1>" when setting up "useLocalIfRemoteUnavailable".

   <option1> is one of the options:

   - local – Enable Local authentication only.
   - ldap – Enable LDAP authentication.
   - radius – Enable Radius authentication.

2. **To determine the authentication type and enable/disable the option of switching to local authentication, at the config:# prompt, type `authentication type <option1> useLocalIfRemoteUnavailable <option2>`, and press Enter.**

   <option2> is one of the options:

   - true – Remote authentication is the first priority. The device switches to local authentication when the remote authentication is not available.
   - false – Retain remote authentication regardless of the availability of remote authentication.

LDAP Settings

If you enable LDAP authentication, you must add at least one LDAP server. Later, you can modify or delete any existing LDAP server as needed.

▼ Add an LDAP Server

You can repeat the following CLI command to add more than one LDAP server.

Note - If any LDAP server settings are identical to an existing LDAP server, you can add it by copying the existing one, instead of using the `ldap add` command.

---

1. **To add an LDAP server, at the config:# prompt, type `authentication ldap add <host> <port> <ldap_type> <security> <bind_type> <base_DN> <login_name_att> <user_entry_class> "Optional Parameters"`, and press Enter.**

   <host> is the IP address or host name of the LDAP server.

   <port> is the port number assigned for communication with the LDAP server.

   <ldap_type> is one of the LDAP server types:

   - openldap – OpenLDAP server.
   - activeDirectory – Microsoft Active Directory.

   <security> is one of the security options:

   - none – No security.
   - startTls – StartTLS.
   - tls – TLS

   <bind_type> is one of the bind options:

   - anonymouseBind – Enable the anonymous Bind. Bind DN and password are not required.
   - authenticatedBind – Enable the Bind with authentication. Bind DN and password are required.

   <base_DN> is the base DN for search.

   <login_name_att> is the login name attribute.

   <user_entry_class> is the User Entry Object Class.

Note - Optional Parameters are one or more parameters. They are required only when the server settings need to specify these parameters. For example, if you set the <bind_type> to `authenticatedBind`, add the parameter `bindDN`.

You can add one or multiple optional parameters, such as specifying the Bind DN or certificate upload, to an LDAP-server-adding command. If adding multiple optional parameters, add them to the end of the command and separate them with a space.

When you add a new LDAP successfully, a list of all LDAP servers appears, including the newly-added one.

2. **Verify all settings of a newly-added server.**

Example 1 Add an OpenLDAP Server

At the config:# prompt, type `authentication ldap add op-ldap.company.com 389 openldap none anonymousBind dc=company,dc=com uidinetOrgPerson`, and press Enter.

Example 2 Add a Microsoft Active Directory Server

At the config:# prompt, type `authentication ldap add ac-ldap.company.com 389 activeDirectory none anonymousBind dc=company,dc=com sAMAccountNameuseradDomain company.com`, and press Enter.

Example 3 Add a An LDAP Server with a TLS Certificate Uploaded

At the config:# prompt, type `authentication ldap add ldap.company.com 389 openldap startTls ... inetOrgPerson verifyServerCertificate true`, and press Enter.

Optional Parameters

Optional Parameter	Description
userSearchSubfilter <filter>	User search subfilter.
bindDN <bind_DN>	System prompts you to enter and re-confirm the bind password after adding the bind DN parameter to the command.
adDomain <AD_domain>	Active Directory Domain name.
verifyServerCertificate <verify_cert>	After setting Certificate verification to true, the system prompts you to upload a certificate.
allowExpiredCertificate <allow_exp_cert>	Whether to accept expired or not valid yet certificate.

<filter> is the user search subfilter you specify.

<bind_DN> is bind DN.

<AD_domain> is the Active Directory Domain.

<verify_cert> is one of the options:

- true – Enable the verification of the LDAP server certificate.
- false – Disable the verification of the LDAP server certificate.

<allow_exp_cert> is one of the options:

- true – Certificates that are either expired or not valid yet are all accepted.
- false – Only valid certificates are accepted.

Example 4 Specify an Active Directory Domain Name

At the config:# prompt, type `authentication ldap add <host> <port> <ldap_type> <security> <bind_type> <base_DN> <login_name_att> <user_entry_class> adDomain <AD_domain>`, and press Enter.

Example 5 Set up an LDAP Server with the Bind DN

At the config:# prompt, type `authentication ldap add <host> <port> <ldap_type> <security> <bind_type> <base_DN> <login_name_att> <user_entry_class> bindDN <bind_DN>`, and press Enter. When prompted, type or copy the certificate content in the CLI, and press Enter.

Note: The certificate's content is located between the line containing "BEGIN CERTIFICATE" and the line containing "END CERTIFICATE".

Example 6 Set up An LDAP server with the bind DN and bind password configured

At the config:# prompt, type `authentication ldap add op-ldap.company.com 389 openldap none authenticatedBind cn=Manager,dc=company,dc=com uid inetOrgPerson bindDN user@company.com`, and press Enter. When prompted, type the bind DN password, and press Enter. Re-type the same password.

▼ Copy the Settings from an Existing Server

If an existing server and a new server share the same settings, you can copy those settings to the new server.

- **To add an LDAP server by copying the settings from an existing server, at the config:# prompt, type `authentication ldap addClone <server_num> <host>`, and press Enter.**

  <host> is the IP address or host name of the LDAP server.

