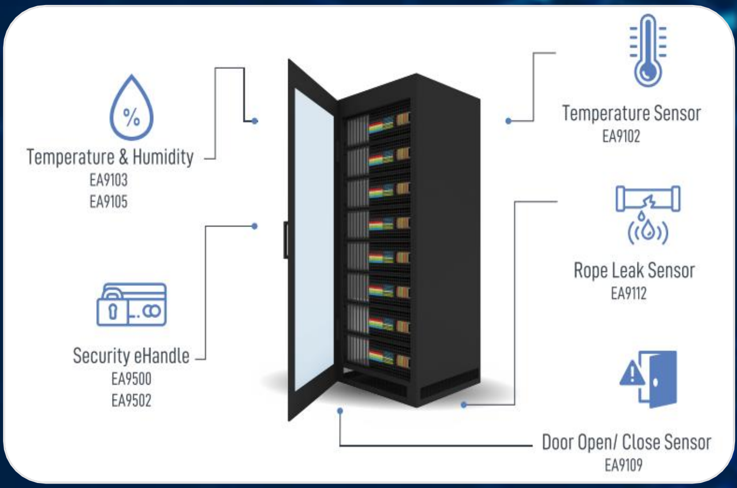
enLOGIC by nVent



Advantage & Secure

Power Distribution Units

USER MANUAL VERSION 1.2

Revision History

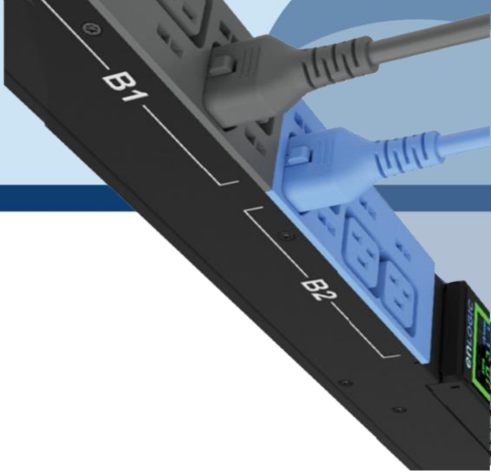
Versions	**Dates**	**Updates**
V1.0	25.09.2023	Preliminary Release
V1.1	18.12.2023	• CLI Commands • Questions & Answers only
V1.2	13.03.2024	• Seven Segment Alarms • NTP Commands • Power Share Features • Curl Commands • Questions & Answers

Table of Contents

Safety Instruction

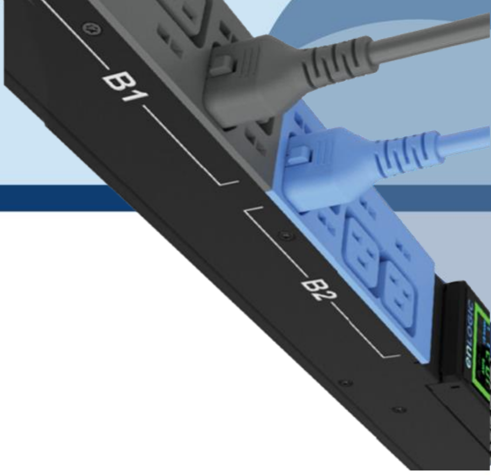
General Installation

Product Description



Network Security Hardening Guide

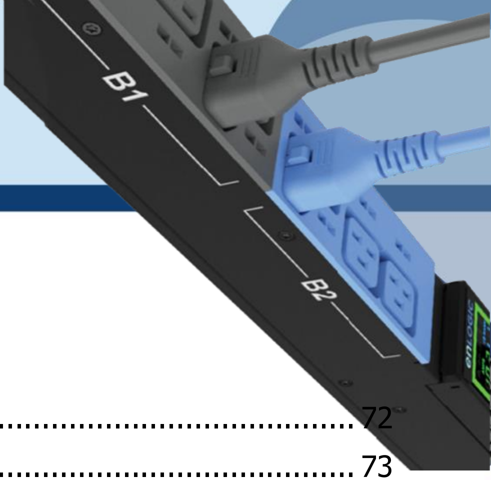
Main Menu Selections

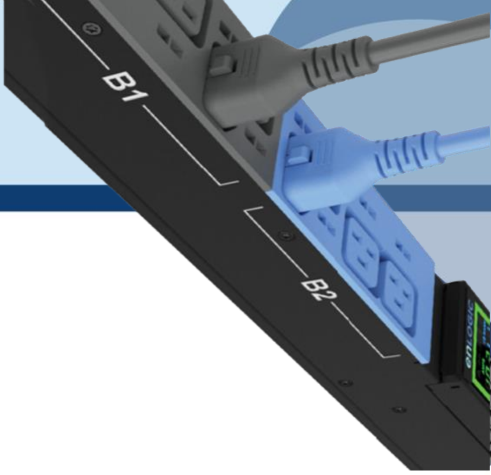


Outlet Units

Mounting PDU in Server Cabinet

Web User Interface (UI)


B1
B2

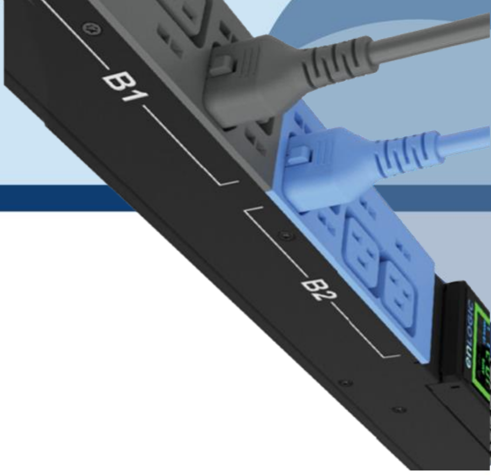


RESTAPI – CURL Commands

The Command Line Interface (CLI)

Sensors

Statutory Information



Safety Instruction

General Safety Instructions

- This Power Distribution Unit (PDU) unit is intended to provide power to the IT equipment only. Do not connect the secondary power units to the outlets of the PDU.

- It is recommended not to operate the system with Internet from a public network, but with an internal network protected externally with firewalls.

- When remote accesses are deployed, select a secure access path, such as VPN (Virtual Private Network) or HTTPS.

- Ensure that the current Enlogic firmware is installed on all Enlogic iPDUs.

- Restrict access authorizations to networks and systems to only persons that need an authorization and disable unused user accounts.

- This product generates, uses, and radiates radio frequency energy, which can cause harmful interference to radio communications if not installed and used in accordance with the instruction manual. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

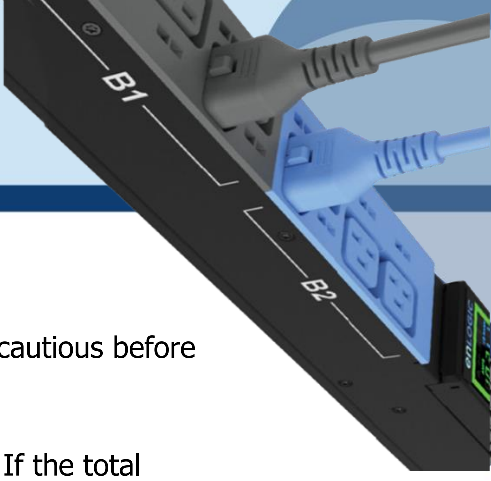
Installation and Operation Safety Instructions

- Assembly and installation of the PDU may only be performed by experienced, trained, and authorized personnel.

- Please observe the valid regulations for electrical installation in the country in which the PDU is installed and operated, and the national regulations for accident prevention. Please also observe any internal company regulations, such as work, operating and safety regulations.

- Operating the system in direct contact with water, aggressive materials or inflammable gases and vapors is prohibited.

- The PDU must not be opened. It does not contain any parts that need servicing.



- Internal parts of the PDU can get extremely hot during operation. Be cautious before handling.

- There is a risk of electrical shock from the ground conductor leakage. If the total leakage current exceeds 3.5 mA or if leakage current of the connected load is unknown, connect the ground terminal of the PDU to a dependable ground/earth connection.

- This equipment must be connected to an electrical supply with protected ground outlets and a branch circuit breaker with the same current rating as the equipment. Test all outlets for proper polarity and grounding. Failure to comply with this requirement can result in severe injury.

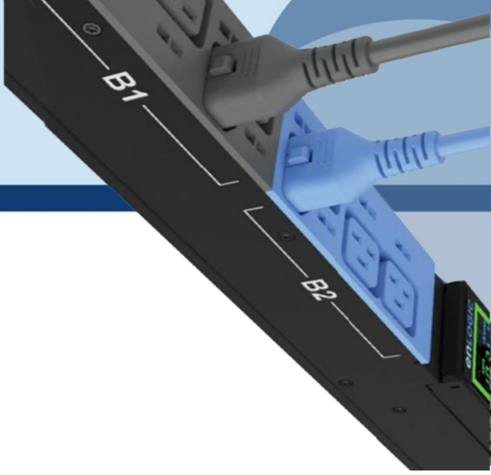
- Use only original Enlogic accessories or products recommended by Enlogic along with the Enlogic iPDU.

- Changes and modifications to this equipment can affect the warranty. Enlogic is not responsible for damage to this product, resulting from accident, disaster, or misuse.

Safety Instructions – Disclaimer

Enlogic by nVent accepts no liability for any errors in this documentation. To the maximum extent permissible by law, any liability for damage, direct or indirect, arising from the supply or use of this documentation is excluded.

Enlogic by nVent retains the right to modify this document, including the liability disclaimer, at any time without notice and accepts no liability for any consequences of such alterations.



Safety Symbols

In these original operating instructions, warning notices point out residual risks that cannot be avoided by constructive means when installing or operating the Enlogic iPDU. The warning notices are classified according to severity of the damage occurring and its statistic occurrence.

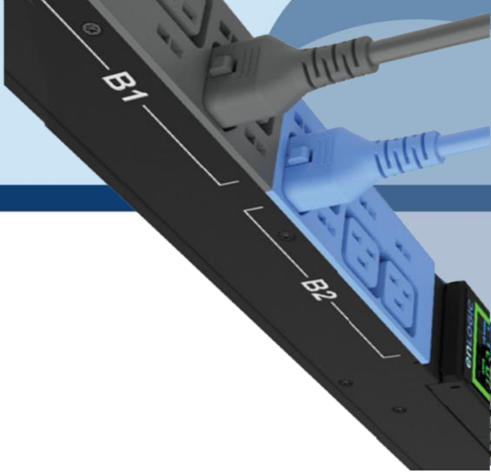
⚠ DANGER	
Symbol	**Brief description of the danger** The signal word DANGER indicates an immediate danger. Non-observance will result in severe injuries or death.

⚠ WARNING	
Symbol	**Brief description of the danger** The signal word WARNING indicates danger. Non-observance can lead to severe injury or death.

⚠ CAUTION	
Symbol	**Brief description of the danger** The signal word CAUTION indicates a danger. Non-observance can lead to injuries.

ATTENTION
Brief description The signal word ATTENTION indicates damages to equipment. Non-observance can lead to damage to the device.

ℹ	**Important Information**



Safety Information for Operators

Only trained specialists are authorized to carry out assembly, commissioning, completion, maintenance, and service of the Enlogic iPDU. The nationally applicable health and safety regulations must be adhered as well.

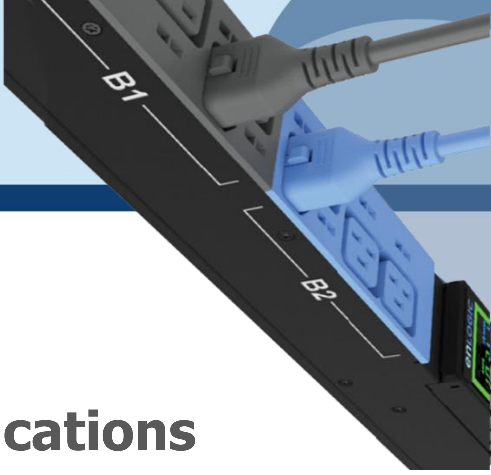
⚠ WARNING	
⚠	**Risk of injury due to insufficient personal protective equipment** If you use wrong / no protective equipment at all, serious injuries are possible. - Wear protective equipment adapted to the work processes. - Check the protective equipment before each use to ensure that it is intact! - Use only approved protective equipment.

Product Labels and Standards

This equipment has been evaluated and found to comply with the limits for a Class A digital device, pursuant to part 15 of the **FCC** Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This product is CE compliant, and UL tested. An appropriate declaration of conformity has been issued and can be supplied on request.

The Power Cable of this product must be used exclusively for the respective PDU only.



References and Architecture Specifications

Related Documents

This product meets the requirements of the following specifications:

Electromagnetic Compatibility

The requirements of the following EMC standards for electrical equipment are fulfilled and verified via an independent EMC test laboratory.

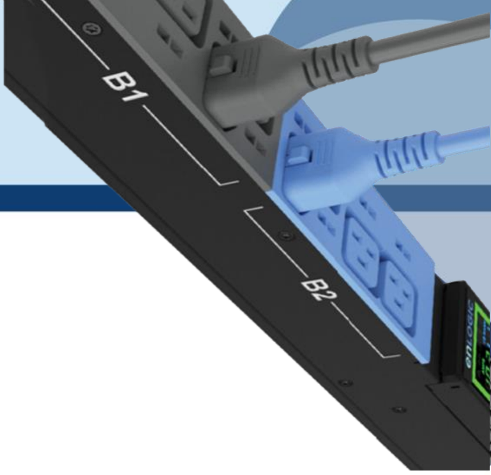
EN 61326-1 class B group 1	Basic Immunity
EN 61000-3-3	Limitation of voltage changes, voltage fluctuations and flicker
EN 61000-3-2	Limits for harmonic current emissions

CE / UKCA Compliance

LVD	2014/35/EU	Low-Voltage Directive
EMC	2014/30/EU	Electromagnetic Compatibility Directive
RoHS	2011/65/EU	RoHS Directive-2

Products fulfilling those requirements are marked with a CE/UKCA label.

For Declarations of Conformity of this product please visit www.enlogic.com



General Installation

Unpacking

ATTENTION

When opening the shipping carton, use caution to avoid damaging the system.

Consider the following when unpacking and storing the system:

- Leave the system packed until it is needed for immediate installation.
- After unpacking the system, save and store the packaging material in case the system must be returned.

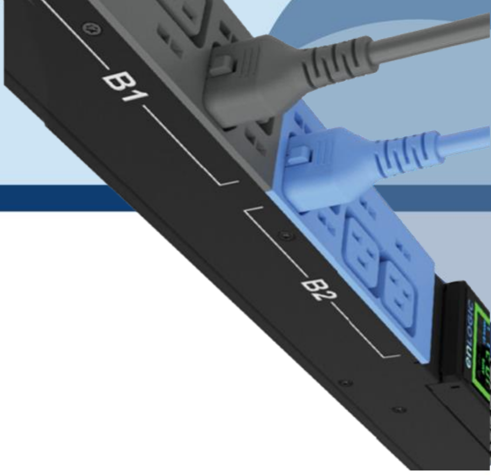
If the packaging is damaged and system damage is present, report to the shipper and analyze the damage.

Initial Operation

⚠ WARNING

Risk of injury and accidents due to insufficiently qualified personnel!
The installation may only be carried out by qualified personnel who are authorized to do so according to the valid safety regulations, e.g., by authorized specialized companies or authorized departments of the company.

- Ensure that the system has not been damaged during transport, storage, or assembly.



UL 2900 Certified by UL CAP

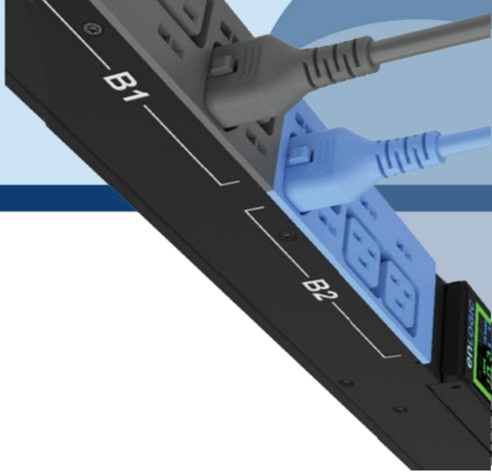
Enlogic iPDUs have been certified by Underwriter Laboratories through the UL Cybersecurity Assurance Program (UL CAP) against the presence of vulnerabilities, malware and security-relevant software weaknesses for cybersecurity assured products.

UL2900 certification specifies the methods by which a product is evaluated and tested for the presence of vulnerabilities, software weaknesses and malware. It has been adopted as an American National Standards Institute (ANSI) standard. The standard includes requirements and methods to evaluate and test network-connectable products, including:

- Software developer requirements and risk management process for the product.
- Evaluation and test methods for the presence of vulnerabilities, software weaknesses, and malware.
- Security risk control requirements for the architecture and design of a product.

As the world becomes more sustainable and electrified and global demand for data continues to grow, we will continue to develop innovative solutions to connect, protect and manage heat in critical systems for our data solutions customers. From energy-efficient cooling solutions to keeping operations safe from cyber threats, we are ready to meet our customers’ ever-changing needs.

UL® CERTIFIED SECURITY



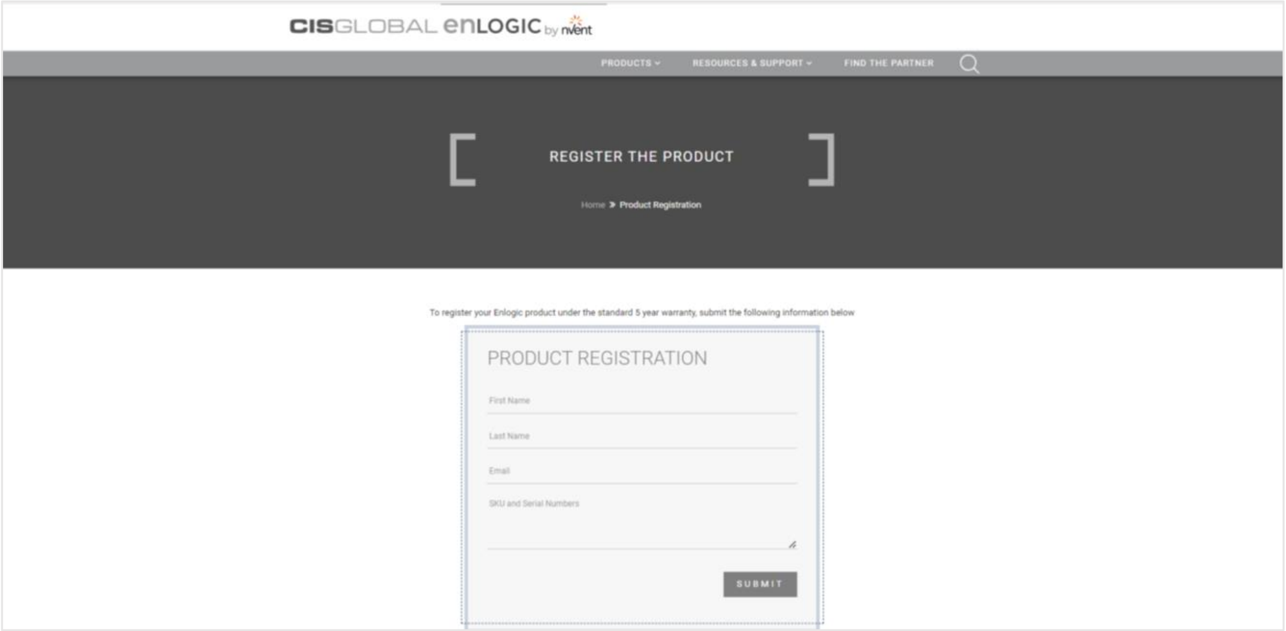
Product & Documents

This unit is delivered in a cardboard box and contains:

- PDU & NMC
- PLUGS & WIRES
- QUICK START GUIDE
- SAFETY INFORMATION SHEET
- WARRANTY CARD

Check the unit for any damage that may have occurred during transport. Any damage and other faults, e.g., incomplete delivery, should be reported immediately, in writing, to the shipping company and to Enlogic Systems LLC.