  <server_num> is the sequential number of the specified server shown on the server list of the HPDU.

▼ Modify an Existing LDAP Server

You can modify one or multiple parameters of an existing LDAP server, such as its IP address, TCP port number, and Base DN. You also can change the priority or sequence of existing LDAP servers in the server list.

- **To modify the settings on an existing LDAP server, at the config:# prompt, type `authentication ldap modify <server_num> "parameters"`, and press Enter.**

  <server_num> is the sequential number of the specified server in the LDAP server list.

  Replace "parameters" with one or multiple commands in the following table, depending on which parameter(s) you want to modify.

LDAP Server Parameter	Description
host <host>	Change the IP address or host name, where <host> is the new IP address or host name.
port <port>	Change the TCP port number, where <port> is the new TCP port number.
serverType <ldap_type>	Change the server type, where <ldap_type> is the new type of the LDAP server. <ldap_type> values include openldap and activeDirectory.
securityType <security>	Change the security type, where <security> is the new security type. <security> values include none, startTls, and ssl.
bindType <bind_type>	Change the bind type, where <bind_type> is the new bind type. <bind_type> values include anonymousBind and authenticatedBind.
searchBaseDN <base_DN>	Change the base DN for search, where <base_DN> is the new base DN for search.
loginNameAttribute <login_name_att>	Change the login name attribute, where <login_name_att> is the new login name attribute.
userEntryObjectClass <user_entry_class>	Change the user entry object class, where <user_entry_class> is the new user entry class.

LDAP Server Parameter	Description
userSearchSubfilter <user_search_filter>	Change the user search subfilter, where <user_search_filter> is the new user search subfilter.
adDomain <AD_domain>	Change the Active Directory Domain name, where <AD_domain> is the new domain name of the Active Directory.
verifyServerCertificate <verify_cert>	Enable or disable the certificate verification, where <verify_cert> enables or disables the certificate verification feature. Available values include true and false.
certificate	Re-upload a different certificate. 1. First add the "certificate" parameter to the command, and press Enter. 2. When prompted, type or copy the content of the certificate in the CLI, and press Enter.
allowExpiredCertificate <allow_exp_cert>	Determine whether to accept a certificate which is expired or not valid yet, where <allow_exp_cert> determines whether to accept an expired or not valid yet certificate. <allow_exp_cert> values include true and false.
bindDN <bind_DN>	Change the bind DN, where <bind_DN> is the new bind DN.
bindPassword	Change the bind DN password. 1. Add the "bindPassword" parameter to the command and press Enter. 2. When prompted, type the password, and press Enter.
sortPosition <position>	Change the priority of the server (sorting), where <position> is the new sequential number of the server in the LDAP server list.

Example 7 Change the IP Address of the 1st LDAP Server

At the config:# prompt, type `authentication ldap modify 1 host 192.168.3.3`, and press Enter.

Example 8 Change the IP address and TCP Port of the 1st LDAP Server

At the config:# prompt, type `authentication ldap modify 1 host 192.168.3.3 port 633`, and press Enter.

Example 9 Change the IP address, TCP Port, and the Type of the 1st LDAP Server

At the config:# prompt, type `authentication ldap modify 1 host 192.168.3.3 port 633 serverType activeDirectory`, and press Enter.

▼ Remove an LDAP Server

- **To remove an existing LDAP server from the server list, at the config:# prompt, type `authentication ldap delete <server_num>`, and press Enter.**

  <server_num> is the sequential number of the specified server in the LDAP server list.

Radius Settings

If you enable Radius authentication, you must add at least one Radius server. Later, you can modify or delete a Radius server.

▼ Add a Radius Server

1. **To add a Radius server, at the config:# prompt, type `authentication radius add <host> <rds_type> <auth_port> <acct_port> <timeout> <retries>`, and press Enter.**

   <host> is the IP address or host name of the Radius server.

   <rds_type> is one of the following Radius authentication types:

Radius Authentication Type	Description
chap	CHAP
pap	PAP
msChapV2	MSCHAP v2

   <auth_port> is the authentication port number.

   <acct_port> is the accounting port number.

   <timeout> is the timeout value between 1 to 10 seconds.

   <retries> is the number of retries between 0 to 5.

2. **To enter the shared secret, at the config:# prompt, type the secret, and press Enter.**

3. **Re-type the same secret and press Enter.**

4. **Repeat Steps 1-3 to add more Radius servers one by one.**

Example 10 Enter the Shared Secret for Adding a Radius Server

At the config:# prompt, type `authentication radius add 192.168.7.99 chap 1812 1813 10 3`, and press Enter.

Modify a Radius Server

You can modify one or multiple parameters of an existing Radius server, or change the priority or sequence of existing servers in the server list.

1. **To change the IP address or host name, at the config:# prompt, type `authentication radius modify <server_num> host <host>`, and press Enter.**
2. **To change the Radius authentication type, at the config:# prompt, type `authentication radius modify <server_num> authType <rds_type>`, and press Enter.**
3. **To change the Radius authentication port, at the config:# prompt, type `authentication radius modify <server_num> authPort <auth_port>`, and press Enter.**
4. **To change the Radius accounting port, at the config:# prompt, type `authentication radius modify <server_num> accountPort <acct_port>`, and press Enter.**
5. **To change the Radius timeout value, at the config:# prompt, type `authentication radius modify <server_num> timeout <timeout>`, and press Enter.**
6. **To change the Radius number of retries, at the config:# prompt, type `authentication radius modify <server_num> retries <retries>`, and press Enter.**
7. **To change the Radius shared secret, at the config:# prompt, type `authentication radius modify <server_num> secret`, and press Enter.**
8. **To change the priority of a server, at the config:# prompt, type `authentication radius modify <server_num> sortPositon <position>`, and press Enter.**

Note - You can add more than one parameter to the command. For example, `authentication radius modify` <*server_num*> `host` <*host*> `authType` <*rds_type*> `authPort` <*auth_port*> `accountPort` <*acct_port*> .

- <server_num> is the sequential number of the specified server in the Radius server list.
- <host> is the new IP address or host name of the Radius server.

- <rds_type> is one of the Radius authentication types: pap, chap, msChapV2
- <auth_port> is the new authentication port number.
- <acct_port> is the new accounting port number.
- <timeout> is the new timeout value in seconds. It ranges between 1 to 10 seconds.
- <retries> is the new number of retries. It ranges between 0 to 5.

▼ Remove a Radius Server

- **To remove a Radius server from the server list, at the config:# prompt, type `authentication radius delete <server_num>`, and press Enter.**
  <server_num> is the sequential number of the specified server in the Radius server list.

Server Reachability Configuration Commands

You can use the CLI to add or delete an IT device, such as a server, from the server reachability list, or modify the settings for a monitored IT device.

▼ Add a Monitored Device

- **To add a new IT device to the server reachability list, at the config:# prompt, type `serverReachability add <IP_host> <enable> <succ_ping> <fail_ping> <succ_wait> <fail_wait> <resume> <disable_count>`, and press Enter.**

  - <IP_host> is the IP address or host name of the IT device that you want to add.
  - <enable> is one of the options:
    - true – Enables the ping monitoring feature for the newly added device.
    - false – Disables the ping monitoring feature for the newly added device.
  - <succ_ping> is the number of successful pings for declaring the monitored device Reachable. Valid range is 0 to 200.
  - <fail_ping> is the number of consecutive unsuccessful pings for declaring the monitored device Unreachable. Valid range is 1 to 100.
  - <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
  - <fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).

- <resume> is the wait time before the HPDU resumes pinging after declaring the monitored device Unreachable. Valid range is 5 to 120 (seconds).
- <disable_count> is the number of consecutive Unreachable declarations before the HPDU disables the ping monitoring feature for the monitored device and returns to the `Waiting for reliable connection` state. Valid range is 1 to 100 or unlimited declarations.

Delete a Monitored Device

- **To delete a monitored device from the server reachability list, at the config:# prompt, type `serverReachability delete <n>`, and press Enter.**

  <n> is a number representing the sequence of the IT device in the monitored server list.

  You can find each IT device sequence number using the CLI command of show serverReachability.

Modify a Monitored Device's Settings

1. **To modify a device IP address or host name, at the config:# prompt, type `serverReachability modify <n> ipAddress <IP_host>`, and press Enter.**
2. **To enable or disable the ping monitoring feature for the device, at the config:# prompt, type `serverReachability modify <n> pingMonitoringEnabled <option>`, and press Enter.**
3. **To modify the number of successful pings for declaring Reachable, at the config:# prompt, type `serverReachability modify <n> numberOfSuccessfulPingsToEnable <succ_number>`, and press Enter.**
4. **To modify the number of unsuccessful pings for declaring Unreachable, at the config:# prompt, type `serverReachability modify <n> numberOfUnsuccessfulPingsForFailure <fail_number>`, and press Enter.**
5. **To modify the wait time after a successful ping, at the config:# prompt, type `serverReachability modify <n> waitTimeAfterSuccessfulPing <succ_wait>`, and press Enter.**
6. **To modify the wait time after an unsuccessful ping, at the config:# prompt, type `serverReachability modify <n> waitTimeAfterUnsuccessfulPing <fail_wait>`, and press Enter.**

7. **To modify the wait time before resuming pinging after declaring Unreachable, at the config:# prompt, type `serverReachability modify <n> waitTimeBeforeResumingPinging <resume>`, and press Enter.**

8. **To modify the number of consecutive Unreachable declarations before disabling the ping monitoring feature, at the config:# prompt, type `serverReachability modify <n> numberOfFailuresToDisable <disable_count>`, and press Enter.**

   <n> is a number representing the sequence of the IT device in the server monitoring list.

   <IP_host> is the IP address or host name of the IT device whose settings you want to modify.

   <option> is one of the options:

   - true – Enables the ping monitoring feature for the monitored device.
   - false – Disables the ping monitoring feature for the monitored device.

   - <succ_number> is the number of successful pings for declaring the monitored device Reachable. Valid range is 0 to 200.
   - <fail_number> is the number of consecutive unsuccessful pings for declaring the monitored device Unreachable. Valid range is 1 to 100.
   - <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
   - <fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).
   - <resume> is the wait time before the HPDU resumes pinging after declaring the monitored device Unreachable. Valid range is 5 to 120 (seconds).
   - <disable_count> is the number of consecutive Unreachable declarations before the HPDU disables the ping monitoring feature for the monitored device and returns to the "Waiting for reliable connection" state. Valid range is 1 to 100 or unlimited.