Use the information provided in the enclosed warranty card to register your product online at www.enlogic.com



To register your Enlogic product under the standard 5 year warranty, submit the following information below

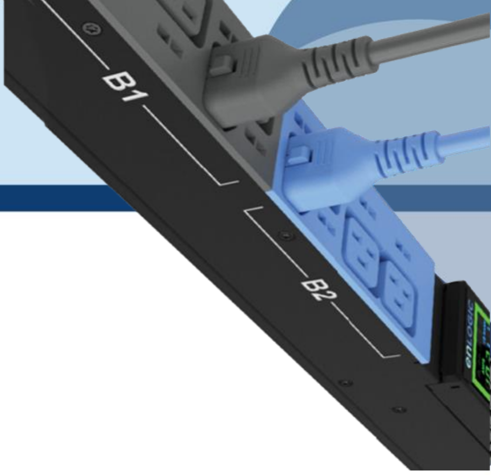
PRODUCT REGISTRATION

First Name

Last Name

Email

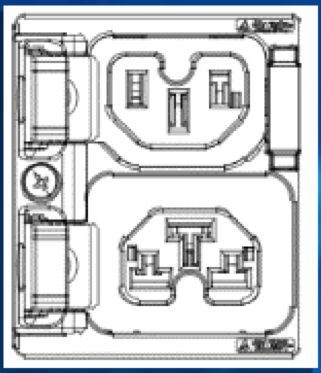
SKU and Serial Numbers

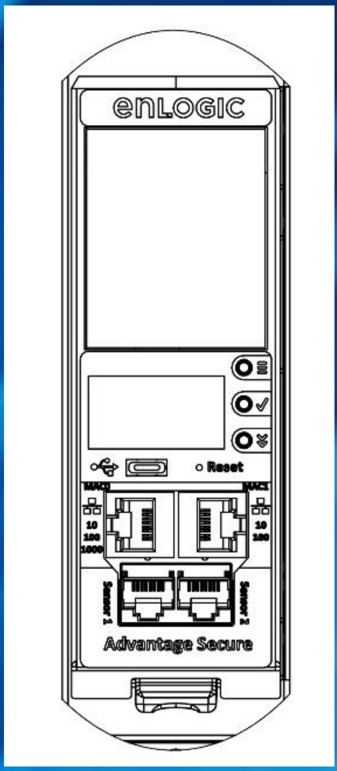


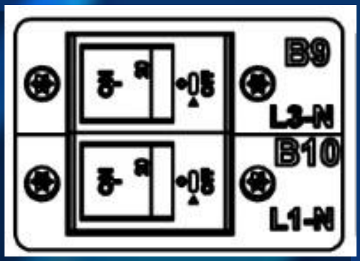
Regions Supported

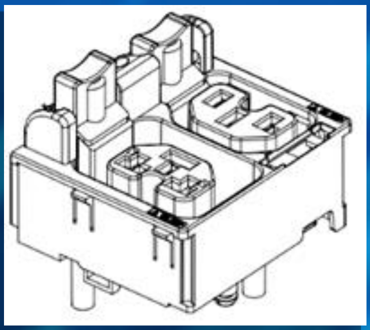
Follow all local and national codes, when installing the PDU. The PDU should be connected to a dedicated circuit protected by a branch circuit breaker matching the PDU input plug-type for your region:

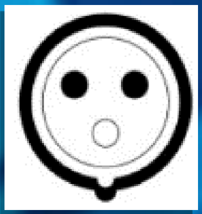
Regions	PDU Input Plug Type	Input Rating
Europe, International	IEC60320 C20 Inlet (Removable Power Cord)	16A SINGLE PHASE
	CEE 7/4, CEE 7/5, CEE 7/7 Plugs	16A SINGLE PHASE
	IEC60309 316P6 or 316P6W	16A SINGLE PHASE
	IEC60309 332P6 or 332P6W	32A SINGLE PHASE
	IEC60309 363P6 or 363P6W	32A SINGLE PHASE
	IEC60309 516P6 or 516P6W	16A THREE PHASE
	IEC60309 532P6 or 532P6W	32A THREE PHASE
	IEC60309 563P6 or 563P6W	63A THREE PHASE
	3-pin (2P+G)	20A SINGLE PHASE
Australia	3-pin (2P+G)	32A SINGLE PHASE
	5-pin (3P+N+G)	20A THREE PHASE
	5-pin (3P+N+G)	32A THREE PHASE
	IEC60320 C20 Inlet (Removable Power Cord)	20A SINGLE PHASE
	NEMA 5-20P or NEMA L5-20P	20A SINGLE PHASE
	NEMA 6-20P or NEMA L6-20P	20A SINGLE PHASE
	NEMA 6-30P or NEMA L6-30P	30A SINGLE PHASE
	NEMA 5-30P or NEMA L5-30P	30A SINGLE PHASE
North America/Japan	IEC60309 330P9 or 330P9W	30A SINGLE PHASE
	CS8265C	50A SINGLE PHASE
	NEMA L21-20P or NEMA L15-20P	20A THREE PHASE
	NEMA L21-30P or NEMA L15-30P	30A THREE PHASE
	CS8365C	50A THREE PHASE
	IEC60309 460P9 or 460P9W	60A THREE PHASE
	IEC60309 520P6 or 520P6W	20A THREE PHASE
	IEC60309 530P6 or 530P6W or NEMA L22-	30A THREE PHASE



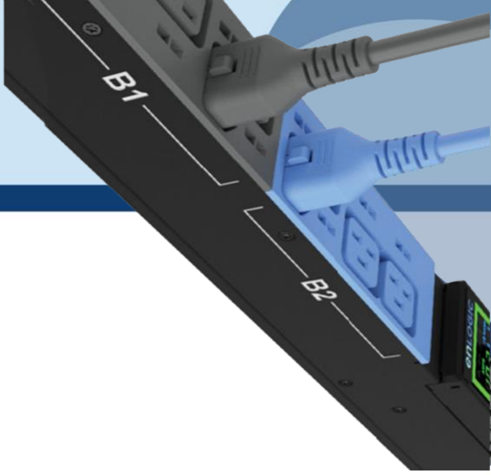








Product & Components



Product Description

The Advantage Secure PDU from Enlogic is a sleek and space saving unit with low profile circuit breakers, color-coded receptacles and different types of power outlets, which can be customized according to the user needs and IT requirements.

The PDU provides efficient and reliable power distribution capabilities, ensuring maximum uptime of IT equipment through intelligent features such as:

- Full featured network management and alerting capabilities supporting HTTP, HTTPS, SSH, SNMP, and email.
- Strong encryption, passwords, and advanced authorization options including local permissions, LDAP, and Active Directory.
- Daisy Chain up to 64 Rack PDUs and supports a maximum of 10 environmental sensors each.
- Power Sharing feature that allows the data of the PDU to be recorded even during a Power Failure.

The power distribution systems offered by the Advantage Secure from Enlogic are as follows:

Product Series	Inlet Power Measurement (Metered)	Outlet Power Measurement	Switchable Outlet
EN1000 Series	✓		
EN2000 Series	✓		✓
EN5000 Series	✓	✓	
EN6000 Series	✓	✓	✓
EZ1000 Series	✓		

Single-Phase Models

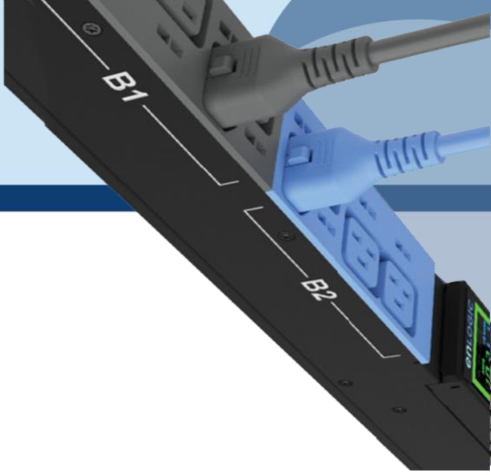
All Single-Phase models support hydraulic-magnetic breakers that are color coded to the corresponding outlets.

Three-Phase Models

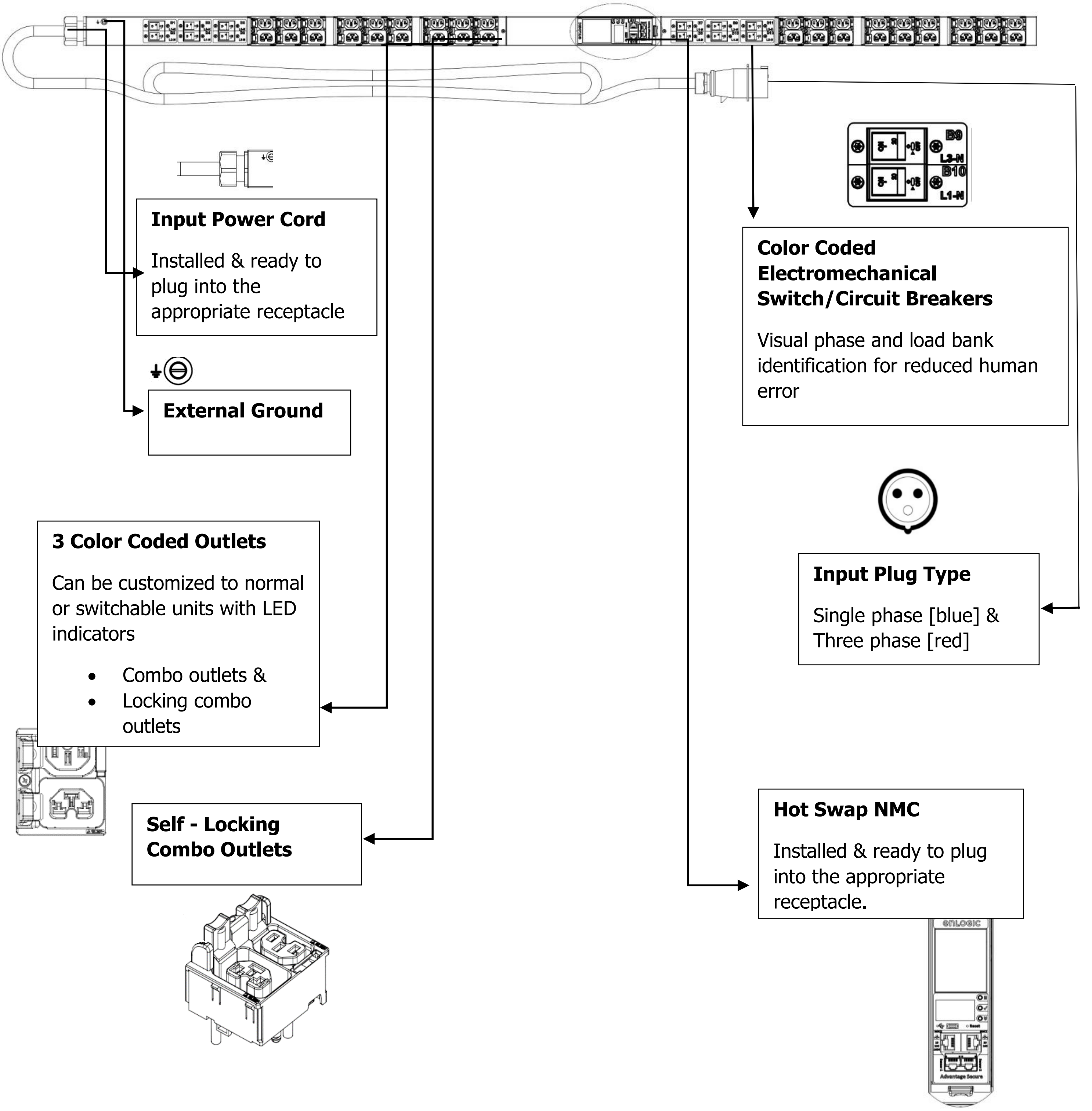
- In standard, 415 V Three-Phase (Wye) configurations, the color of each circuit breaker and outlet corresponds to the appropriate input phase. The PDU is labelled to indicate the input phase associated with each circuit breaker and outlets.

- In North America 208 V Three-phase (delta) configurations, the color of the circuit breaker corresponds to the line connections and includes a label of the two connected input-phases, (i.e., L1-L2, L2-L3, or L3-L1).

- All Three-Phase models rated above 20 A and 16 A, will also use an outlet indicator LED in color Green.



iPDU & its Components



Input Power Cord

Installed & ready to plug into the appropriate receptacle

External Ground

3 Color Coded Outlets

Can be customized to normal or switchable units with LED indicators

- Combo outlets &
- Locking combo outlets

Self - Locking Combo Outlets

Color Coded Electromechanical Switch/Circuit Breakers

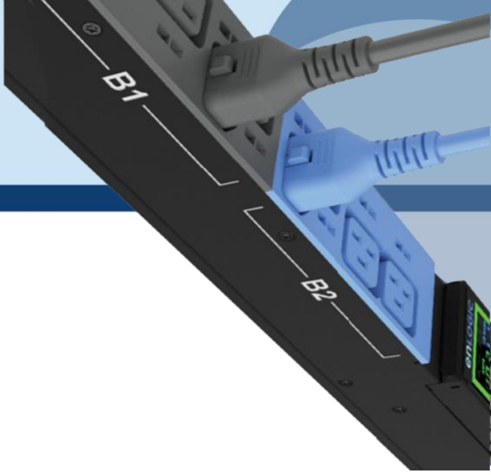
Visual phase and load bank identification for reduced human error

Input Plug Type

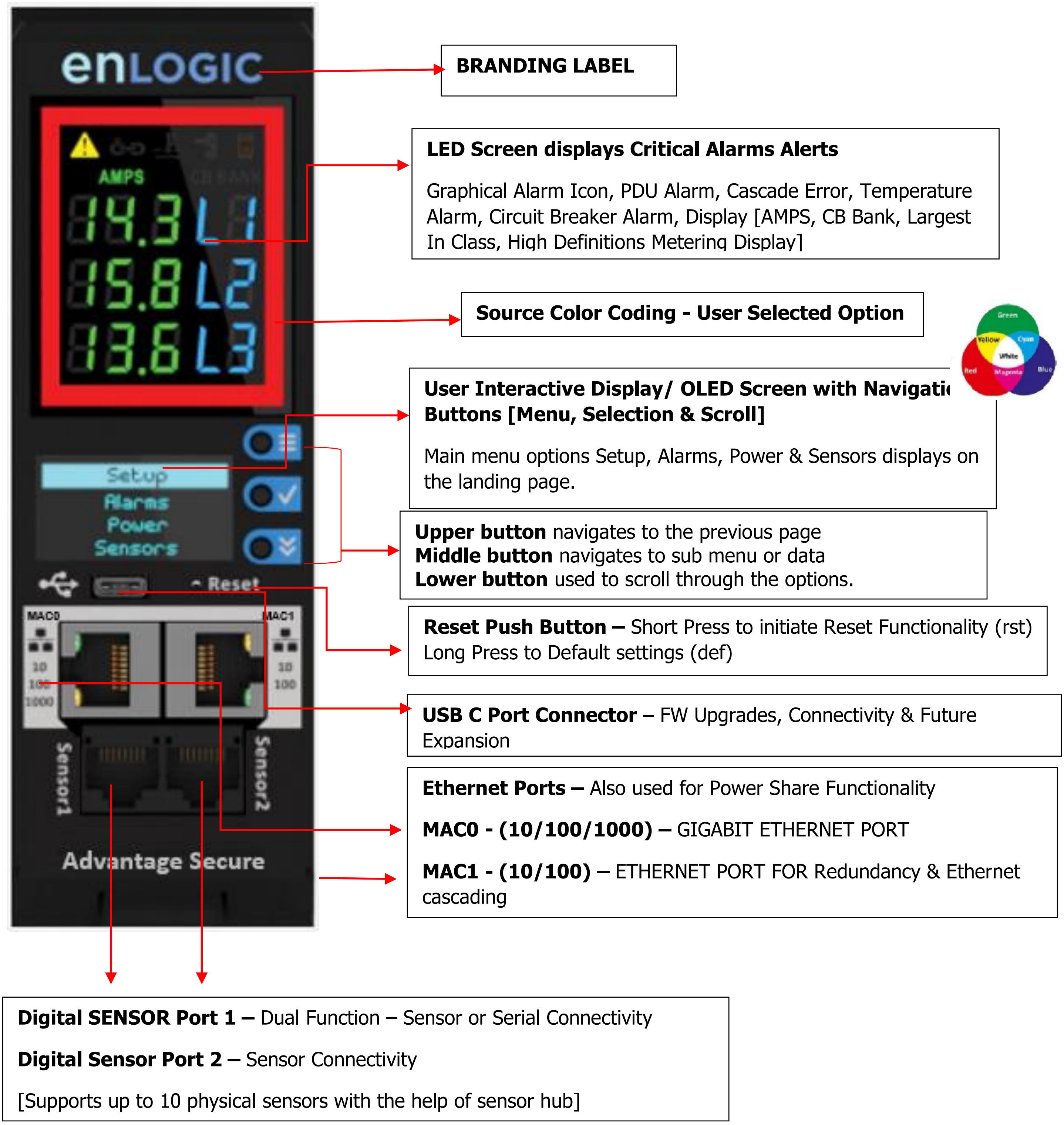
Single phase [blue] & Three phase [red]

Hot Swap NMC

Installed & ready to plug into the appropriate receptacle.



Product Components Network



BRANDING LABEL

LED Screen displays Critical Alarms Alerts

Graphical Alarm Icon, PDU Alarm, Cascade Error, Temperature Alarm, Circuit Breaker Alarm, Display [AMPS, CB Bank, Largest In Class, High Definitions Metering Display]

Source Color Coding - User Selected Option

User Interactive Display/ OLED Screen with Navigatio Buttons [Menu, Selection & Scroll]

Main menu options Setup, Alarms, Power & Sensors displays on the landing page.

Upper button navigates to the previous page
Middle button navigates to sub menu or data
Lower button used to scroll through the options.

Reset Push Button – Short Press to initiate Reset Functionality (rst)
Long Press to Default settings (def)

USB C Port Connector – FW Upgrades, Connectivity & Future Expansion

Ethernet Ports – Also used for Power Share Functionality

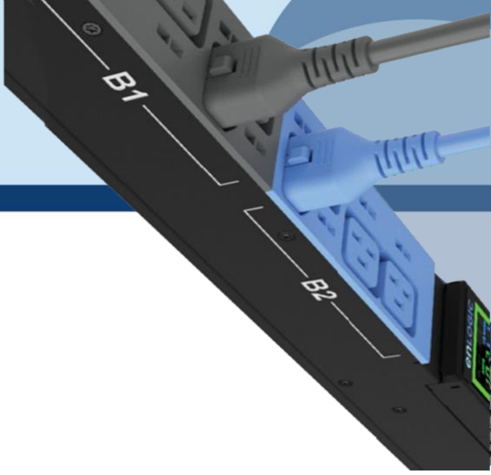
MAC0 - (10/100/1000) – GIGABIT ETHERNET PORT

MAC1 - (10/100) – ETHERNET PORT FOR Redundancy & Ethernet cascading

Digital SENSOR Port 1 – Dual Function – Sensor or Serial Connectivity

Digital Sensor Port 2 – Sensor Connectivity

[Supports up to 10 physical sensors with the help of sensor hub]



Displays

There are two displays on all standard Advantage Secure models, as specified below:

- The Seven Segment LED display shows data in high visibility at Phase Level and CB Level.
    - LED Graphical Alarm Icons: PDU Alarm, Cascade Error Alarm, Temperature Alarm, Security Handle Alarm, and Circuit Breaker Alarm.
    - Display (AMPS, CB BANK): Largest In-class HD Metering Display.
- The OLED screen will display a status bar, when the PDU operating system is loading.
    - OLED display: Set up, Alarms, Power, Sensors (click menu, select, and scroll to operate).

Interfaces

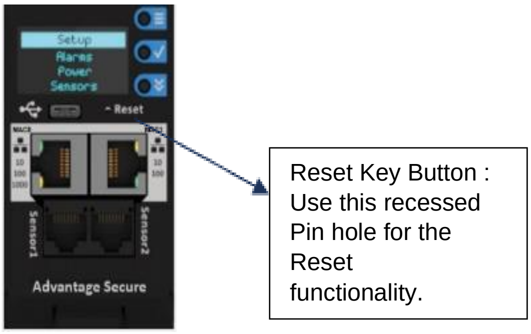
There are five interfaces on all standard Advantage Secure models, as specified below:

- USB-C: Fast Configuration, Fast upload of firmware and download log files.
- Ethernet Port 1: 1x Gigabit Ethernet (10/100/1000 Mbps) - Primary network port / Power Share.
- Ethernet Port 2: 1x (10/100 Mbps) - Daisy chain / Power Share / RNA / Network.
- Sensor-1: Primary Sensor Port / Serial Port –The Serial function is a user interface that enables the user to configure Features and update Firmware.
- Sensor-2: Secondary Sensor Port – This port also can connect the sensors.