Example 11 Server Settings Changed

The following command modifies several ping monitoring settings for the second server in the server reachability list.

```
serverReachability modify 2 numberOfSuccessfulPingsToEnable 10
numberOfUnsuccessfulPingsForFailure 8 waitTimeAfterSuccessfulPing 30
```

Cisco EnergyWise Configuration Commands

You can configure the Cisco EnergyWise settings that monitor power consumption.

Enabling or Disabling EnergyWise

- **To determine whether the Cisco EnergyWise endpoint implemented on the HPDU device is enabled, at the config:# prompt, type `energywise enabled <option>`, and press Enter.**

  - true – Enables Cisco EnergyWise.
  - false – Disables Cisco EnergyWise.

Specify the EnergyWise Domain

- **To specify which Cisco EnergyWise domain the HPDU device belongs, at the config:# prompt, type `energywise domain <name>`, and press Enter.**

  <name> is a string comprising up to 127 ASCII printable characters, with no spaces and asterisks.

Specify the EnergyWise Secret

- **To specify the password (secret) to enter the Cisco EnergyWise domain, at the config:# prompt, type `energywise secret <password>`, and press Enter.**

  <password> is a string comprising up to 127 ASCII printable characters with no spaces and asterisks.

Change the UDP Port

- **To specify the UDP port for communications in the Cisco EnergyWise domain, at the config:# prompt, type `energywise port <port>`, and press Enter.**

  <port> is the UDP port number ranging between 1 and 65535.

Set the Polling Interval

- **To determine the polling interval at which the Cisco EnergyWise domain queries the HPDU device, at the config:# prompt, type `energywise polling <timing>`, and press Enter.**

<timing> is an integer number in seconds. It ranges between 30 and 600 seconds.

Example 12 Set Up EnergyWise

At the config:# prompt, type `energywise enabled true port 10288`, and press Enter.

The EnergyWise feature implemented on the HPDU is enabled.

The UDP port is set to 10288.

Serial Port Configuration Commands

You can configure the serial port by setting the baud rate and forcing Device Detection mode.

▼ Set the Baud Rates

You can set the baud rate (bps) of the serial port labeled CONSOLE/MODEM on the HPDU device. Change the baud rate before connecting it to a device, such as a computer or a modem, through the serial port, or communications errors occur. If you change the baud rate dynamically after the connection is made, reset the HPDU or power cycle the connected device for proper communications.

1. **To determine the console baud rate, at the config:# prompt, type `serial consoleBaudRate <baud_rate>`, and press Enter.**

2. **To determine the modem baud rate, at the config:# prompt, type `serial modemBaudRate <baud_rate>`, and press Enter.**

   <baud_rate> is one of the baud rate options:

   - 1200
   - 2400
   - 4800
   - 9600
   - 19200
   - 38400
   - 57600
   - 115200

▼ Force the Device Detection Mode

- **To force the serial port on the HPDU to enter a device detection mode, at the config:# prompt, type `serial deviceDetectionType <mode>`, and press Enter.**

  <mode> is one of the detection modes:

Detection Mode	Description
automatic	HPDU automatically detects the type of the device connected to the serial port. Select this option unless your HPDU cannot correctly detect the device type.
forceConsole	HPDU attempts to recognize that the connected device is set for the console mode.
forceAnalogModem	HPDU attempts to recognize that the connected device is an analog modem.
forceGsmModem	HPDU attempts to recognize that the connected device is a GSM modem.

Example 13 Set the Console Baud Rate of the HPDU Device Serial Port to 9600 bps

```
serial consoleBaudRate 9600
```

Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command to perform all of them at a time. All combined commands must belong to the same configuration type, such as commands prefixed with network, user modify, or sensor externalsensor.

A multi-command syntax looks like this:

<configuration type> <setting 1> <value 1> <setting 2> <value 2> <setting 3> <value 3>

EXAMPLE 14 Combination of IP, Subnet Mask and Gateway Parameters

The following multi-command syntax configures IPv4 address, subnet mask and gateway for the network connectivity simultaneously.

```
network ipv4 ipAddress 192.168.84.225 subnetMask 255.255.255.0 gateway 192.168.84.0
```

- The IP address is set to 192.168.84.225.
- The subnet mask is set to 255.255.255.0.
- The gateway is set to 192.168.84.0.

EXAMPLE 15 Combination of Upper Critical and Upper Warning Settings

The following multi-command syntax simultaneously configures Upper Critical and Upper Warning thresholds for the RMS current of the 2nd overcurrent protector.

```
sensor ocp 2 current upperCritical disable upperWarning 15
```

- The Upper Critical threshold of the 2nd overcurrent protector's RMS current is disabled.
- The Upper Warning threshold of the 2nd overcurrent protector's RMS current is set to 15A and enabled at the same time.

EXAMPLE 16 Combination of SSID and PSK Parameters

This multi-command syntax configures both SSID and PSK parameters simultaneously for the wireless feature.

```
network wireless SSID myssid PSK encryp_key
```

- The SSID value is set to myssid.
- The PSK value is set to encryp_key.

▼ Unblocking a User

If any user is blocked from accessing the HPDU, you can unblock them at the local console.

1. **Log in to the CLI interface using any terminal program through a local connection.**
2. **When the Username prompt appears, type unblock, and press Enter.**
3. **When prompted, type the name of the blocked user, and press Enter.**
   A message appears, indicating that the specified user was unblocked successfully.

▼ Restarting the HPDU

You can reset the HPDU device to factory defaults, or restart the HPDU using the CLI commands, which is not a factory default reset.

1. **Ensure you have entered administrator mode and the # prompt is displayed.**
2. **Type either of the following commands to restart the HPDU device.**
3. **At the # prompt, type `reset unit` or `reset unit/y`.**
4. **If you entered the command without "/y" in Step 2, a message appears prompting you to confirm the operation. Type y to confirm the reset.**
5. **Wait until the Username prompt appears, indicating the reset is complete.**

Note - Note: If you are performing this command over a USB connection, re-connect the USB cable after the reset is completed, or the CLI communications are lost.

▼ Resetting Active Energy Readings

You can reset either one active energy sensor or all active energy sensors at a time to restart the energy accumulation process.

1. **Verify that you have the Admin role.**
2. **To reset all active energy readings of the HPDU, at the # prompt, type `reset activeEnergy pdu` or `reset activeEnergy pdu /y`.**
3. **To reset the active energy readings for one inlet, at the # prompt, type `reset activeEnergy inlet <n>` or `reset activeEnergy inlet <n> /y`.**

▼ Resetting to Factory Defaults

1. **To reset HPDU settings after login, at the # prompt, type `reset factorydefaults` or `reset factorydefaults/y`.**
2. **To reset HPDU settings before login, for Username, type `factorydefaults`.**

Network Troubleshooting

The HPDU provides four diagnostic commands for troubleshooting network problems: nslookup, netstat, ping, and traceroute. The diagnostic commands function as corresponding Linux commands and can get corresponding Linux outputs.

▼ Entering Diagnostic Mode

Diagnostic commands function in Diagnostic mode only.

1. **At the # prompt or > prompt, type `diag`, and press Enter.**

2. **At the diag# or diag> prompt, type any diagnostic commands for troubleshooting.**

▼ Quitting Diagnostic Mode

- **At the diag# or diag> prompt, type `exit`.**

▼ Using Diagnostic Commands

The diagnostic command syntax varies, depending on the command.

1. **To query Internet domain name server (DNS) information of a network host, at diag>, type nslookup <host>.**

   <host> is the name or IP address of the host whose DNS information you want to query.

2. **To display network connections and the status of ports, at diag>, type netstat <option>.**

   <option> is one of the options:

Network Connection Option	Description
ports	Shows TCP/UDP ports.
connections	Shows network connections.

3. **To test the network connectivity, at diag>, type ping <host>.**

   <host> is the host name or IP address whose networking connectivity you want to check.

   The ping command sends the ICMP ECHO_REQUEST message to a network host for checking its network connectivity. If the output shows the host is responding properly, the network connectivity is good. If not, either the host is shut down or it is not being properly connected to the network.

You can include any or all of the additional options in the following table.

Network Connectivity Option	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number between 1 and 100.
size <number2>	Determines the packet size. <number2> is an integer number in bytes between 1 and 65468.
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds ranging from 1 to 600.

The command with all options: `ping <host> count <number1> size <number2> timeout <number3>`

Example 17 Example - Ping Command

The following command checks the network connectivity of the host 192.168.84.222 by sending the ICMP ECHO_REQUEST message to the host for 5 times.

At diag>, type ping 192.168.84.222 count 5.

▼ Tracing the Route

- **To trace the network route between your HPDU device and a network host, at diag>, type traceroute <host>.**

  <host> is the name or IP address of the host you want to trace.

▼ Retrieving Previous Commands

- **If you want to retrieve any command that was previously typed in the same connection session, press the Up arrow on the keyboard several times until the command you want displays.**

▼ Automatically Completing a Command

1. **To have a command completed automatically, type initial letters or words of the command.**

Ensure the letters or words you typed are unique so that the CLI can identify the command you want.

2. **Press Tab or Ctrl+i until the complete command appears.**

3. **If there are more than one possible commands, when a list of these commands displays, type the full command.**

▼ Logging Out of CLI

After completing your tasks using the CLI, always log out of the CLI to prevent others from accessing the CLI.

1. **Ensure that you are in Administrator mode and the # prompt displays.**

2. **Type `exit` and press Enter.**

SNMP

You can set up the HPDU for use with an SNMP manager, and configure the HPDU to send traps, inform an SNMP manager, and receive GET and SET commands to retrieve status and configure basic settings.

▼ Enabling and Configuring SNMP

1. **To enable SNMP protocols, select Device Settings → Network Services → SNMP.**

2. **In the SNMP Agent section, enable SNMP v1/v2c or SNMP v3.**

3. **Configure the settings, such as the community strings.**

4. **Select User Management → Users.**

5. **If authentication and privacy is enabled, configure the SNMP password(s) in the user settings.**

6. **If you enabled SNMP v3, perform these steps.**

   a. **Determine which users need SNMP v3 access permission.**

   b. **Create or modify users to enable their SNMP v3 access permission.**

Enabling SNMPv2c Notifications

1. **Select Device Settings → Network Services → SNMP.**
2. **In the SNMP Agent, ensure Enable SNMP v1/v2c is selected.**
3. **In the SNMP Notifications section, ensure Enable SNMP Notifications is selected.**
4. **Select SNMPv2c Trap or SNMPv2c Inform as the notification type.**
5. **Type values in the following fields and click Save.**

   Note - Any changes you make to the SNMP Notifications section on the SNMP page updates the settings of the System SNMP Notification Action, and vice versa.