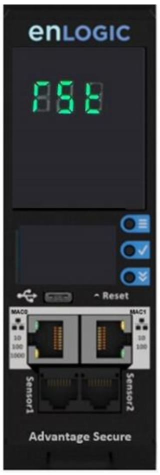
Note – *Overall, the sensor ports support connecting up to total 10 sensors with the help of the sensor hub.*

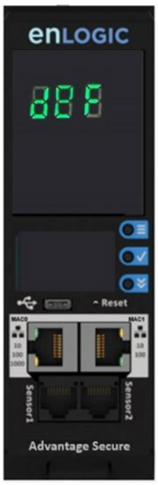
Reset Button

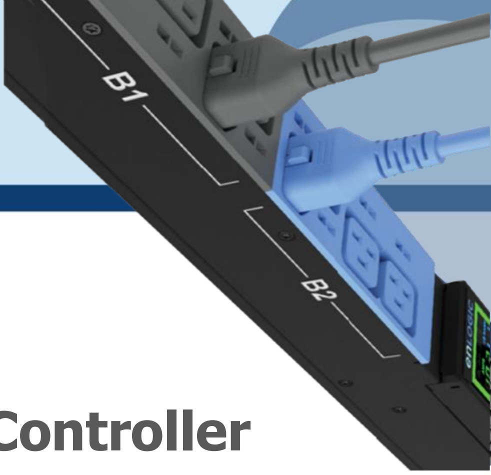
Outcome	Action
NMC Reboot **[RST]**	Use a pin, press, and hold the recessed RESET key button for about 8 seconds, which will initiate the reset option without changing any configuration values. The OLED display will show the **RST** during this operation.
NMC Reboot **[DEF]** To set it to default settings if user does not know the password	Use a pin, press, and hold the RESET key button for about 20 seconds, which will initiate the **DEF** option in the LED display. This action initiates the NMC to reset to the factory default settings.
NMC Quick/Forced Restart	Use the pin, press, and hold the RESET key button along the scroll button simultaneously. This action initiates a quick/forced NMC restart.



Reset Key Button : Use this recessed Pin hole for the Reset functionality.







Advanced Network Management Controller (NMC) Network Security

Enlogic iPDUs and in-line meters are equipped with:

- The latest network security protocols (secured by encryption algorithms).
- The latest support for remote authentication (Active Directory, LDAP & RADIUS) and
- Aggressive USER Login and Password Policies.

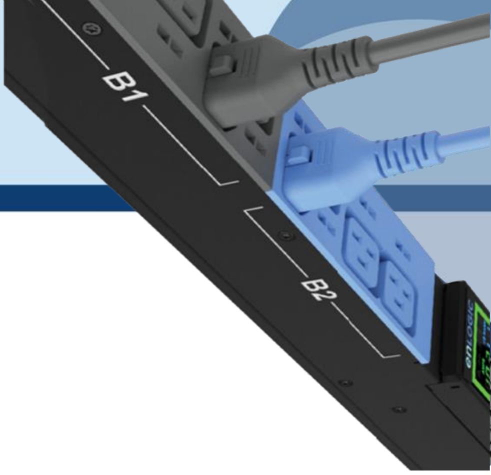
The Firmware updates are released on a quarterly basis, to ensure that Enlogic iPDUs will always provide the highest-level network security, which protects against attacks in high-risk environments.

Encryption

Communication Protocol	Supported Encryption
HTTP/HTTPS/REDFISH API	TLS 1.2 2048 key length supported
SNMPv2c/v3	SNMPv2c Encryption: Based on community string SNMPv3 Authentication: MD5, SHA, Privacy: AES128, AES192, AES256
SSH	TCP/IP SSL Support for user-defined ports Up to 16 SSH user sessions at the same time
FTP/FTPS	File Transport Protocol (FTP) File Transport Protocol Secure (FTPS) (TLS1.2 encryption)
Active Directory, Open LDAP, and RADIUS	Privilege assignment over Active Directory, LDAP, and RADIUS

Remote Authentication

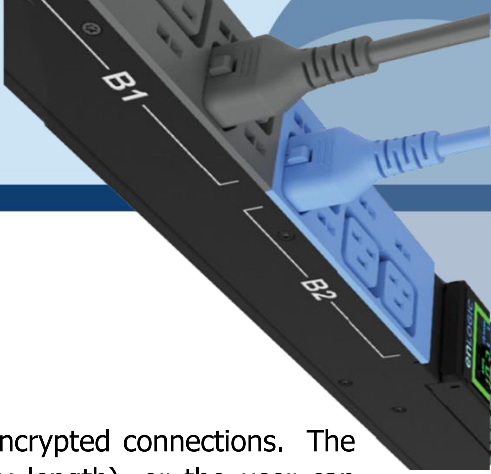
Authentication Protocol	Supported
Active Directory	YES Supported
Open LDAP	YES Supported
RADIUS	YES Supported



Login & Password Policy

Security Tools	Supported
Strong Password	Supports case sensitive alphanumeric and symbols
Creating Password Exceptions	Supports ASCII 33 to 47 only. Refer the table below for supported alphanumeric and symbols
Minimum password length	Passwords must be greater than eight characters
Forced password change on first login	User must assign an 8-32 character password at first login
User blocking after failed attempts	User definable number of attempts
Password Aging Interval	1-to-365-days expiration, or set it to 'never expire'
User Lockout Time	Specifies the duration time of lockout the user experiences before logging in again after the failed attempts
Automatic Idle Out	User definable idle out timer

Password Exceptions	Supported
For Creating Passwords - Supported character set from ASCII 33 to 47	Supports case sensitive alphanumeric and symbols ! 33 exclamation mark " 34 quotation mark # 35 number sign $ 36 dollar sign % 37 percent sign & 38 ampersand ' 39 apostrophe (40 left parenthesis) 41 right parenthesis * 42 asterisk + 43 plus sign , 44 comma - 45 hyphen . 46 period / 47 slash



Certificates

Enlogic iPDUs supports X.509 PEM digital certificates to create secure encrypted connections. The device is loaded with built-in default SSL certificate (1024 or 2048 key length), or the user can choose created SSL certificates. Key lengths supported are 1024 or 2048 bit.

Firmware and Conf file Encryption

Secure Encryption Design is adopted for files used to configure iPDU.

Firmware File

- enlogic.fw is a secured firmware file.
- The below mentioned attributes makes enlogic.fw secure:
    - Supports Secure Boot.
    - Supports Chain of Trust.
    - Support Firmware file signature.
    - Encrypted using AES256.

File	Encryption
Checksum	SHA256
Encryption Algorithm	AES256
Chain of Trust	AES192, AES256, RSA4096, SHA256
Signature Algorithm	ECDSA, SHA256

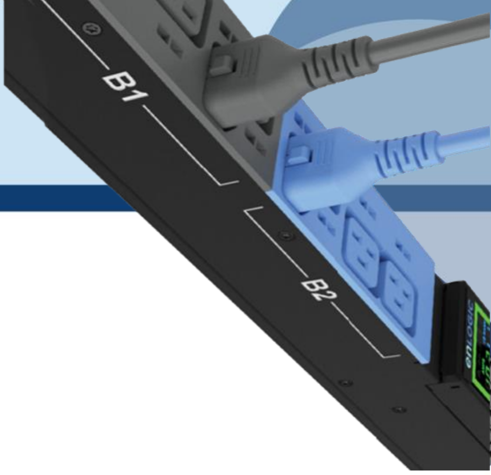
Chain of Trust Firmware Signature

Validation:

- File tampering is rejected from firmware to overcome Denial of Service (DoS).
- With strong algorithm check process, foreign file penetration into firmware application is avoided.

Secure Boot

Secure Boot makes sure that a device boots using only software that is trusted.



Conf File

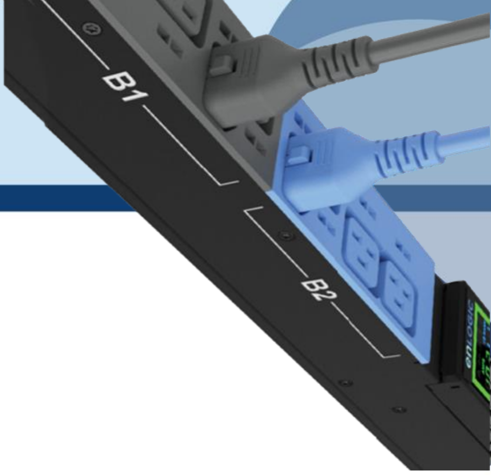
- CONF File downloaded is encrypted using AES256.
- EEPROM version validation is added to make sure NMC gets exact conf file.

File	Encryption
Encryption	AES256
Checksum	SHA256

Other Vulnerabilities:

Following vulnerabilities are avoided in firmware:

- **WEBSERVER – Weak Ciphers**
    - Weak Ciphers are removed from TLS Support.
- **WEBSERVER – Privilege Escalation & Improper Authentication**
    - Unique Role and ID is assigned to each user.
- **WEBSERVER – Click Jacking**
    - X-Frame option request header is added.
- **UNUSED Ports**
    - All unused ports in firmware are closed.
    - Ports used for internal use will not be accepting any external requests.



Network Security Hardening Guide

This section provides recommendations for hardening the security of products that connects to the network using an Advanced Network Management Controller (NMC).

Recommendations

To ensure that the product has the latest security enhancements and features available, verify that it is running the latest firmware version. Visit the Enlogic website at: *https://Enlogic.com/firmware-software/firmware* to find the latest firmware for your device.

Disable all unused protocols

If a protocol is not in use, ensure it is disabled to reduce your threat surface. This applies to protocols such as HTTP, HTTPS, SSH, SMTP, FTP, FTPS, etc.

Use custom network ports where applicable

If a non-standard port is in use, the device may not be detected by scans, which verify only standard ports. This applies to protocols such as HTTP, HTTPS, SSH, SMTP, FTP, FTPS, etc.

Disable HTTP and enable HTTPS for web support

To use secure and encrypted web protocol, disable HTTP and enable HTTPS. By default, HTTP is disabled on Network Management Controller-enabled products.

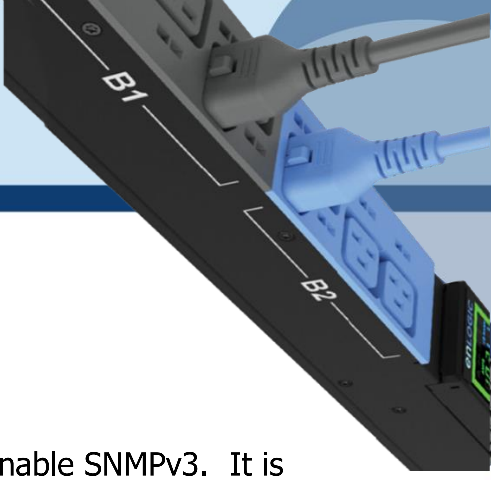
Disable older versions of TLS

Transport Layer Security (TLS) is a cryptographic protocol that provides communication security over the internet. Ensure that older versions of TLS are disabled on your Network Management Controller-enabled device and use the latest version available. PDU latest firmware supports ONLY TLS 1.2

Disable FTPS

For secure, encrypted file transfer protocol, enable FTPS if it is disabled. When FTPS is not in use, disable it to help harden security on your device. By default, PDU firmware supports data communication over TLS1.2.

Note: *If FTP login data is sent over plain text (not secured) from computer FTP client to the PDU FTPS server, the PDU authentication server will close the connection with error code 421.*



Disable SNMPv1 and enable SNMPv3

For encrypted SNMP protocol, disable SNMPv1 if it is enabled and enable SNMPv3. It is recommended to use SNMPv3 as it is more secure than SNMPv1. By default, SNMPv1 is Enabled and SNMPv3 is disabled.

Note: When SNMPv1 is not in use, it is recommended to disable SNMPv1.

Configure SNMPv3 to use AES/SHA

Configure SNMPv3 to use the most secure algorithms, AES, and SHA, to provide encryption and authentication.

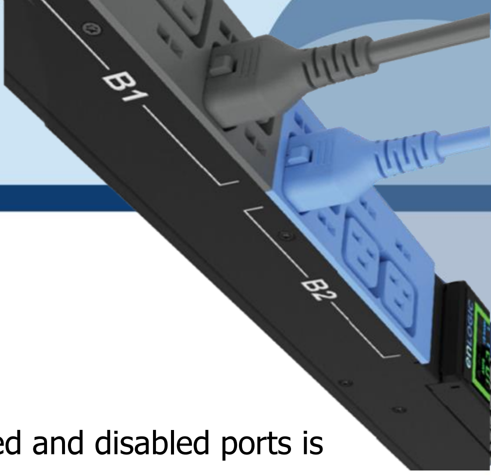
Change the admin User account password

After installation and initial configuration of your Network Management Controller-enabled device, immediately change the default admin user account password.

Note: You will be prompted to change the admin password at first login to the NMC.

Enable Strong Passwords

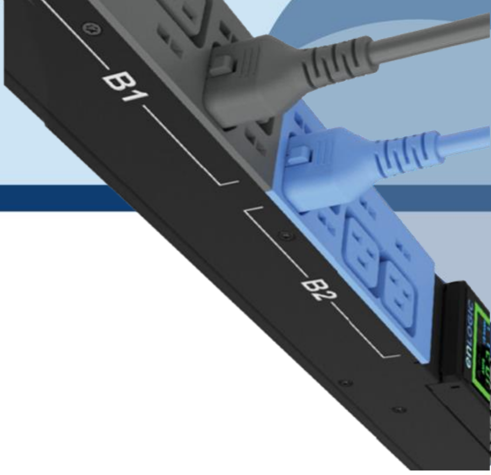
Enable this feature to ensure strong passwords are created. All passwords will be required to be a minimum length and contain special characters to make passwords harder to guess.



Default Ports

Following are the default ports the NMC supports. The list of enabled and disabled ports is also mentioned below:

Default Enabled Ports	
Port Number	Protocol
port 21	FTP over TLS1.2
port 22	SSH
port 443	HTTPS
port 8001	Cascade Function – Not accessible on Network
port 161	SNMP
Default Disabled Ports	
port 80	HTTP
port 162	SNMP Traps
port 514	SYSLOG
port 389	LDAP
port 25	SMTP



Seven Segment LED Display

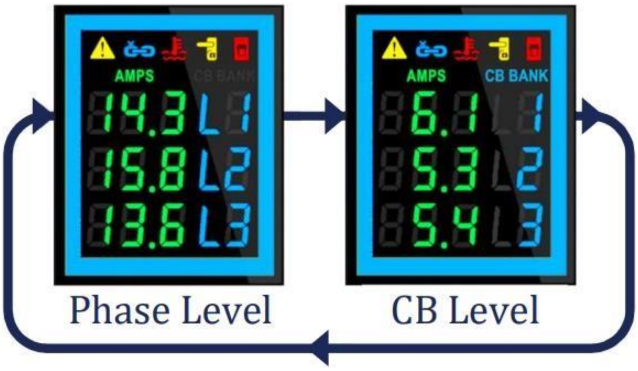
The Seven Segment LED display shows data in high visibility at Phase Level and CB Level.

- **Phase Level**

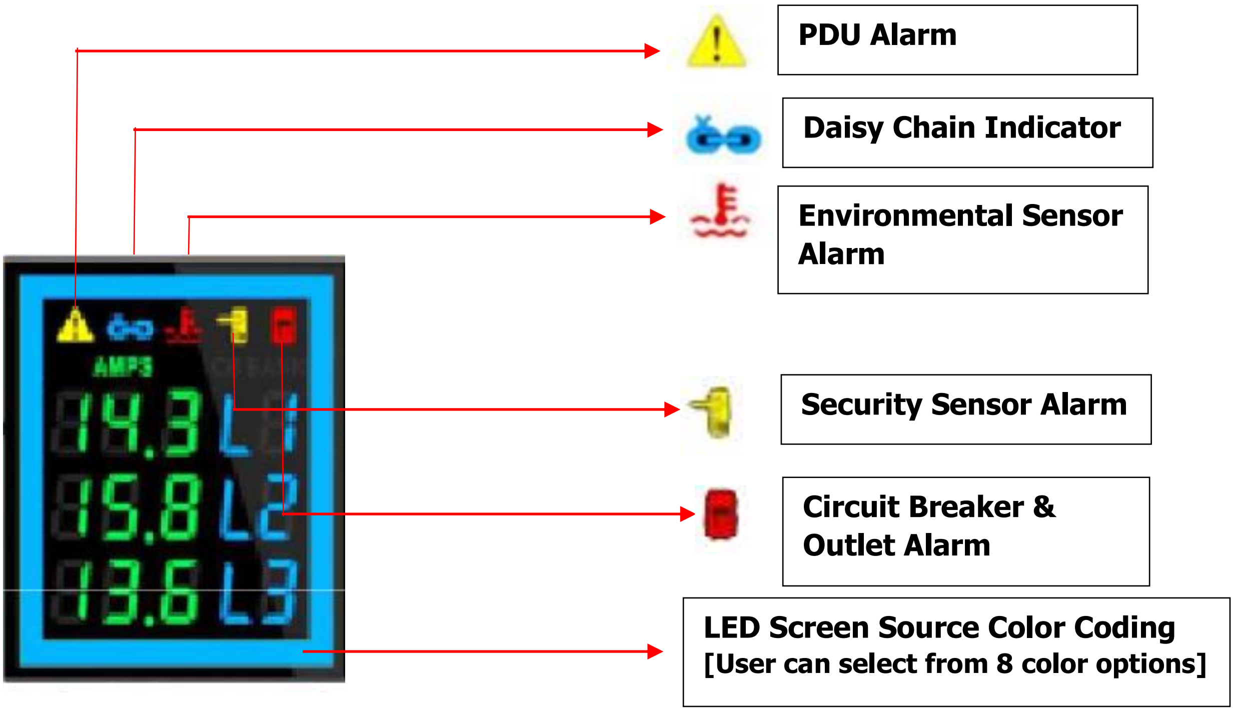
In this level information about the Current Input at each respective line, L1, L2 and L3.

- **CB Level**

In this level information about the Current Input at each respective Circuit breaker, 1, 2 and 3.



Indicators and Alarms shown on the Seven Segment LED display



PDU Alarm

Daisy Chain Indicator

Environmental Sensor Alarm

Security Sensor Alarm

Circuit Breaker & Outlet Alarm

LED Screen Source Color Coding [User can select from 8 color options]

1. **PDU Alarm -** It shows the user when a Critical Alarms or Warning Alarms occurs in a PDU. Displays the Active Power Alarms, Voltage, Current Unit Power, Frequency, Power Share.
2. **Daisy Chain Indicator -** It displays for about 30 mins if the Daisy Chain connection is disconnected. PDU becomes standalone.
3. **Environmental Sensor Alarm -** It shows the user if there is an alarm related to the environmental sensors. Displays the Temperature sensor, Humidity sensor, Rope sensor, and Dry sensor.
4. **Circuit Breaker & Outlet Alarm -** It shows the user if there is an alarm related to the circuit breaker. Displays the Outlet Alarms and CB Alarms.
5. **Security Sensor Alarm -** It shows the user if there is an alarm related to the door sensors.
6. **LED Source Color coding-** The user can choose from a list of eight LED screen color options.

OLED Display and Network Management Controller (NMC)

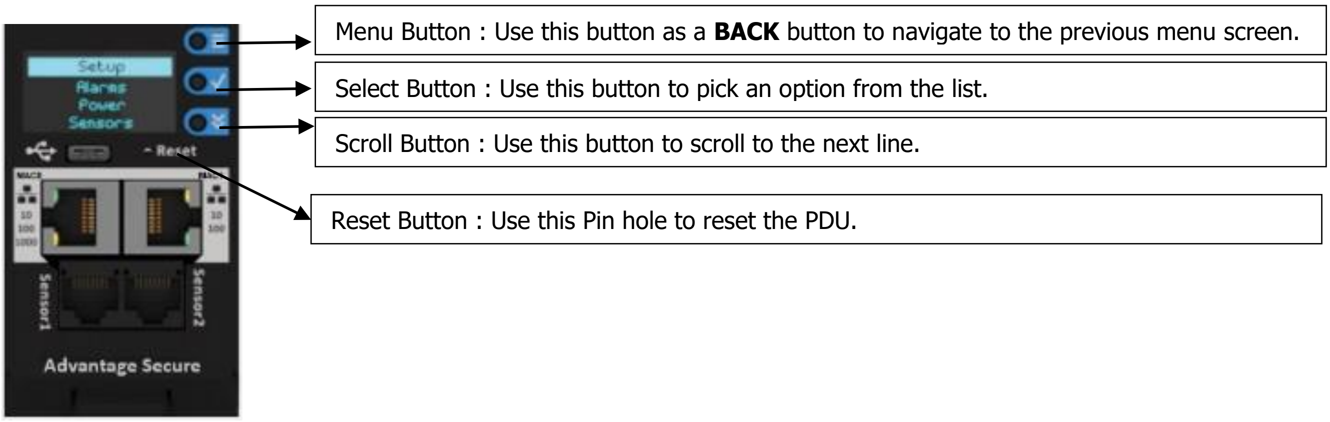
The Onboard Display provides information about the PDU and connected devices. The Network Management Controller (NMC) of the PDU has a three-button. Use the buttons to change the screen display and retrieve specific data.

OLED Navigation

☰ → Press on the **Menu** button to access the OLED **Main Menu** or previous **Submenu**.

≫ → Press on the **Scroll** button to navigate through the options.

✓ → Press on the **Select** button to choose the option.



Menu Button : Use this button as a **BACK** button to navigate to the previous menu screen.

Select Button : Use this button to pick an option from the list.

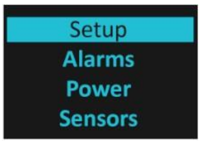
Scroll Button : Use this button to scroll to the next line.

Reset Button : Use this Pin hole to reset the PDU.

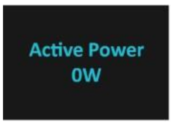
Note: *The highlighted menu item is ready to be selected.*

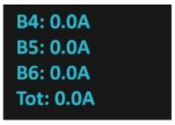
The Network Controller Display has three modes:

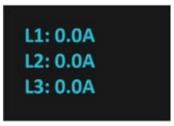
1. **Menu mode:** (Network Controller Display main menu): When the PDU is powered up or when a button is pushed while in Standby Mode or Power Save mode.

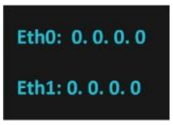


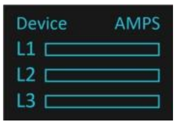
2. **Standby mode**: This happens when a PDU is idle (no buttons pushed) for 2 minutes while in Menu mode. The following screen savers with the respective data comes into view.


Active Power
0W


B4: 0.0A
B5: 0.0A
B6: 0.0A
Tot: 0.0A


L1: 0.0A
L2: 0.0A
L3: 0.0A

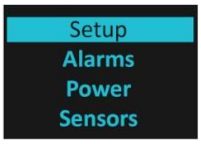

Eth0: 0. 0. 0. 0
Eth1: 0. 0. 0. 0



3. **Power Save mode:** The PDU enters Power Save mode when it has been in Standby mode for 30 minutes. The screen is switched off to save power. To exit Power Save mode, press any button on the display.

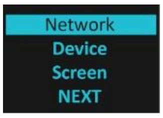
Main Menu Selections

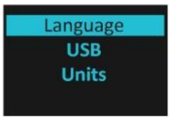
The PDU menu selection hierarchy consists of Setup, Alarms, Power, and Sensors. On the main menu, scroll down to highlight **Setup**. Press **Select**. Scroll down to select a submenu and press **Select** to display the submenu options. Press **Menu** to return to the previous menu.



Setup Menu

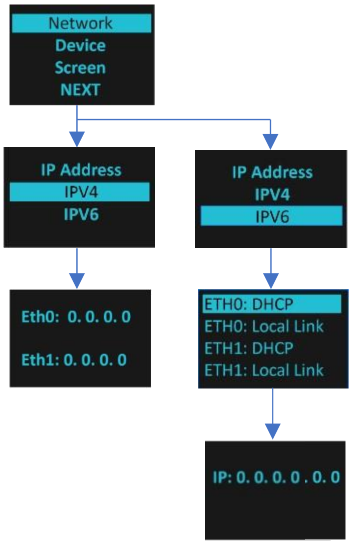
The **Setup** menu provides user configuration options including Network, Device, Screen, Language, USB, and Units.





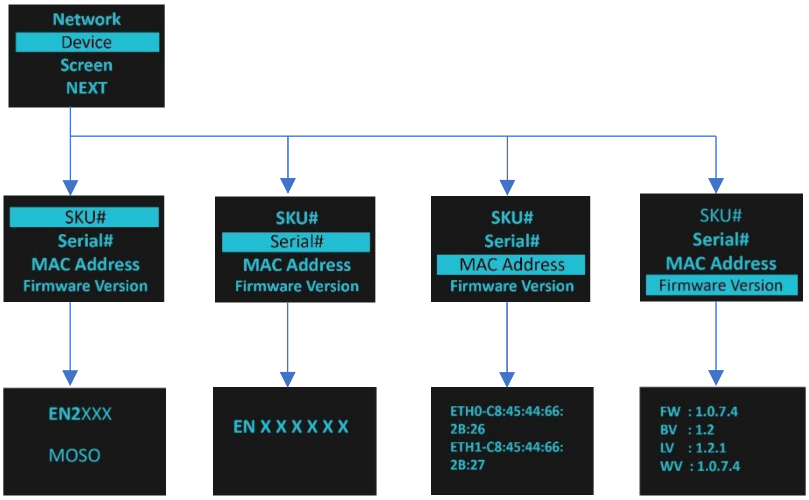
Network Submenu

The **Network** submenu allows you to view IP address IPv4 or IPv6. On the **Setup** menu, scroll down to Network. Press **Select** to enter the Network Submenu. Scroll down to highlight the selected option from the menu. Press **Select** to display the screens that display the IP address. Press **Menu** to return to the previous menu.



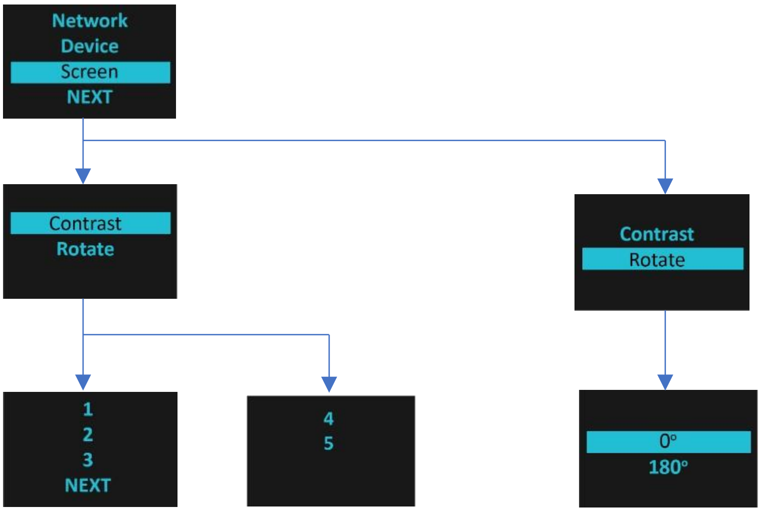
Device Submenu

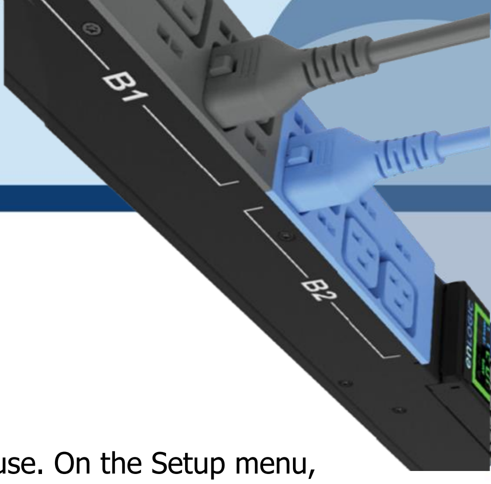
The **Device** submenu provides the SKU number, Serial number, MAC address and Firmware version. On the **Setup** menu, scroll down to highlight **Device** submenu. Press **Select** to enter the **Device** Submenu. Scroll down to the item you wish to display, and press **Select**. Press **Menu** to return to the previous menu.



Screen Submenu

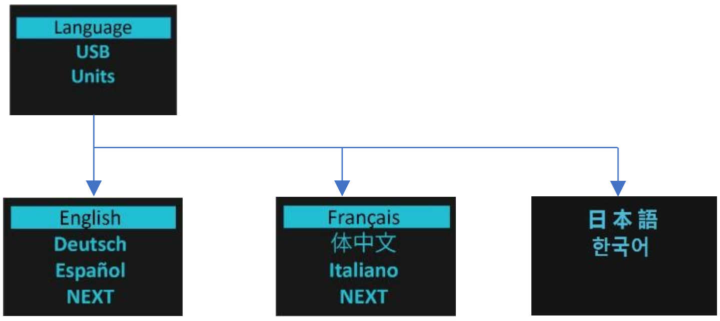
The **Screen** submenu allows you to customize settings for Contrast and Rotate. In the **Setup** menu, scroll down to highlight Screen. Press **Select** to select the submenu. Press **Menu** to return to the previous menu.





Language Submenu

The **Language** submenu allows you to select the language you need to use. On the Setup menu, scroll down to highlight Language. Press Select to display the screens to select the submenu. After you select the values, press Select to set the values as displayed on the screen. Press Menu to return to the previous menu.

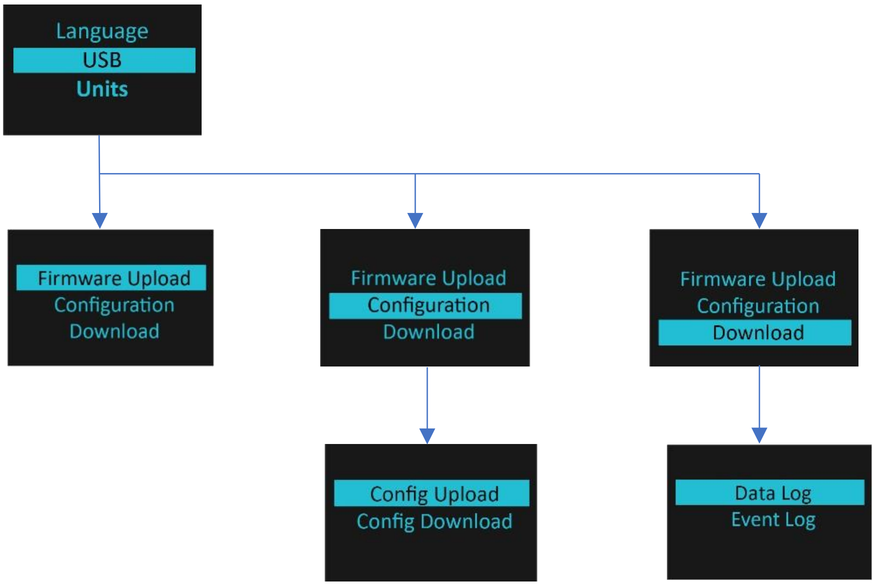


USB Submenu

The **USB** submenu allows you to upload firmware file, upload configuration file and download event log or data log.

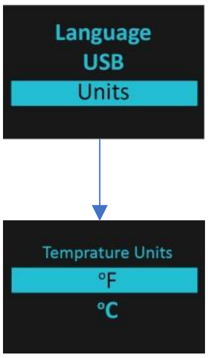
On the **Setup** menu, scroll down to highlight USB. Press **Select** to enter the **USB** Submenu. The user can select the Operation and Mode to proceed further.

***Note**: If a USB drive is not present in the USB slot the PDU will enter normal operation.*



Units Submenu

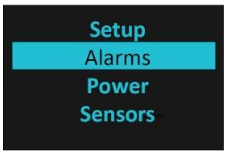
The **Units** submenu displays the temperature units. On the **Setup** menu, scroll down to highlight Units. Press **Select** to enter the **Units** Submenu. After you select the values, press **Select** to set the values as displayed on the screen. Press **Menu** to return to the previous menu.



***Note**: This can only be done locally at the PDU and also using the WEBUI.*

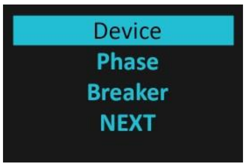
Alarms Menu

The **Alarms** menu displays active alarms for the PDU. On the **Main** Menu, scroll down to highlight **Alarms**. Press **Select** to display the **Alarm** Screen. When you finish your review, press **Menu** to return to the main menu.

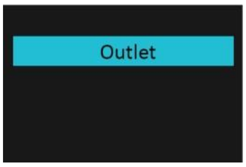


Power Menu

The **Power** menu manages Device, Phase, Breaker, and Outlet. On the **Main** Menu, scroll down to highlight **Power**. Press **Select**. Scroll down to select a submenu and press **Select** to display the submenu options. Press **Menu** to return to the previous menu.



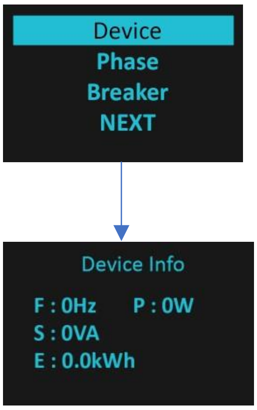
Device
Phase
Breaker
NEXT



Outlet

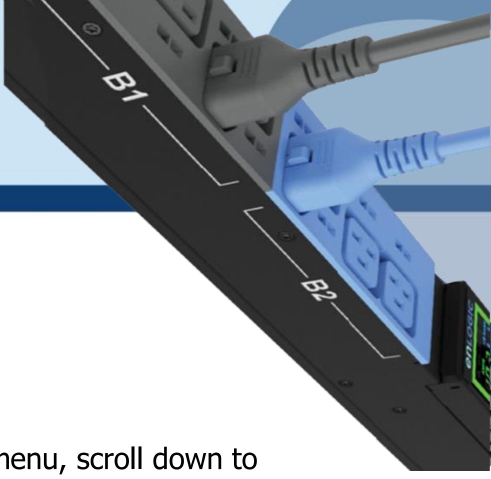
Device Submenu

The **Device** submenu is to Display Current, Voltage and Power. On the **Power** menu, scroll down to highlight **Device**. Press **Select** to display the power values for the entire PDU. Press **Menu** to return to the previous menu.



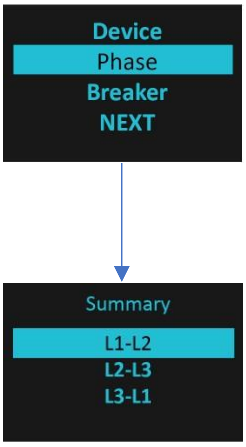
Device
Phase
Breaker
NEXT

Device Info
F : 0Hz P : 0W
S : 0VA
E : 0.0kWh



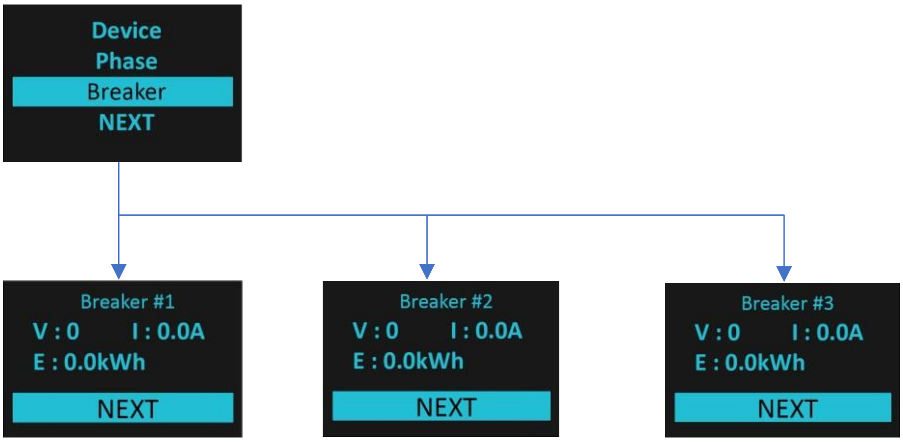
Phase Submenu

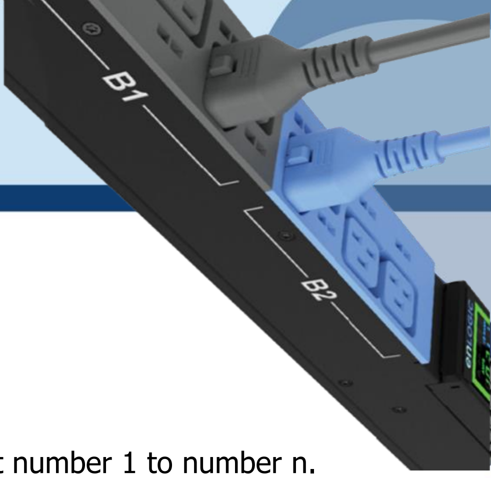
The **Phase** submenu is to display the status of 3-Phase. On the **Power** menu, scroll down to highlight Phase. Press **Select** to display the screens to set the values for the submenu. After you select the phase, press **Select** to display the values for that phase on the screen. Press **Menu** to return to the previous menu.



Breaker Submenu

The **Breaker** submenu is to display power values for the breakers. Press **Select** to display the values of the first breaker. To go to the next breaker, Select **Next**. Press **Menu** to return to the previous menu.

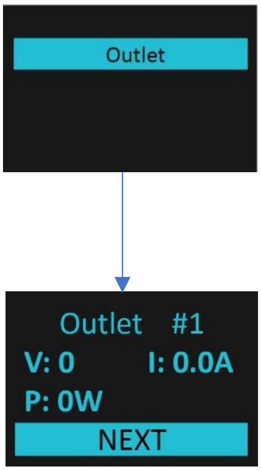




Outlet Submenu

The **Outlet** submenu is to display voltage, current and power from outlet number 1 to number n. On the **Power** menu, scroll down to highlight **Outlet**. Press **Select** to display values for the first outlet. To go to the next outlet, **Select** next. Press **Menu** to return to the previous menu.

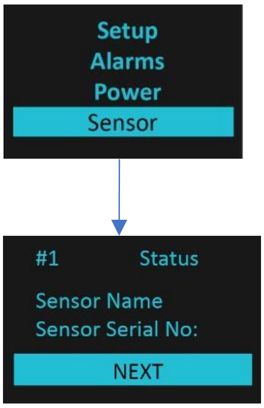
***Note**: Custom outlet names noted in the Web GUI do not make changes to the local display. This is done to make it easier to map to outlet numbers which can locally be seen on the outlets themselves.*

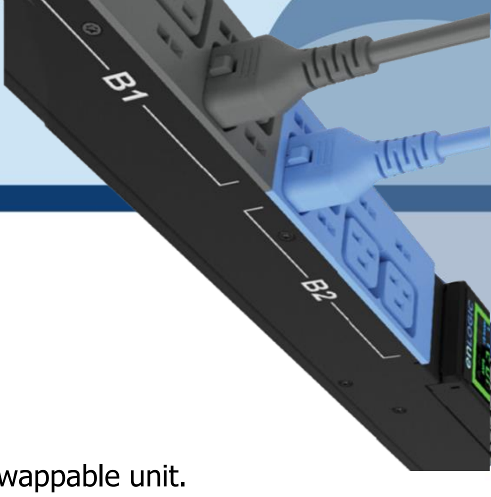


Sensors Menu

The Sensor menu is to display temperature, humidity, door switch, fluid leak etc. On the Main Menu, scroll down to highlight Sensor. Press Select. This will display the sensor data for the first sensor. To go to the next sensor, Select next. Press Menu to return to the previous menu.

***Note**: Maximum of ten sensors are configured per PDU.*





NMC Hot Swap

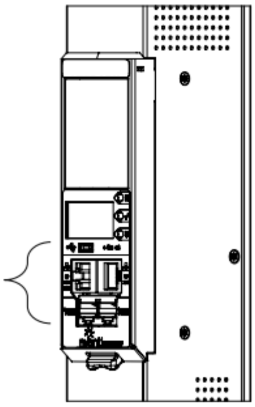
The Network Management Controller (NMC) for a vertical iPDU, is a hot-swappable unit.

Ribbon Cable

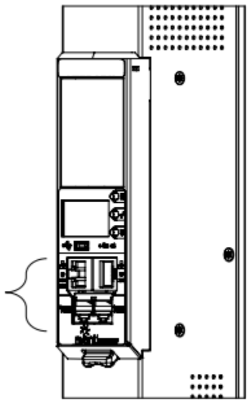
Installation

Disconnect the NMC

1. Write down the details of the ports and the RJ45 plugs connected, this will enable reconnecting them after installing the replacement NMC.



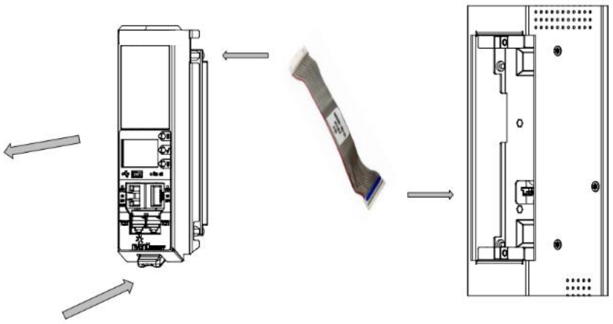
2. Remove all the connectors from the ports of the existing NMC (Ethernet, Serial, Sensor, etc.).



3. Push the bottom snap lock button **UP**. Gently pull the NMC to unmount, without disconnecting the Ribbon cable. The Ribbon cable can be extended only to a comfortable length, care should be taken to avoid any damages to the Ribbon cable.

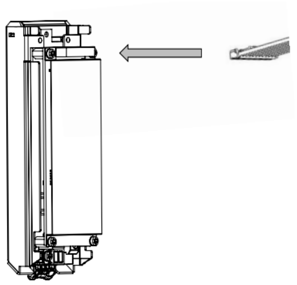
   Note - *Do not disconnect the Ribbon cable from the PDU back board.*

4. Only, in case of damages to the existing Ribbon cable, replace it with the new Ribbon cable provided in the box package. Then, detach the Ribbon cable from the PDU back board also and then re-plug it.