SNMPv2c Notification Setting	Description
Timeout	Interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
Number of Retries	Number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
Host	IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent. You can specify up to 3 SNMP destinations.
Port	Port number used to access the device(s).
Community	SNMP community string to access the device(s). The community is the group representing the HPDU and all SNMP management stations.

Enabling SNMPv3 Notifications

1. **Select Device Settings → Network Services → SNMP.**
2. **In the SNMP Agent section, ensure Enable SNMP v1/v2c is selected.**
3. **In the SNMP Notifications section, ensure Enable SNMP Notifications is selected.**
4. **Select SNMPv3 Trap or SNMPv3 Inform as the notification type.**
5. **Type values in the following fields and click Save.**

Note - Any changes you make to the SNMP Notifications section on the SNMP page updates the settings of the System SNMP Notification Action, and vice versa.

SNMPv3 Notification Setting	Description
Timeout	Interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
Host	IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent.
Number of Retries	Specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
Port	Port number used to access the device(s).
Community	SNMP community string to access the device(s). The community is the group representing the HPDU and all SNMP management stations..

▼ Downloading SNMP MIB

Download an SNMP MIB file for SNMP communications. Always use the latest SNMP MIB downloaded from the current firmware of your HPDU.

- **You can download the MIBs from two different pages of the web interface.**

  - **To download MIB from the SNMP page:**

    a. **Select Device Settings → Network Services → SNMP.**

    b. **Click the Download MIBs title bar.**

    c. **Select the MIB file to download.**

       - PDU2-MIB – SNMP MIB file for HPDU power management.
       - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
       - LHX-MIB: The SNMP MIB file for managing the LHX/SHX heat exchanger(s).

    d. **Click Save to save the file onto your computer.**

- **To download MIB from the Device Information page:**

  a. **Select Maintenance → Device Information.**

  b. **In the Information section, click the download link:**

     - PDU2-MIB
     - ASSETMANAGEMENT-MIB
     - LHX MIB (Available only after you enable LHX/SHX support)

  c. **Click Save to save the file onto your computer.**

SNMP Gets and Sets

In addition to sending notifications, the HPDU can receive SNMP get and set requests from third-party SNMP managers.

- Get requests – Retrieves information about the HPDU, such as the system location.
- Set requests – Configures a subset of the information, such as the SNMP system name.

Note - The SNMP system name is the HPDU device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The HPDU does not support configuring IPv6-related parameters using the SNMP set requests.

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

HPDU MIB

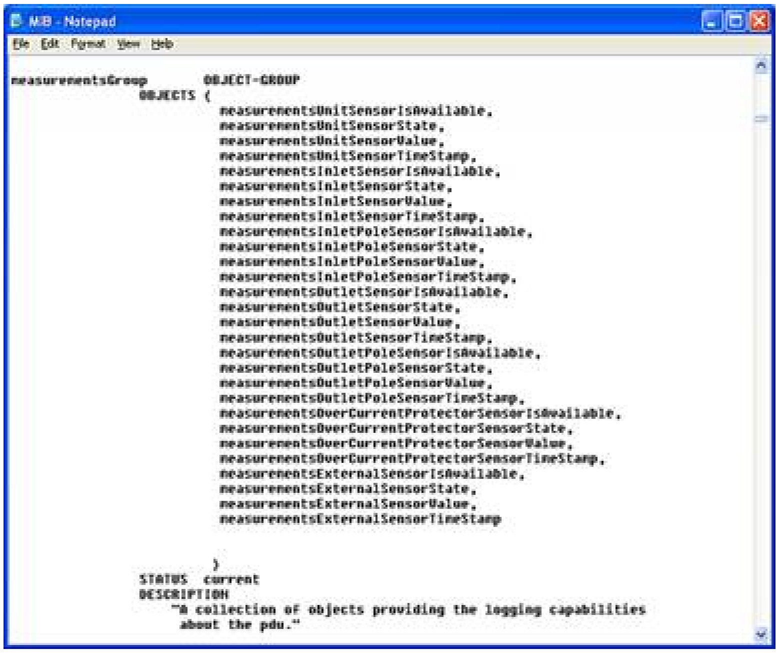
The SNMP MIB file is required for using your HPDU device with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Layout

Opening the MIB reveals the custom objects that describe the HPDU system at the unit level.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.