Installing the new NMC

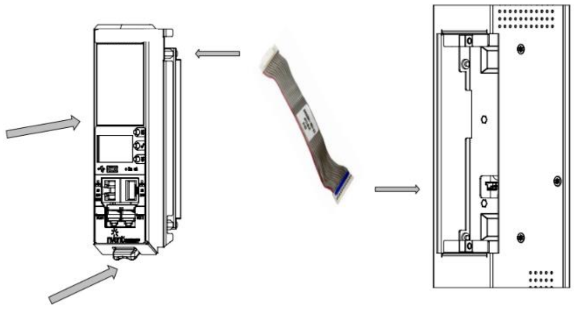
5. Plug the Ribbon cable into the connecting socket on the top section of the replacement NMC. Gently fold the Ribbon cable. Mount the NMC back into the PDU chassis.

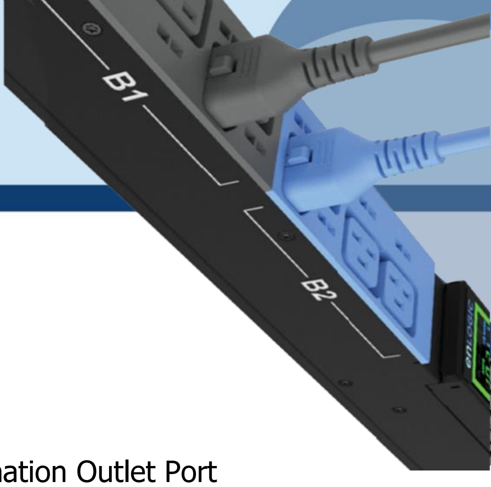


6. Align the NMC and connect the Ribbon cable back to the PDU back board. Now, slide the top flange to align in the slot. Push the bottom snap lock button **UP** and gently fix the NMC into the PDU chassis.

   Note - *Do not strain or kink any of the wires in the Ribbon cable.*

7. Verify if replaced NMC is powered **ON**.
8. The replacement NMC is mounted on the PDU chassis.



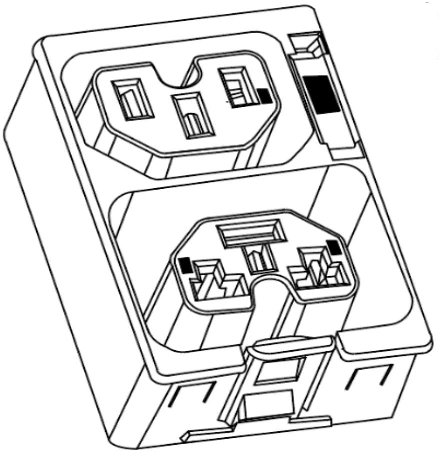


Outlet Units

Combo Outlets

The Advantage Secure PDU features a C13/C15 and C13/C15/C19 combination Outlet Port configuration, which increases the adaptability.

This helps the user to get the highest level of versatility allowing the connection of both ICE C14 and C16 plugs into the same C13/C15 (2-in-1) combination Outlet Port and ICE C14, C16 and C20 plugs into the same C13/ C15/C19 (3-in-1) combination Outlet Port.



Combo Outlet

C13/C15 [2 in 1] Outlet

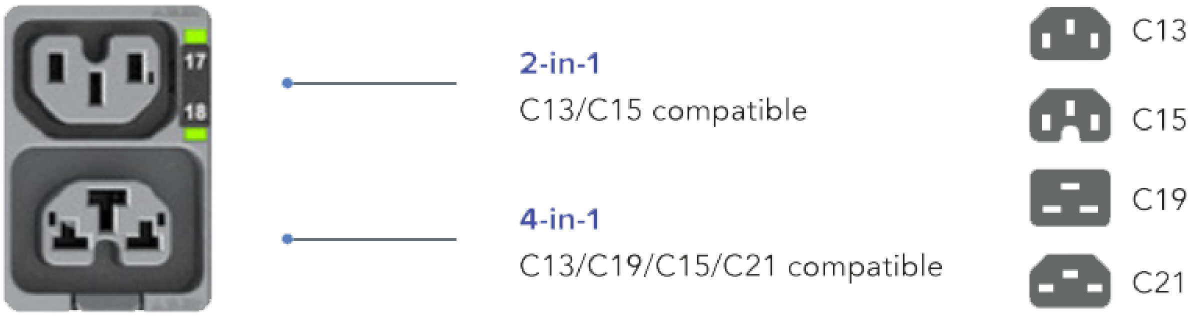
NAM & EAU 10 A / 250 V

C13/C15/C19 [3-in-1] Outlet

NAM & EAU 16 A / 250 V

New 4 in 1 Combination Outlets – Flexible & Future Proof

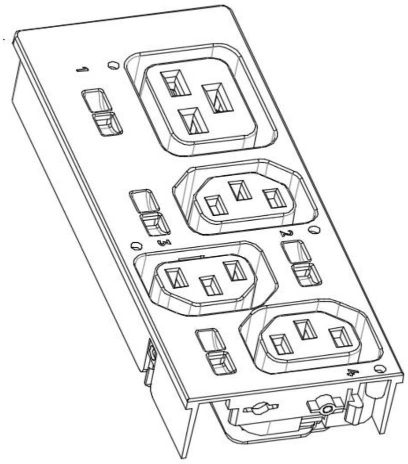
The Advantage Secure PDU features C13/C15 and C19/21 combinations 4 in1 Combo Outlet Port configurations.



Apollo Outlet

The Advantage Secure PDU features a C13 and C19 combination discreet

Outlet Port configurations. The specifications of the Outlet Unit are as follows:



Apollo Outlet

C13 Outlet

NAM & EAU 10A / 250V

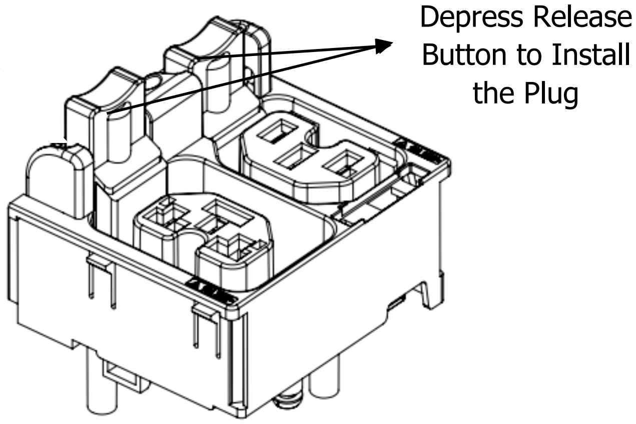
C19 Outlet

NAM & EAU 16A / 250V

- Degree of protection by enclosure according to IEC60529 is IP20.
- Mating plug inserting force is 70 N max.
- Mechanical operation cycles without load are 1000 cycles and with load is 500 cycles.
- Temperature range: 25 °C – 100 °C.
- Rated impulse voltage: 2.5 kV.

Self- Locking Combo Outlet

The Advantage Secure PDU features C13/C15 and C13/C15/C19 combination Locking Outlet Port configurations.



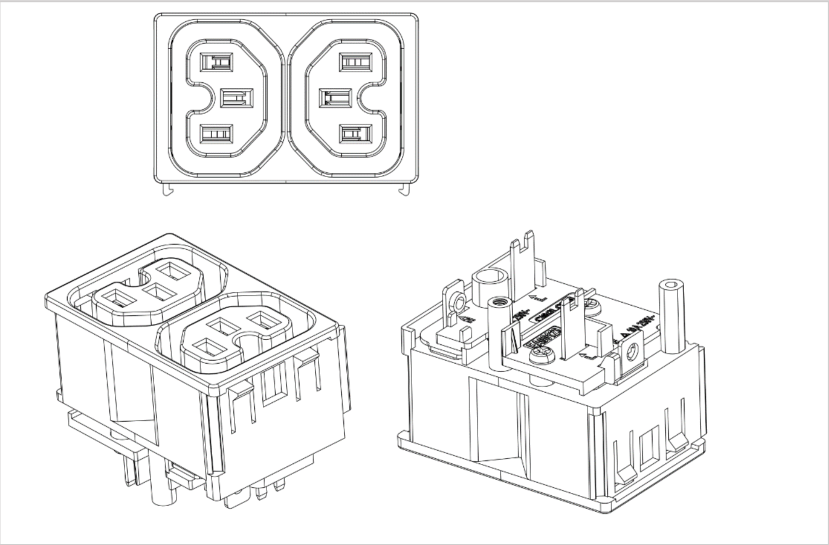
Locking Combo Outlet port features both the Combo Outlet C13/C15 [2 in 1] Outlet NAM & EAU 10 A / 250 V and C13/C15/C19 [3-in-1] Outlet NAM & EAU 16 A / 250 V with an additional locking port facility.

The specifications of these Locking Combo Outlet Units are :

- The release button must be fully pressed [depress it] prior to installing the plug.
- Both type of plugs with and without locking clips can be inserted.
- The plugs can be installed just by pushing into the outlets directly without depressing release button.
- To unlock, fully depress release button and remove plug.

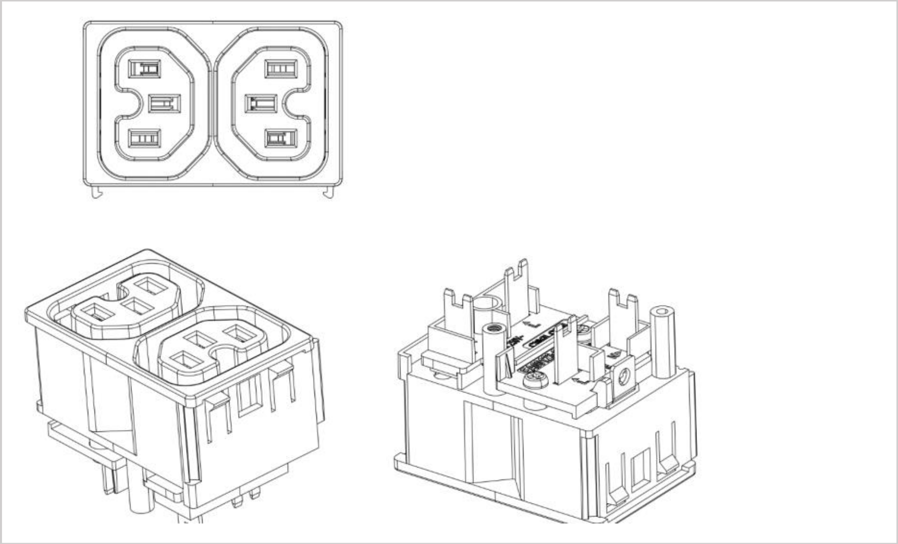
Newly Launched Outlets & Variants

The Advantage Secure PDU features a new range of individual and combination Regular/Locking Outlet Port configurations.



Outlet 2xC13 Combo

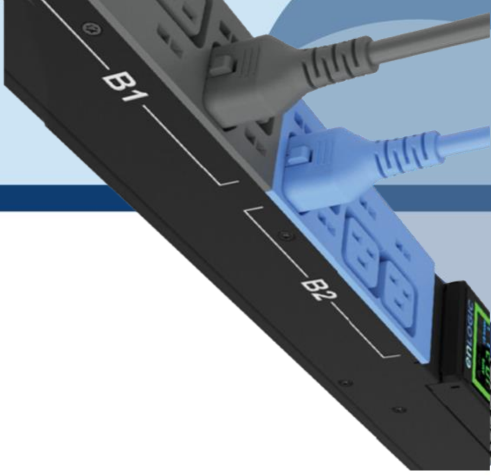
12 A / 250 V

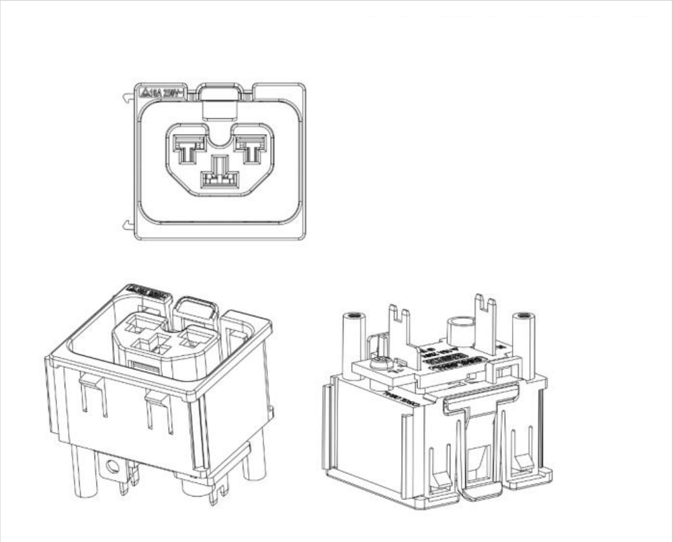


Outlet 2xC13 Combo

12 A / 250 V

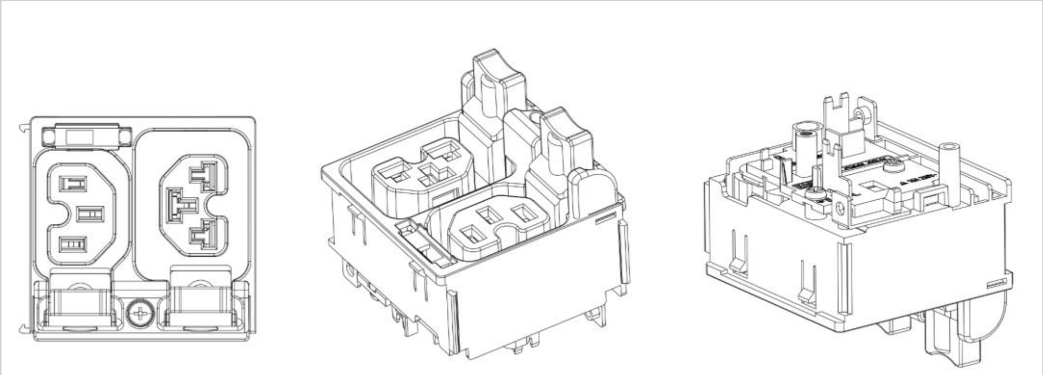
Each Outlet can be monitored independently





Outlet 1xC19 Combo

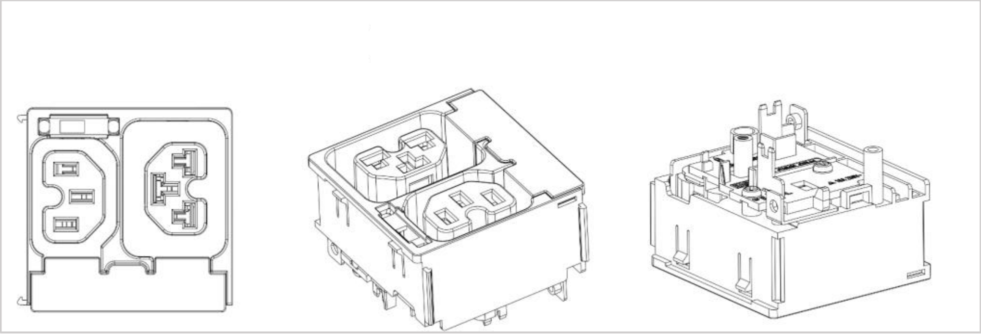
16 A / 250 V



Outlet C13/ C19 Locking

C13 - 12 A / 250 V

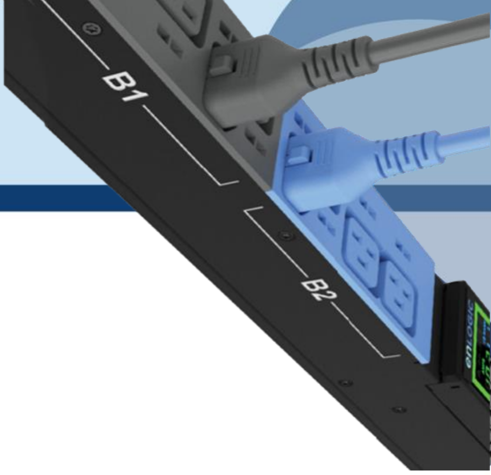
C19 - 16 A / 250 V



Outlet C13/ C19 Combo

C13 - 12 A / 250 V

C19 - 16 A / 250 V



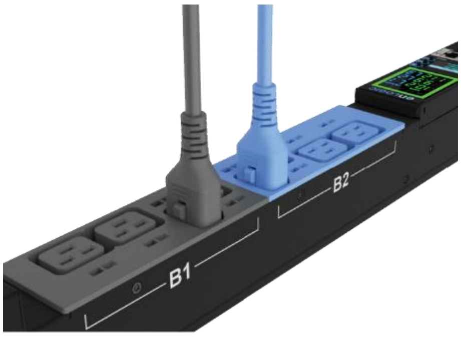
Self-Locking Cable & Non-Locking Cable

The IEC plug connectors will securely lock into the combo outlets. Both connections require deliberate action in order to plug/release the locking/non-locking buttons.

The locking/non-locking power cord is an inventive step to avoid loose IEC power connections and accidently unplugging the equipment. Enlogic’s reliable and secure locking power cords ensures reduction of risk and protection of vital IT assets.

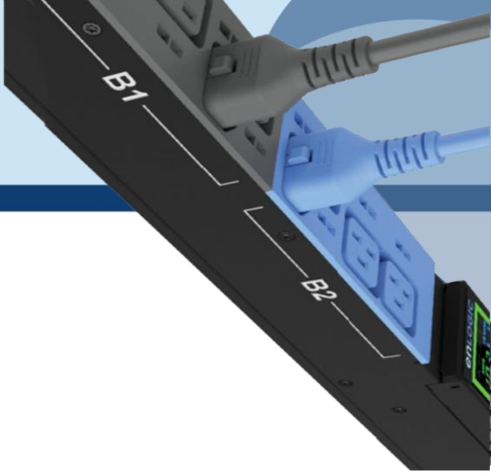
Locking Power Cords

Enlogic two way locking IEC power cords provide protection against accidental power loss from your attached IT equipment when used with the Enlogic PDUs. A small tab fits into the IEC C13 or C19 outlet of any PDU providing an error proof locking mechanism.



enLOGIC by nVent

Getting Started



Mounting PDU in Server Cabinet

Enlogic iPDUs are built with tool-less mounting in most rack enclosure designs.

(If the standard mounting pegs or mounting bracket do not comply with your rack configuration, contact Enlogic support for assistance.) Installation of a bracket can require a screwdriver.

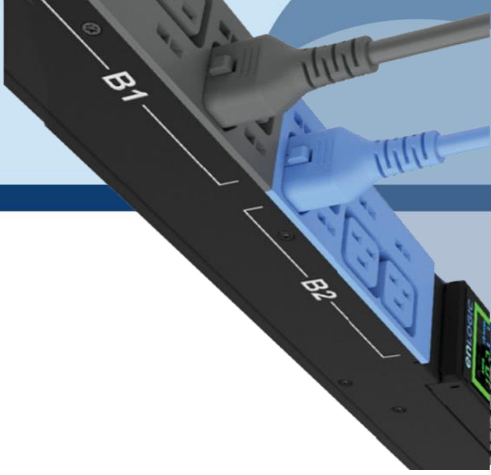
1. The Advantage Secure PDU comes with tool-less mounting pegs for ease and convenience.
2. Determine where the Advantage Secure PDU is mounted in the inside of the server cabinet.

   Note*: If your rack does not require mounting brackets, skip step 4 and 5. If required, attach the mounting brackets to the server cabinet. The standard Enlogic mounting brackets are secured to the rack using a screwdriver.*

3. Attach the enclosed mounting brackets to the server cabinet using the screws.
4. Insert the pegs into the server rack mounting holes or into the mounting brackets and tighten the mounting pegs into place.

   Note*: The distance between the mounting pegs varies depending on PDU models.*

5. Pull the power cord through the cabinet and tighten the mounting pegs. Proceed with connecting to a power source.



Connecting to Power Source

Before initiating the installation procedure, check the Branch Circuit Rating in the Safety Information section of this manual. Always follow local and national codes when installing the PDU. The PDU should be connected to a dedicated circuit protected by a branch circuit breaker that matches the PDU input-plug type.

Note: When connecting the Enlogic iPDU to a Power Source, make sure that you have enough length in the PDU power cord to reach the PDU power source.

1. Turn Off the feed circuit breaker.
2. Make sure that all circuit breakers on the Enlogic iPDU are set to ON.
3. Connect each Enlogic iPDU to an appropriately rated branch circuit.
4. Note: Refer to the label on the PDU for the input ratings.
5. Turn ON the feed circuit breaker.

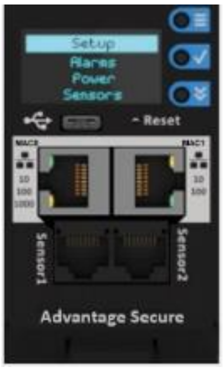
The OLED screen will display a status bar, when the PDU operating system is loading. The LED code on the OLED screen will flash in light pink. After 3 seconds, the Main Menu (Setup, Alarms, Power, Sensors) will display on the LED screen. Switched PDUs in the EN2000 series or EN6000 series show a light corresponding to each outlet as it is powered up.

Connecting PDU to Network

The Enlogic range of PDUs are set to obtain an IP address via DHCP by default. Therefore, when an Enlogic iPDU is connected to a network for the first time, the PDU will automatically obtain an IP address. In case the PDU is placed within a static network environment, users can configure the PDU to a Static IP via connecting to the PDU by serial cable or uploading a configuration file via USB. The PDU automatically obtains an IP address via DHCP, when connected to a network. Login to the Web UI to configure the PDU and assign a static IP address (if required).

1. Connect a standard Ethernet patch cable to Ethernet Port1/Port2 on the Advantage Secure PDU.
2. Connect the other end of the Ethernet cable to the LAN.
3. Make sure that the Ethernet port on the PDU shows a solid green light on the left and a flashing yellow light on the right to indicate successful connectivity to the network. (Gigabit Router is used in this network connection.)
4. Use the menu buttons to look up the IP address of the device on the OLED display by selecting Setup > Network > IPv4 or IPv6 as applicable.
5. In a standard web browser, type the PDU IP address and proceed to configure the PDU.

Connecting with Serial Connection

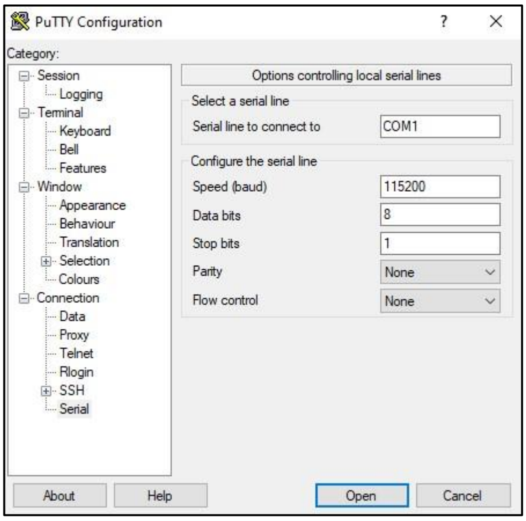


Alternatively, you can configure the network settings using the command line interface (CLI) with a serial connection. Users can either connect serially using the optional Enlogic RJ45-DB9 Cable (SKU EA9119) or by creating a unique pinout as described below.

1. Connect the RJ45 end of the serial cable into the port sensor 1 on the PDU.
2. Connect the DB9 end of the cable into the communications (COM) port on your computer.
3. Note: You can need to use a DB9 serial to USB connection cable for this step to connect via USB, if a DB9 serial port is not available on your computer.
4. Open a communications program such as HyperTerminal or PUTTY. Select the COM port.

Set the communications port as follows:

- Bits per second: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 115200

Data bits: 8

Stop bits: 1

Parity: None

Flow control: None

1. Use the default initial login indicated below.
   Note: Username and Password are both case sensitive.
   - Username: admin
   - Password: 12345678
2. The EN2.0> prompt appears after you have logged in.
3. To configure network settings, Type the appropriate net commands in Command prompt and press **Enter** button. All commands are case sensitive. You can type "?" to access the commands.
   - For the Net eth0 and eth1 IPv4 DHCP configuration, configure the below parameter.
   - net tcpip eth0dhcp
   - net tcpip eth1dhcp
   - Enter "Y" to validate and reboot the network management card.
   - For the static IPv4 configuration, configure the below parameters.
   - net tcpip eth0static x.x.x.x (ipaddress) x.x.x.x (netmask) x.x.x.x (gateway) Example: net tcpip eth0static 192.168.1.100 255.255.255.0 192.168.1.1
   - Enter "Y" to validate and reboot the network management card.

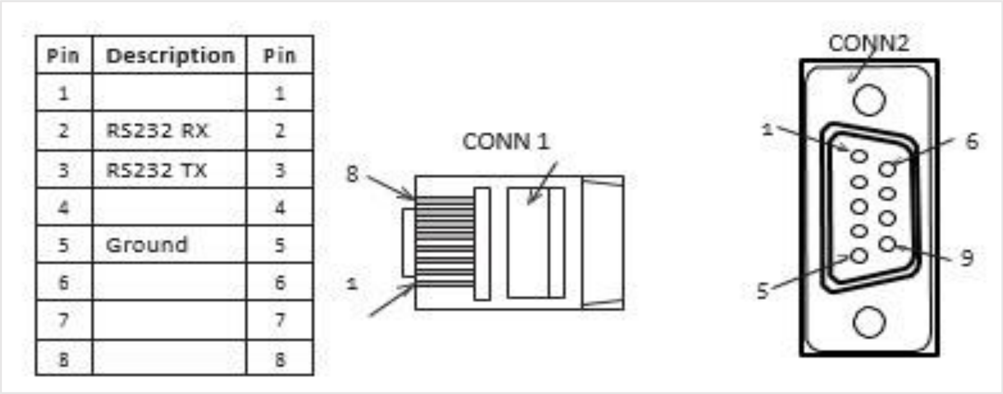
OR

   - net tcpip eth1static x.x.x.x (ipaddress) x.x.x.x (netmask) x.x.x.x (gateway) Example net tcpip eth1static 192.168.1.100 255.255.255.0 192.168.1.1

Creating Unique Pinout Connection

Enlogic recommends purchasing our serial cable for use with the Advantage Secure iPDU. This ensures an accurate connection. However, to create your own pinout connection for the RJ45 to Serial cable, make the wired connections as shown:

Refer to the **Web UI** section and **Command Line Interface** section for more information about managing the PDU.

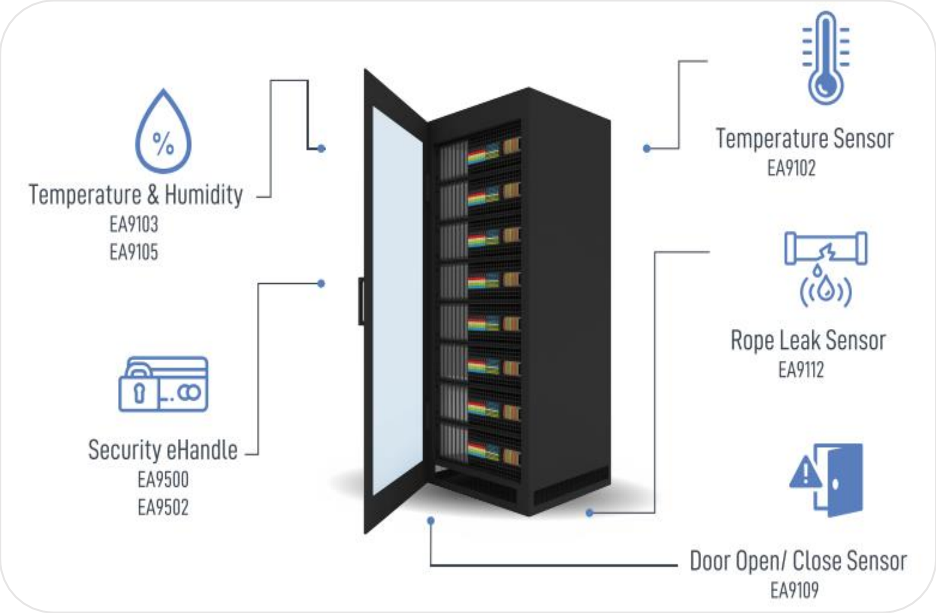


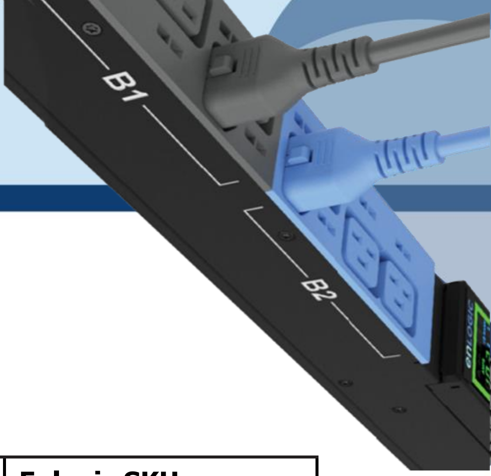
Pin	Description	Pin
1		1
2	RS232 RX	2
3	RS232 TX	3
4		4
5	Ground	5
6		6
7		7
8		8

Connecting Sensors (Optional)

To enable the Advantage Secure device to detect Enlogic conditions, connect one or more sensors to the PDU sensor port 1 or 2. The maximum distance for sensor cabling, which is plugged into the device sensor port should not exceed 100 feet (30 m). The maximum number of sensor detection points should not exceed 10.

Refer to the table below to determine the sensor detection points for each sensor used. For example: If you are using the 3 Temperature sensor + 1 Humidity sensor, 4 sensor points are in use, so only 4 additional sensor points are available.





Accessories & Sensor Description	No of Sensor Points	Enlogic SKU
Temperature Sensor	1	EA9102
Temperature and Humidity Sensor	2	EA9103
(3) Temperature + (1) Humidity Sensor	4	EA9105
Sensor Input Hub (3 sensor inputs)	NA	EA9106
Door Switch Sensor	1	EA9109
Dry Contact Cable	1	EA9110
Spot Fluid Leak Sensor	1	EA9111
Rope Fluid Leak Sensor	1	EA9112
LED Light Strip Sensor	1	EA9125
RJ45-DB9 CABLE	1	EA9119
USB TO RS232 CABLE	1	EA9128
HID RACK ACCESS Kit	1	EA9130
E-Handle (RFID) – no keypad available • E-Handle (with addition sensors of 3 Temperature + 1 Door)	2 6	EA9502
E-Handle (RFID & User PIN authentication) – with keypad • E-Handle (with addition sensors of 3 Temperature + 1 Door)	2 6	EA9500

For more information about Enlogic sensors, refer to the Installation sheet included with each sensor.

Web User Interface

Web User Interface (UI)

Connect the ethernet cable to the NMC, ensure it is active, which is indicated by a solid green light on the right and a flashing yellow light on the left. This indicates successful connectivity to the network.

Use the menu buttons to look up the IP address of the device on the OLED display by selecting Setup **> Network > IPv4 or IPv6 as applicable.**

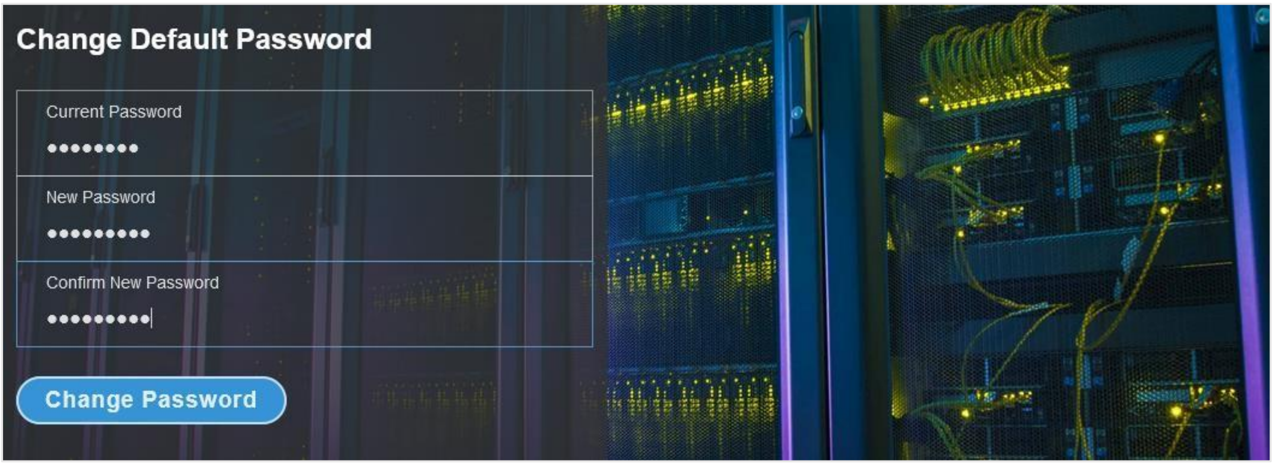
In a standard web browser, enter the PDU IP address ("https://IP ADDRESS") and proceed to configure the PDU as shown in the Web Configuration section. The supported Web browsers are Google Chrome (mobile and desktop), Mozilla Firefox, and Microsoft Edge on desktop. If browser displays "can't reach this page" please double check that you are using the "https://" protocol not "http://"

Introduction to Web UI

When the user logs in for the first time or in the case of a password expiry, the password must be entered on the login page.

On the login page:

1. A **Change Default Password** screen comes to view.
2. Type the **Current Password**, **New Password** and **Confirmed New Password**.



Change Default Password

Current Password
••••••••

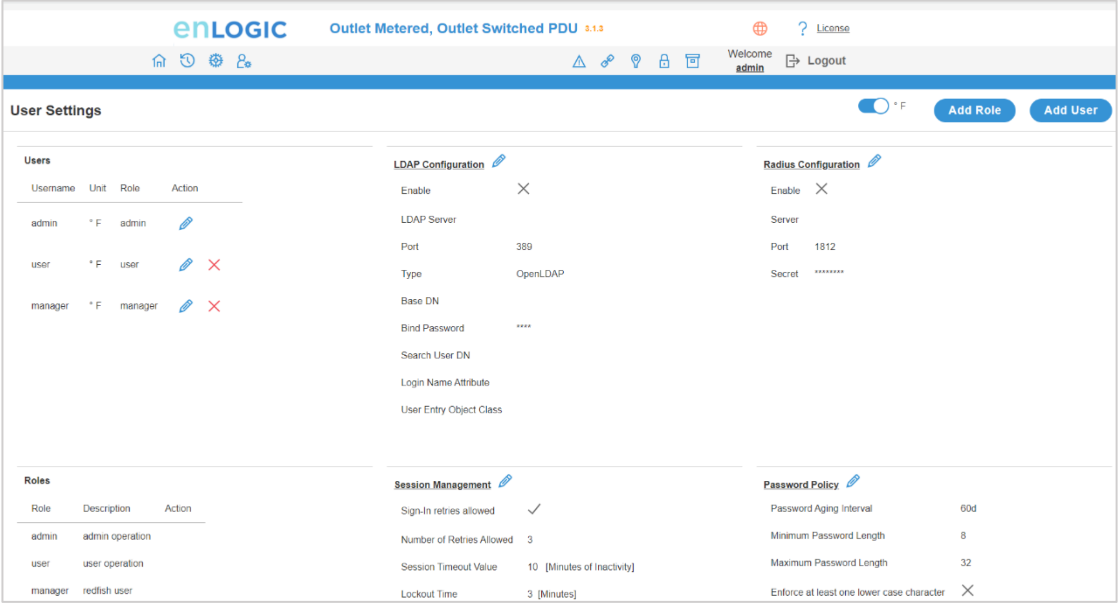
New Password
•••••••••

Confirm New Password
•••••••••

3. Click **Change Password** button to complete the process.

If the user needs to change the password using the web UI:

1. Click on the **User Settings** icon, the User Settings page comes to view.



User Settings

Users

Username	Unit	Role	Action
admin	° F	admin	✎
user	° F	user	✎ ✕
manager	° F	manager	✎ ✕

LDAP Configuration

Enable	✕
LDAP Server	
Port	389
Type	OpenLDAP
Base DN	
Bind Password	****
Search User DN	
Login Name Attribute	
User Entry Object Class	

Radius Configuration

Enable	✕
Server	
Port	1812
Secret	********

Roles

Role	Description	Action
admin	admin operation	
user	user operation	
manager	redfish user	

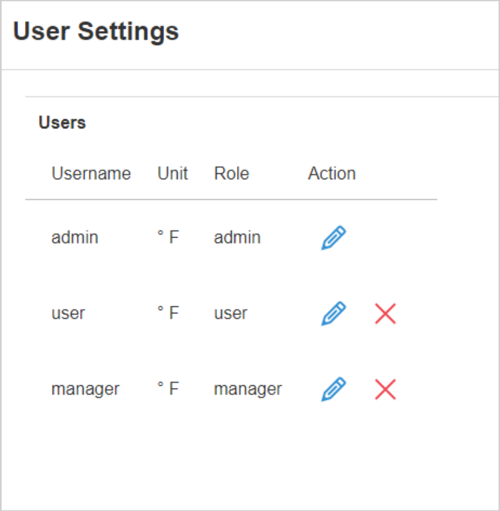
Session Management

Sign-In retries allowed	✓
Number of Retries Allowed	3
Session Timeout Value	10 [Minutes of Inactivity]
Lockout Time	3 [Minutes]

Password Policy

Password Aging Interval	60d
Minimum Password Length	8
Maximum Password Length	32
Enforce at least one lower case character	✕

2. In the **Users** section, under the category **Action**, click ✎ the icon next your **Username** and **Role** to edit/change the password

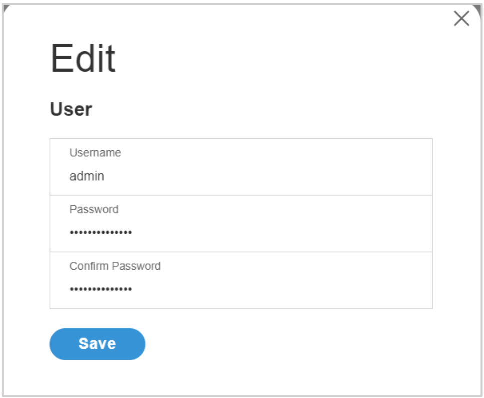


User Settings

Users

Username	Unit	Role	Action
admin	° F	admin	✎
user	° F	user	✎ ✕
manager	° F	manager	✎ ✕

3. Type the new password in the **Password** and **Confirm Password**.
4. Click **Save** button to complete the setting.



Edit

User

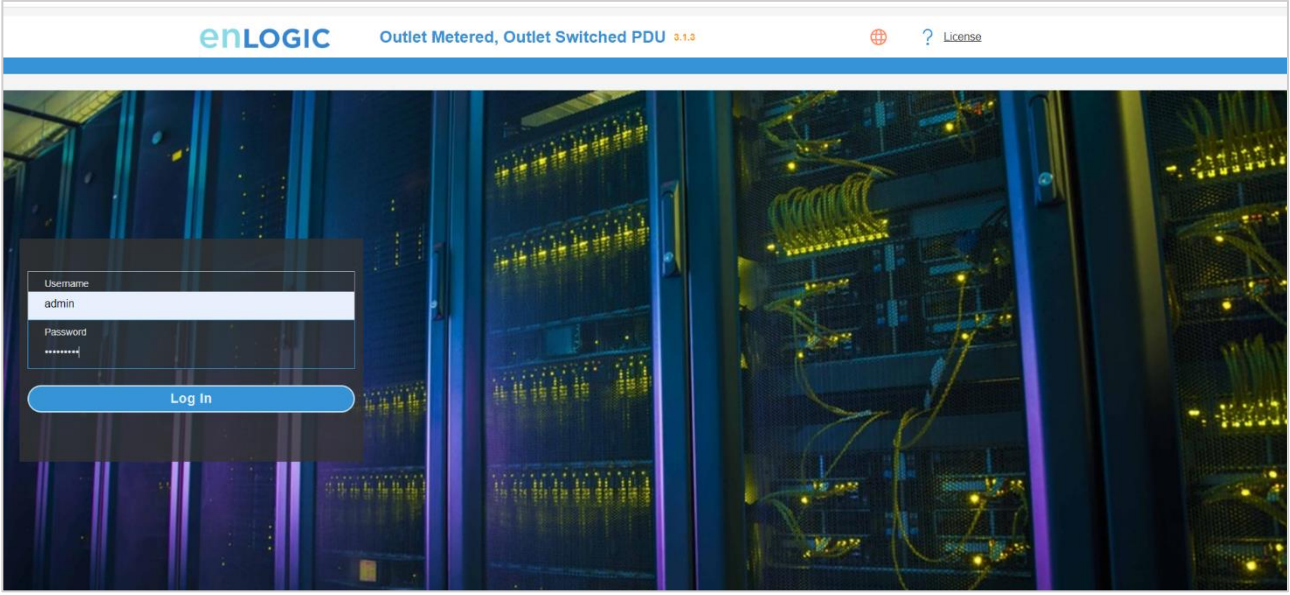
Username: admin

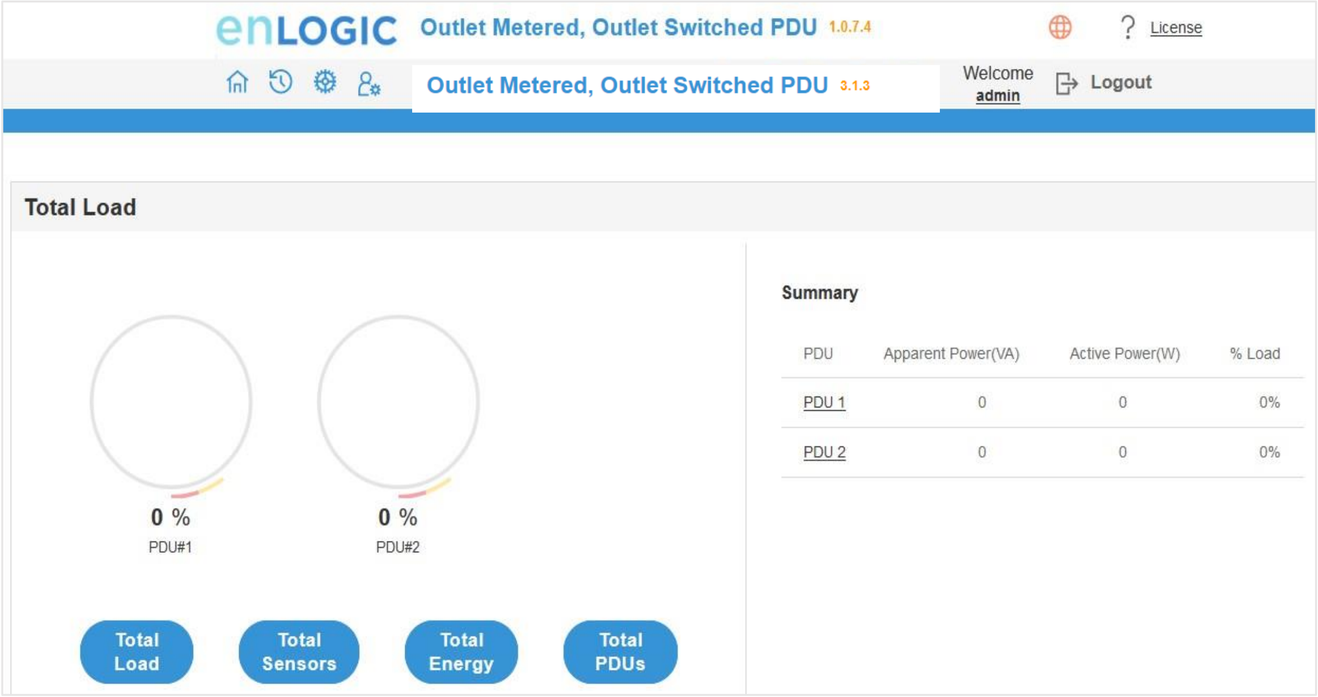
Password: ••••••••••••••

Confirm Password: ••••••••••••••

Navigating through the Web UI

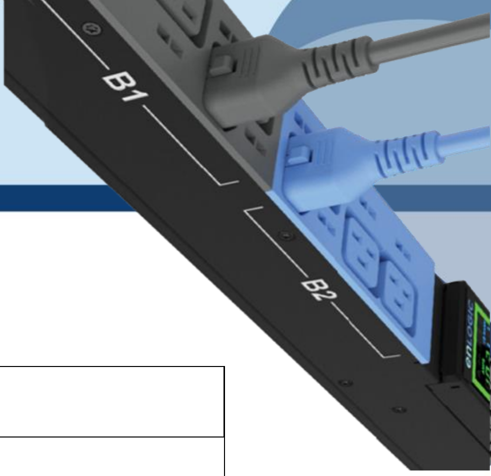
The landing page, followed by the login page.