For example, the measurementsGroup group contains objects for sensor readings of HPDU as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor value". pduRatedCurrent, part of the configGroup group, describes the HPDU current rating.



```
measurementsGroup        OBJECT-GROUP
                 OBJECTS {
                           measurementsUnitSensorIsAvailable,
                           measurementsUnitSensorState,
                           measurementsUnitSensorValue,
                           measurementsUnitSensorTimeStamp,
                           measurementsInletSensorIsAvailable,
                           measurementsInletSensorState,
                           measurementsInletSensorValue,
                           measurementsInletSensorTimeStamp,
                           measurementsInletPoleSensorIsAvailable,
                           measurementsInletPoleSensorState,
                           measurementsInletPoleSensorValue,
                           measurementsInletPoleSensorTimeStamp,
                           measurementsOutletSensorIsAvailable,
                           measurementsOutletSensorState,
                           measurementsOutletSensorValue,
                           measurementsOutletSensorTimeStamp,
                           measurementsOutletPoleSensorIsAvailable,
                           measurementsOutletPoleSensorState,
                           measurementsOutletPoleSensorValue,
                           measurementsOutletPoleSensorTimeStamp,
                           measurementsOverCurrentProtectorSensorIsAvailable,
                           measurementsOverCurrentProtectorSensorState,
                           measurementsOverCurrentProtectorSensorValue,
                           measurementsOverCurrentProtectorSensorTimeStamp,
                           measurementsExternalSensorIsAvailable,
                           measurementsExternalSensorState,
                           measurementsExternalSensorValue,
                           measurementsExternalSensorTimeStamp


                          }
                 STATUS   current
                 DESCRIPTION
                     "A collection of objects providing the logging capabilities
                      about the pdu."
```

SNMP Sets and Thresholds

You can configure objects with a MAX-ACCESS level of read-write in the MIB from the SNMP manager using SNMP set commands.

These objects include threshold objects, which causes the HPDU to generate a warning and send an SNMP notification when certain parameters are exceeded.

Note - When configuring thresholds with SNMP set commands, ensure the value of upper critical threshold is higher than that of upper warning threshold.

▼ Configure NTP Server Settings

Using SNMP, you can change the following NTP server-related settings in the unitConfigurationTable:

1. **Enable or disable synchronization of the device date and time with NTP servers (synchronizeWithNTPServer).**
2. **Enable or disable the use of DHCP-assigned NTP servers if synchronization with NTP servers is enabled (useDHCPProvidedNTPServer).**
3. **Manually assign the primary NTP server if the use of DHCP-assigned NTP servers is disabled (primaryNTPServerAddressType and primaryNTPServerAddress).**
4. **Manually assign the secondary NTP server (optional) (secondaryNTPServerAddressType and secondaryNTPServerAddress).**

Note - When using the SNMP SET command to specify or change NTP servers, it is required that you set both the NTP server address type and address in the command line simultaneously.

For example, the following SNMP command changes the primary NTP server address from IPv4 (192.168.84.84) to host name:

snmpset -v2c -c private 192.168.84.84 firstNTPServerAddressType = dns firstNTPServerAddress = "angu.pep.com"

Caution - When enabling previously-disabled thresholds through SNMP, ensure you set a correct value for all thresholds that are supposed to be enabled before actually enabling them. Otherwise, you might get an error message.

Secure Copy (SCP) Commands

You can perform a Secure Copy (SCP) command to update the HPDU firmware, perform a bulk configuration, or back up and restore the configuration.

▼ Firmware Update through SCP

A firmware update through SCP is the same as any HPDU firmware update, where all user management operations are suspended and all login attempts fail during the SCP firmware update.

1. **Type `scp <firmware file> <user name>@<device ip>:/fwupdate` and press Enter.**

   <firmware file> –- HPDU firmware file name. If the firmware file is not in the current directory, include the path in the file name.

   <user name> – Admin or any user profile with the Firmware Update permission.

   <device ip> – IP address of the HPDU that you want to update.

   SCP example – `scp pdu-px2-030000-41270.bin admin@192.168.87.50:/fwupdate`

   Windows PSCP example – `pscp <firmware file> <user name>@<device ip>:/fwupdate`

2. **When prompted, type the password, and press Enter.**

   The system transmits the specified firmware file to the HPDU, and shows the transmission speed and percentage. When the transmission is complete, a message appears indicating that the HPDU starts the firmware update. The connection is closed.

3. **Wait until the upgrade finishes.**

▼ Bulk Configuration through SCP

1. **Save a configuration from a source HPDU.**

2. **Copy the configuration file to one or multiple destination HPDUs.**

3. **To save the configuration through SCP:**

   a. **Type `scp <user name>@<device ip>:/bulk_config.txt` and press Enter.**

      <user name> – Admin or any user profile with the Firmware Update permission.

      <device ip> – IP address of the HPDU that you want to update.

   b. **When prompted, type the user password, and press Enter.**

      The system saves the configuration from the HPDU to a file named `bulk_config.txt`.

4. **To copy the configuration through SCP:**

   a. **Type `scp bulk_config.txt <user name>@<device ip>:/bulk_restore` and press Enter.**

      <user name> – Admin or any user profile with the Firmware Update permission.

      <device ip> – IP address of the HPDU that you want to update.

   b. **When prompted, type the user password, and press Enter.**

      The system copies the configuration included in the file `bulk_config.txt` to another HPDU, and displays a message about starting the restore operation and closing the connection.

▼ Back up and Restore through SCP

To back up all HPDU settings, including device settings, perform the backup operation instead of the bulk configuration through SCP. You can restore all settings to previous ones after a backup file is available.

1. **To back up all HPDU settings, type `scp <user name>@<device ip>:/backup_settings.txt` and press Enter.**

   <user name> – Admin or any user profile with the Firmware Update permission.

   <device ip> – IP address of the HPDU that you want to update.

2. **When prompted, type the user password, and press Enter.**

   The system saves the settings from the HPDU to a file named `backup_settings.txt`.

3. **To restore the settings through SCP:**

   a. **Type `scp backup_settings.txt <user name>@<device ip>:/settings_restore` and press Enter.**

      <user name> – Admin or any user profile with the Firmware Update permission.

      <device ip> – IP address of the HPDU that you want to update.

   b. **When prompted, type the user password, and press Enter.**

      The system copies the configuration included in the file `backup_settings.txt` to the HPDU, and displays a message about starting the restore operation and closing the connection.

▼ Downloading Diagnostic Data through SCP

1. **Type one of the following SCP commands and press Enter.**

   - **Use the default SCP port and default file name. For example, `scp <user name>@<device ip>:/diag-data.zip .`**

     SSH/SCP port is the default (22), and the accessed HPDU is a standalone device.

     The diagnostic file default file name is `diag-data.zip`. Add a period (.) at the end of the SCP command.

   - **Specify a different SCP port but use the default file name. For example, `scp -P <port> <user name>@<device ip>:/diag-data.zip .`**

     SSH/SCP port is NOT the default (22), or the accessed HPDU is a Port-Forwarding slave device.

     The diagnostic file default file name is `diag-data.zip`. Add a period (.) at the end of the SCP command.

   - **Specify a new file name but use the default SCP port. For example, `scp -P <port> <user name>@<device ip>:/diag-data.zip <filename>`**

     SSH/SCP port is the default (22), and the accessed HPDU is a standalone device.

     Rename the diagnostic file.

If you specify a new filename in the command, the downloaded file is renamed accordingly.

- **Specify a different SCP port and a new filename.**

  SSH/SCP port is not the default (22), or the accessed HPDU is a Port-Forwarding slave device.

  Rename the diagnostic file.

<user name> – Admin or any user profile with the Firmware Update permission.

<device ip> – IP address of the HPDU that you want to update.

<port> – Current SSH/SCP port number, or the port number of a slave device in the Port-Forwarding chain.

<filename> – New filename of the downloaded diagnostic file.

2. **Type the password when the system prompts you to type it.**

   The system downloads the diagnostic data from the HPDU to your computer.

   If you do not specify a new filename in the command, the downloaded file default name is `diag-data.zip`.

   If you specify a new filename in the command, the downloaded file is renamed accordingly.

Servicing HPDUs

You can replace the controller on a HPDU.

Replaceable Controller

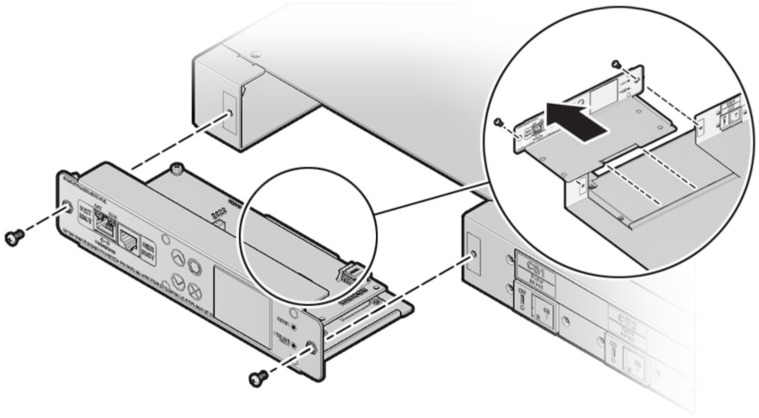
The connection ports and LCD display are located on a replaceable controller. If the controller is faulty, you can send the controller to Oracle for repair, or purchase a new controller from Oracle.

▼ Replace a Controller

1. **Attach a wrist strap to your wrist and to the ESD grounding jack on the rear rail of the rack.**

2. **With the HPDU powered on, use a #1 Phillips screwdriver to remove the screws on the left and right sides of the front of the HPDU controller, and pull out the controller.**

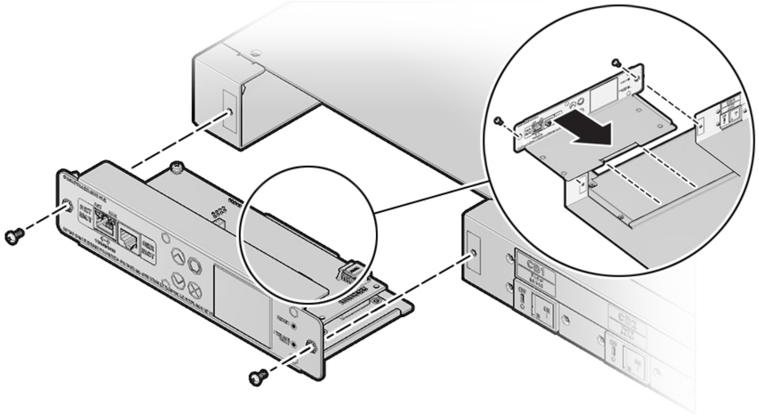
3. **Disconnect the HPDU controller cable from the controller.**



4. **Connect the HPDU controller cable to the new controller.**

5. **Push the new controller back into the HPDU until the controller flange clips to the back of the chassis edge.**

6. **Use a #1 Phillips screwdriver to secure the screws on the left and right sides of the front of the HPDU controller.**



Index