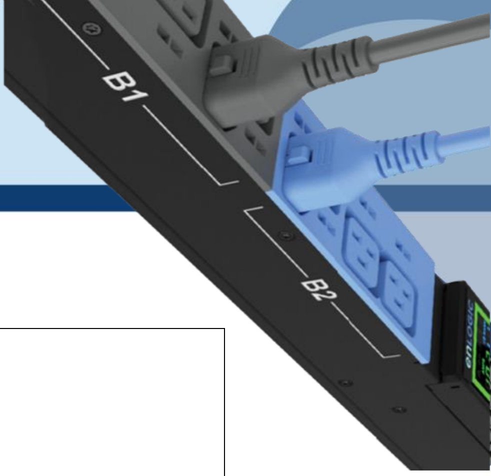


Summary

PDU	Apparent Power(VA)	Active Power(W)	% Load
PDU 1	0	0	0%
PDU 2	0	0	0%



Icon	Description
⌂	**Home Icon** Click this Home icon to redirect/move to home page. Home page provides an overview of the PDU with access to the Dashboard, Identification and Control & Manage.
↺	**Logs icon** Click this icon to view and download the logs and data logs of the PDU.
⚙	**Settings Icon** This settings icon allows the user to setup the Network Settings, System Management, SNMP Manager, Email Setup, Event Notifications, Trap Receiver, Thresholds, Rack Access Control and Smart Rack Control.
👤⚙	**User Settings Icon** Click this icon to view the logged-in user or admin or manager. Also, the user can change the account passwords and manage user accounts through this page. Users and Roles can be added. Also, configure the RADIUS and LDAP servers
⚠	**Alarms** Click this Alarm icon to view the details of the active critical alarms and active warning alarms. The Alarms are configured, based on different Thresholds which are set by the user on different parameters like Power, Voltage, Input Phase, Circuit Breaker, and External Sensors. Icon colors can be changed based on PDU alarm status. Critical Alarm always have high precedence over warnings. • **Red** - Critical Alarms • **Yellow** - Warnings
🔗	**Link** This Icon indicates the daisy-chain connection status alarms.

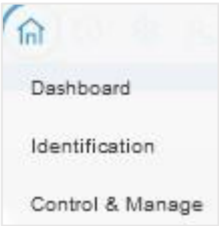


📍	**Sensor Warning** This icon represents the sensor related alarms like: • Temp • Humidity • Dry
🔒	**Status Alarms** This icon indicates the Door and HID sensor status alarms.
🗃	**Status Alarms** This icon indicates the CB and Outlet status alarms.
🌐	**Select a Language** This icon allows the user to select a Language. Currently eight languages are available to choose: English, French, Italian, Korean, German, Spanish, Japanese and Chinese.
?	Click this icon to download system diagnostic logs or navigate to the user guide.

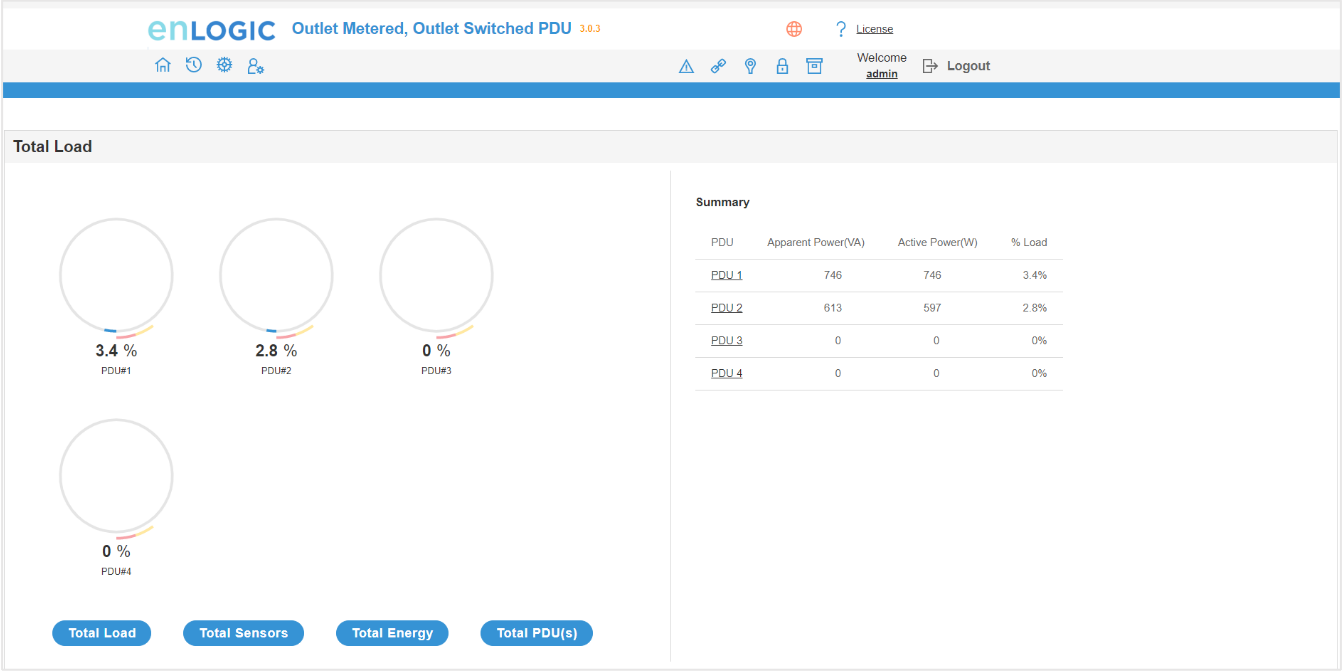
Dashboard

In this page, the user can view information of Total Load, Total Sensors, Total Energy and Total PDUs.

1. Click on the **Home** icon to dropdown the Home menu.
2. Select **Dashboard** to view information

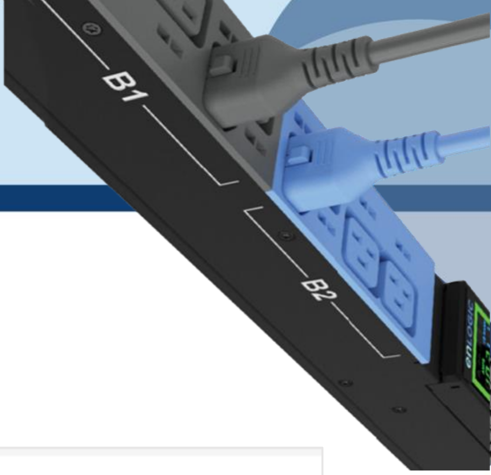


Total Load

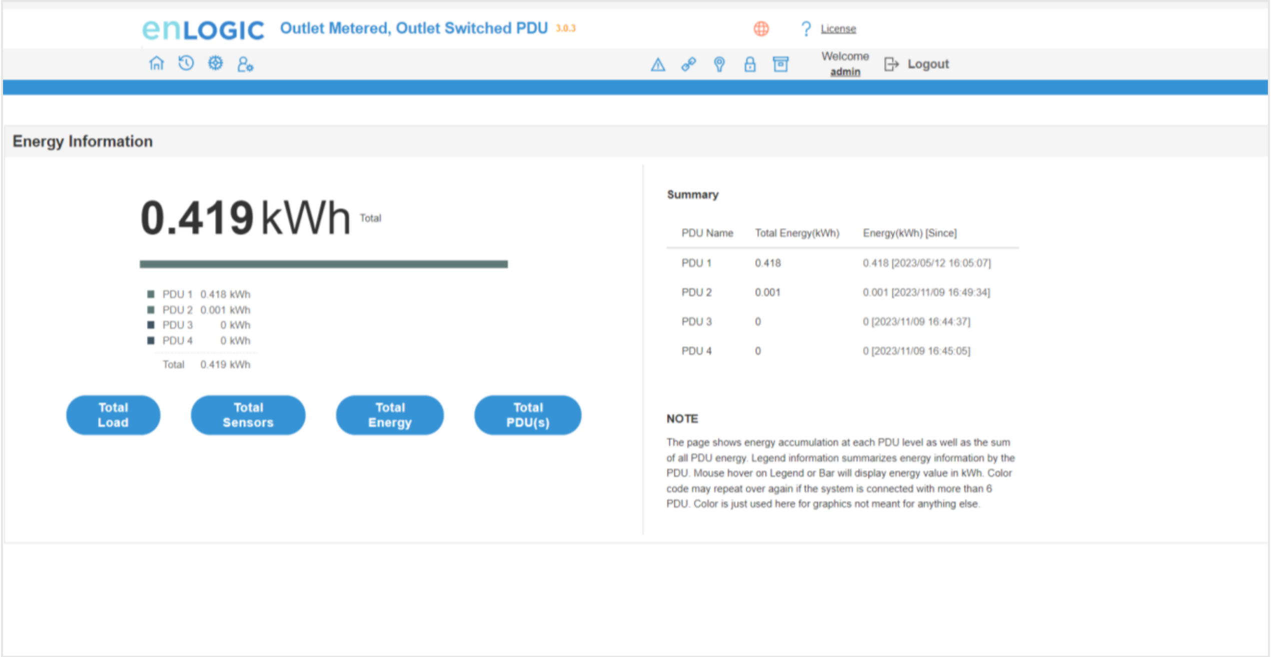


Summary

PDU	Apparent Power(VA)	Active Power(W)	% Load
PDU 1	746	746	3.4%
PDU 2	613	597	2.8%
PDU 3	0	0	0%
PDU 4	0	0	0%



Total Energy



Energy Information

0.419 kWh Total

■	PDU 1	0.418 kWh
■	PDU 2	0.001 kWh
■	PDU 3	0 kWh
■	PDU 4	0 kWh
	Total	0.419 kWh

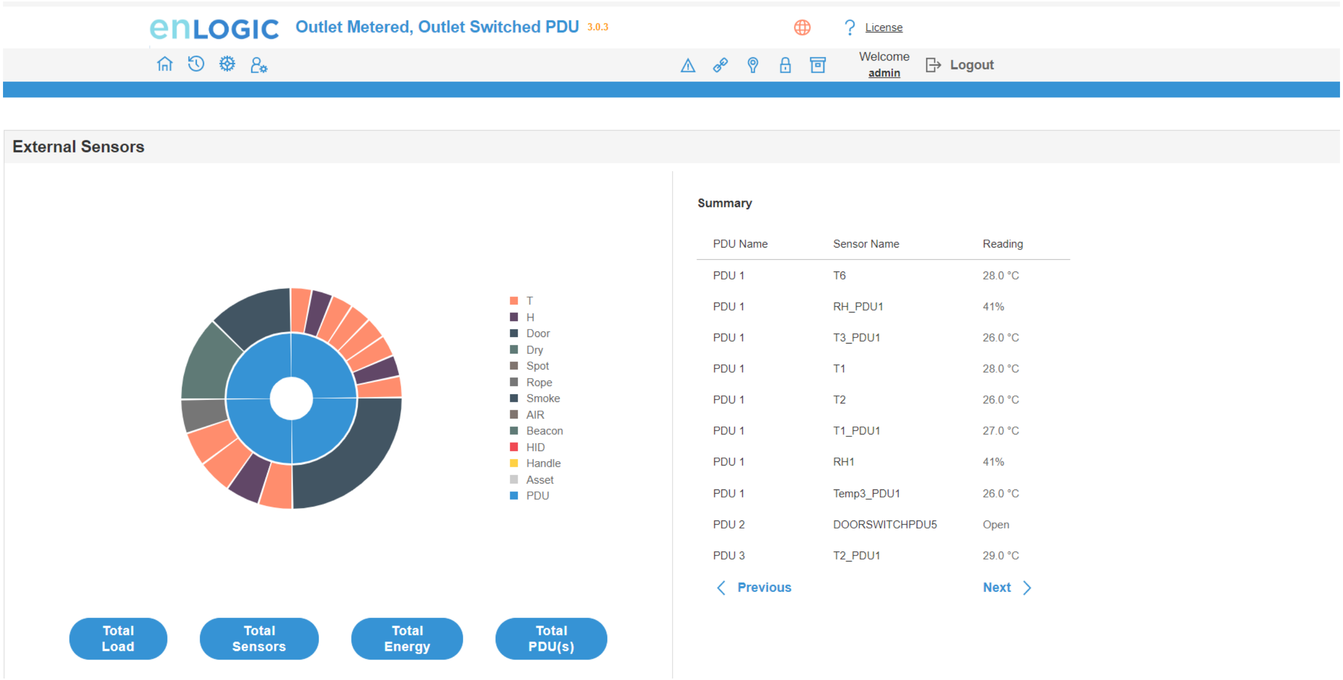
Summary

PDU Name	Total Energy(kWh)	Energy(kWh) [Since]
PDU 1	0.418	0.418 [2023/05/12 16:05:07]
PDU 2	0.001	0.001 [2023/11/09 16:49:34]
PDU 3	0	0 [2023/11/09 16:44:37]
PDU 4	0	0 [2023/11/09 16:45:05]

NOTE

The page shows energy accumulation at each PDU level as well as the sum of all PDU energy. Legend information summarizes energy information by the PDU. Mouse hover on Legend or Bar will display energy value in kWh. Color code may repeat over again if the system is connected with more than 6 PDU. Color is just used here for graphics not meant for anything else.

Total Sensors

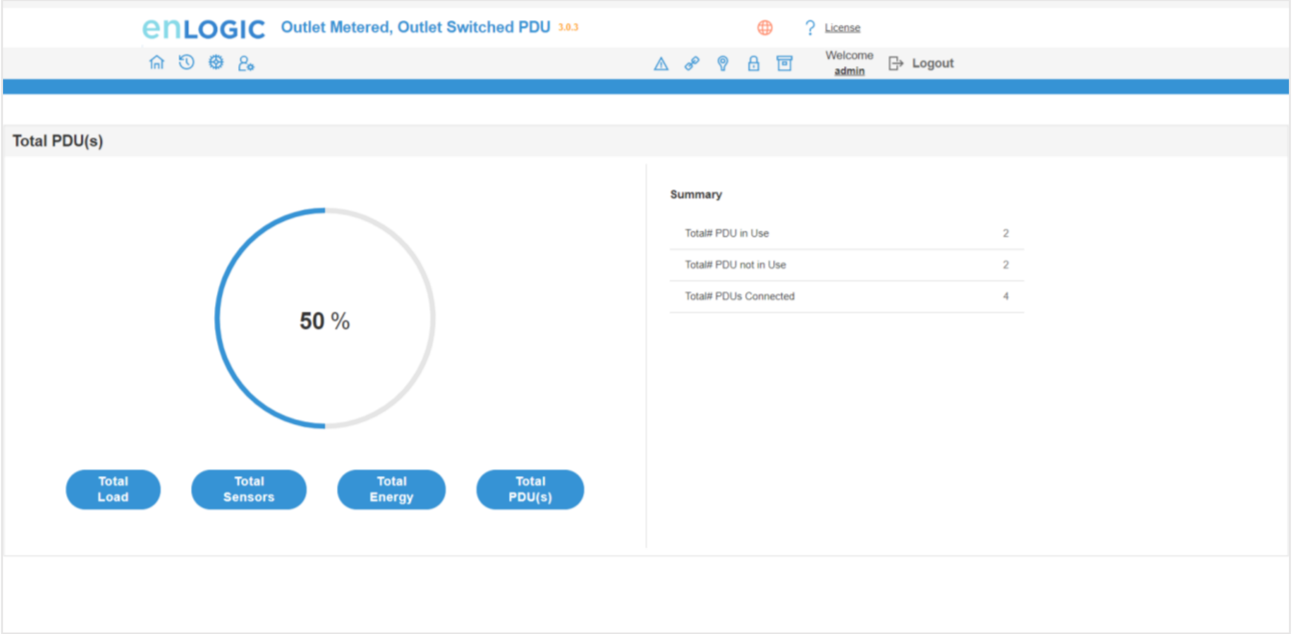


External Sensors

Summary

PDU Name	Sensor Name	Reading
PDU 1	T6	28.0 °C
PDU 1	RH_PDU1	41%
PDU 1	T3_PDU1	26.0 °C
PDU 1	T1	28.0 °C
PDU 1	T2	26.0 °C
PDU 1	T1_PDU1	27.0 °C
PDU 1	RH1	41%
PDU 1	Temp3_PDU1	26.0 °C
PDU 2	DOORSWITCHPDU5	Open
PDU 3	T2_PDU1	29.0 °C

Total PDUs



Total PDU(s)

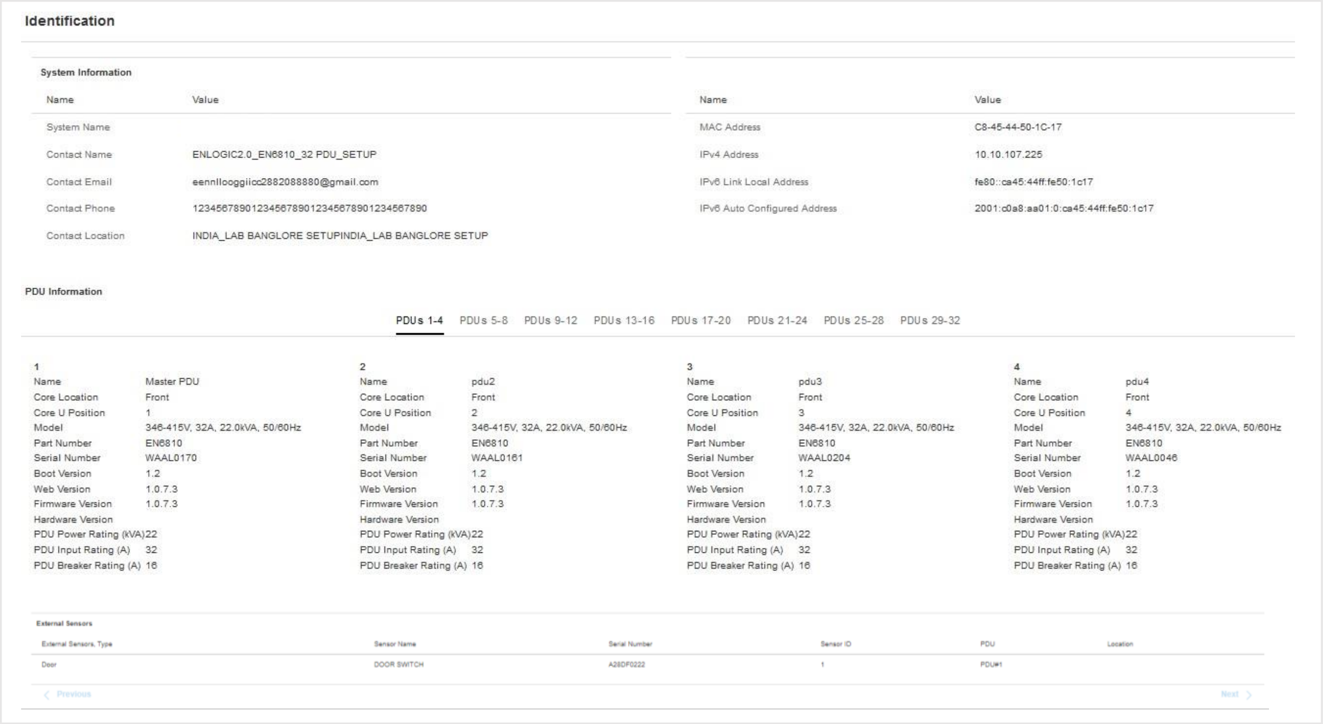
Summary

Total# PDU in Use	2
Total# PDU not in Use	2
Total# PDUs Connected	4

Identification

In this page, the user can view the **System Information**, and individual **PDU Information**.

1. Click on the **Home** icon to dropdown the Home menu
2. Select **Identification** to view the information and details about the External sensors connected.



Identification

System Information

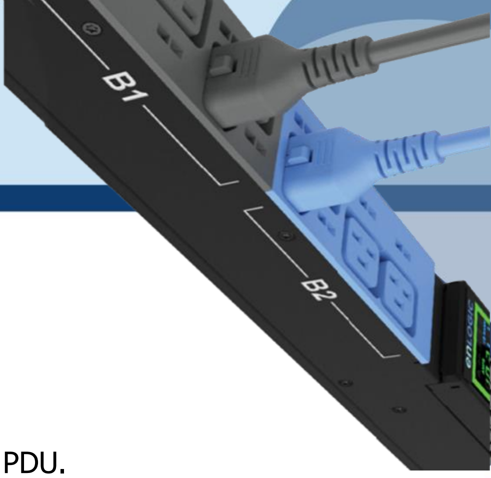
Name	Value	Name	Value
System Name		MAC Address	C8-45-44-50-1C-17
Contact Name	ENLOGIC2.0_EN6810_32 PDU_SETUP	IPv4 Address	10.10.107.225
Contact Email	eennllooggiicc2882088880@gmail.com	IPv6 Link Local Address	fe80::ca45:44ff:fe50:1c17
Contact Phone	1234567890123456789012345678901234567890	IPv6 Auto Configured Address	2001:c0a8:aa01:0:ca45:44ff:fe50:1c17
Contact Location	INDIA_LAB BANGLORE SETUPINDIA_LAB BANGLORE SETUP		

PDU Information

1		2		3		4	
Name	Master PDU	Name	pdu2	Name	pdu3	Name	pdu4
Core Location	Front	Core Location	Front	Core Location	Front	Core Location	Front
Core U Position	1	Core U Position	2	Core U Position	3	Core U Position	4
Model	346-415V, 32A, 22.0kVA, 50/60Hz	Model	346-415V, 32A, 22.0kVA, 50/60Hz	Model	346-415V, 32A, 22.0kVA, 50/60Hz	Model	346-415V, 32A, 22.0kVA, 50/60Hz
Part Number	EN6810	Part Number	EN6810	Part Number	EN6810	Part Number	EN6810
Serial Number	WAAL0170	Serial Number	WAAL0161	Serial Number	WAAL0204	Serial Number	WAAL0046
Boot Version	1.2	Boot Version	1.2	Boot Version	1.2	Boot Version	1.2
Web Version	1.0.7.3	Web Version	1.0.7.3	Web Version	1.0.7.3	Web Version	1.0.7.3
Firmware Version	1.0.7.3	Firmware Version	1.0.7.3	Firmware Version	1.0.7.3	Firmware Version	1.0.7.3
Hardware Version		Hardware Version		Hardware Version		Hardware Version	
PDU Power Rating (kVA)	22	PDU Power Rating (kVA)	22	PDU Power Rating (kVA)	22	PDU Power Rating (kVA)	22
PDU Input Rating (A)	32	PDU Input Rating (A)	32	PDU Input Rating (A)	32	PDU Input Rating (A)	32
PDU Breaker Rating (A)	16	PDU Breaker Rating (A)	16	PDU Breaker Rating (A)	16	PDU Breaker Rating (A)	16

External Sensors

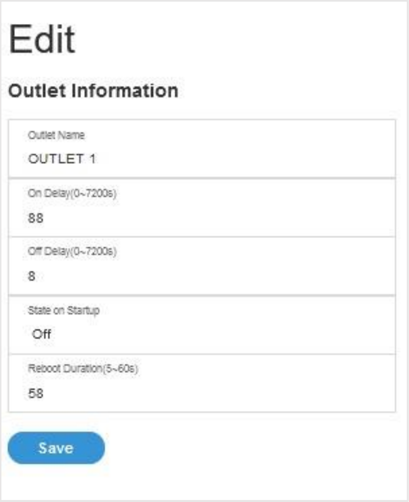
External Sensors, Type	Sensor Name	Serial Number	Sensor ID	PDU	Location
Door	DOOR SWITCH	A28DF0222	1	PDU#1	



Control and Manage

In this page, the user can view and control the **Power Outlet** of the PDU.

1. Click on the Home icon to dropdown the Home menu
2. Select Control & Manage.
3. Enable the Outlet Control Enabled.
4. Click on the ✎ icon.
5. Edit/change the Outlet information below:
   - **Outlet name to identify the outlet**
   - **On delay time** (0-7200 seconds)
   - **Off delay time** (0-7200 seconds)
   - **State on startup** (On, Off, and last known can be selected)
   - **Reboot duration** (configure time between 5 to 60 seconds)



Edit

Outlet Information

Outlet Name
OUTLET 1

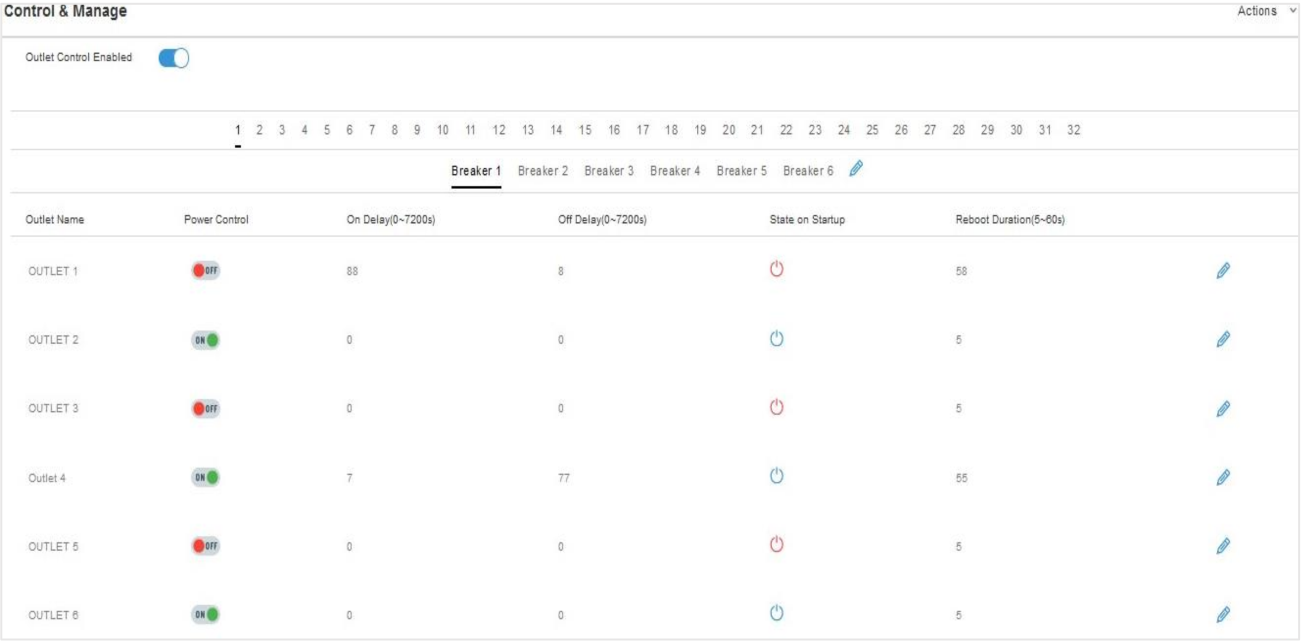
On Delay(0~7200s)
88

Off Delay(0~7200s)
8

State on Startup
Off

Reboot Duration(5~60s)
58

6. On the top right side of the Control & Manage page there is an Actions ⌄ icon, to **Reset PDU Energy**

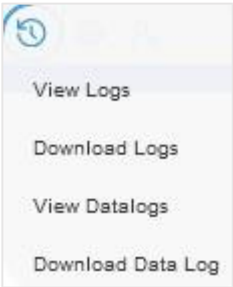


Control & Manage

Outlet Control Enabled ●

Outlet Name	Power Control	On Delay(0~7200s)	Off Delay(0~7200s)	State on Startup	Reboot Duration(5~60s)	
OUTLET 1	OFF	88	8	⏻	58	✎
OUTLET 2	ON	0	0	⏻	5	✎
OUTLET 3	OFF	0	0	⏻	5	✎
Outlet 4	ON	7	77	⏻	55	✎
OUTLET 5	OFF	0	0	⏻	5	✎
OUTLET 6	ON	0	0	⏻	5	✎

View Logs



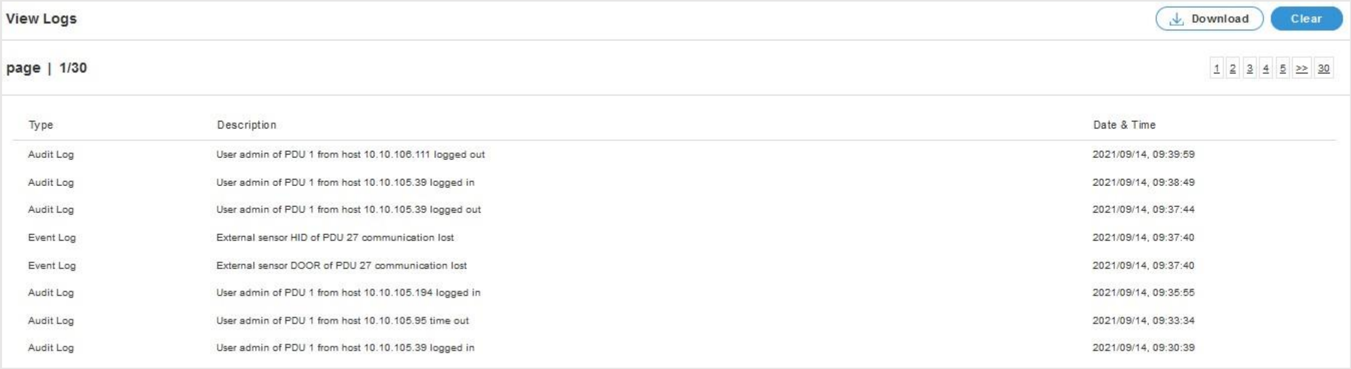
In this page, the user can view, download, and clear the Actions performed by the PDU.

Some of the actions performed by the PDU are:

- Generating **Event**, **Audit** and **Application logs**,
- Recording **Power Share** details.

Click on the **System Administration** icon to dropdown the menu.

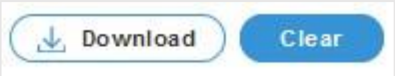
1. Select the **View Logs** to view the information.

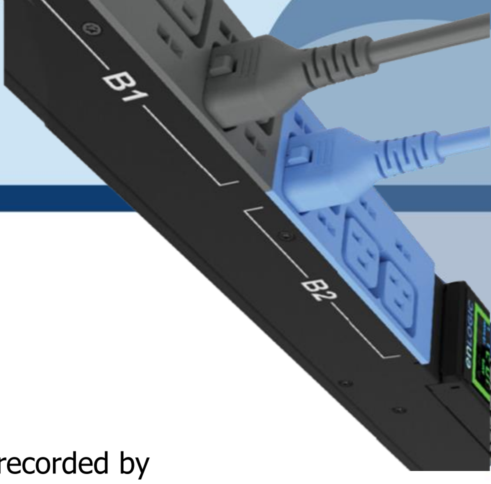


page | 1/30

Type	Description	Date & Time
Audit Log	User admin of PDU 1 from host 10.10.106.111 logged out	2021/09/14, 09:39:59
Audit Log	User admin of PDU 1 from host 10.10.105.39 logged in	2021/09/14, 09:38:49
Audit Log	User admin of PDU 1 from host 10.10.105.39 logged out	2021/09/14, 09:37:44
Event Log	External sensor HID of PDU 27 communication lost	2021/09/14, 09:37:40
Event Log	External sensor DOOR of PDU 27 communication lost	2021/09/14, 09:37:40
Audit Log	User admin of PDU 1 from host 10.10.105.194 logged in	2021/09/14, 09:35:55
Audit Log	User admin of PDU 1 from host 10.10.105.95 time out	2021/09/14, 09:33:34
Audit Log	User admin of PDU 1 from host 10.10.105.39 logged in	2021/09/14, 09:30:39

2. On the top-right side of the view log page, Click the below options as required:
3. **Download** Log: to download the logs
4. **Clear** Log: to delete/clear the logs.



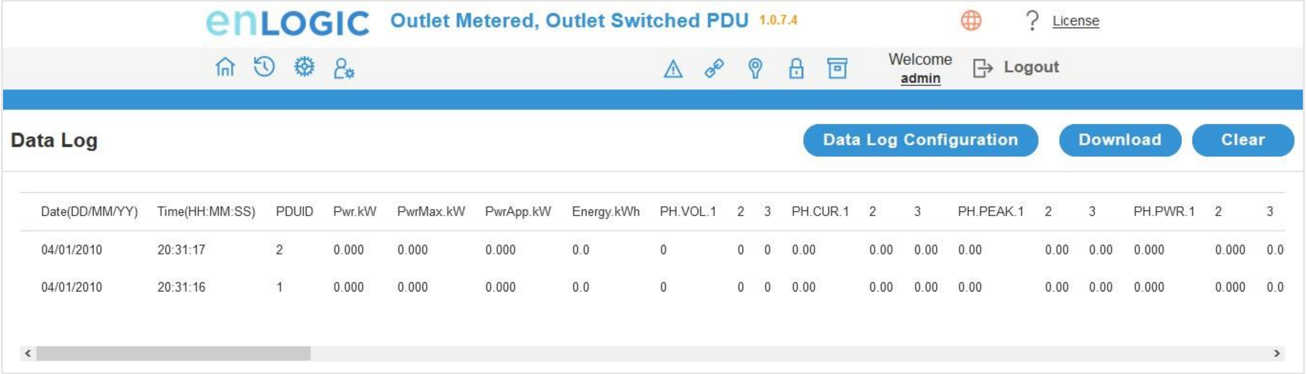


View Data Logs

In this page, the user can view, configure, download, and clear the Data recorded by the PDU. The Data recorded by the PDU are:

- **Energy** information
- **Power** information
- **Date and Time** information

1. Click on the **System Administration** icon to dropdown the menu.
2. Select the **View Data Logs** to view the information.

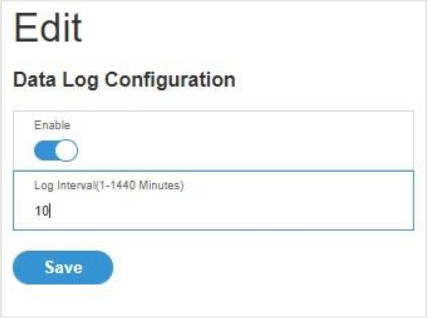


Data Log

Date(DD/MM/YY)	Time(HH:MM:SS)	PDUID	Pwr.kW	PwrMax.kW	PwrApp.kW	Energy.kWh	PH.VOL.1	2	3	PH.CUR.1	2	3	PH.PEAK.1	2	3	PH.PWR.1	2	3
04/01/2010	20:31:17	2	0.000	0.000	0.000	0.0	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00	0.000	0.000	0.0
04/01/2010	20:31:16	1	0.000	0.000	0.000	0.0	0	0	0	0.00	0.00	0.00	0.00	0.00	0.00	0.000	0.000	0.0

3. On the top- right side of the View Data Log page, Click the below options as required:

- **Data Log Configuration,** Click on this button to:
  - **Enable** Data Log Configuration if data log is required.
  - **Log Interval** time that needs to be recorded.
- **Download** Data Log: to download the logs.
- **Clear** Data Log: to delete/clear the logs.

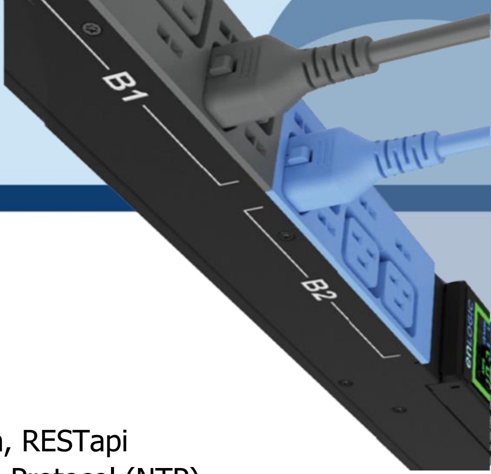


Edit

Data Log Configuration

Enable

Log Interval(1-1440 Minutes)
10

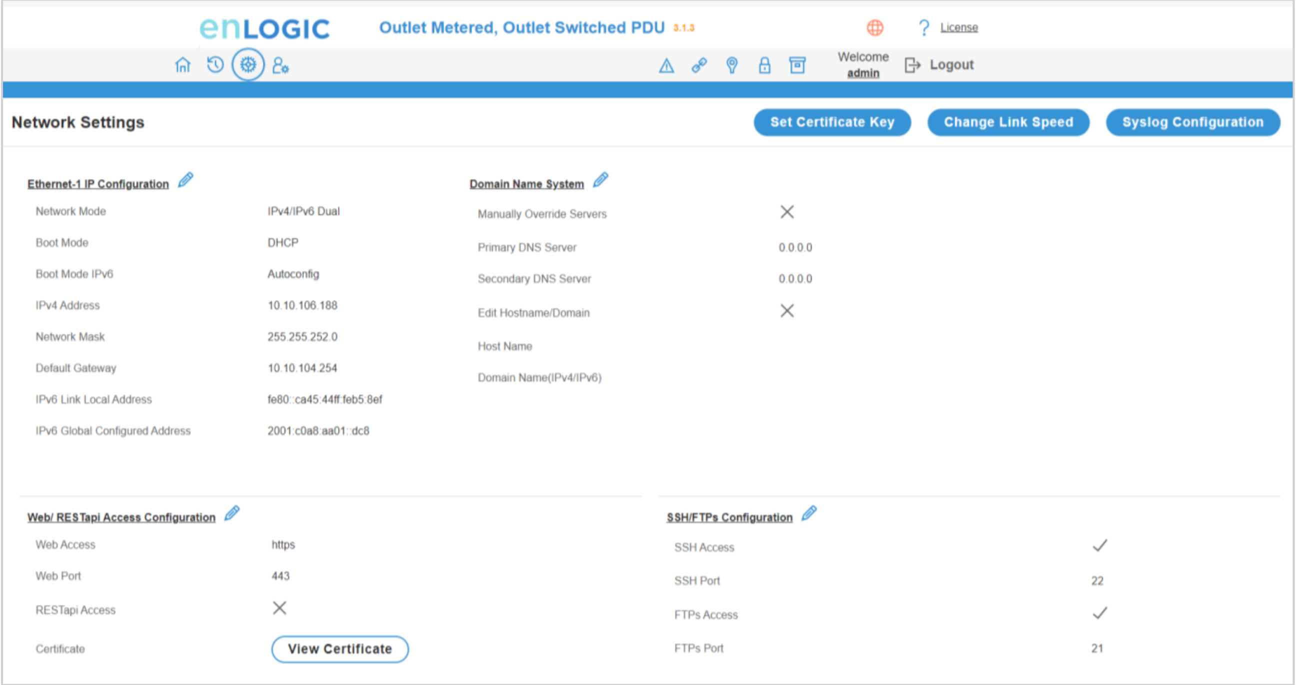


Network Settings

This page allows the management of IP Configuration, Web Configuration, RESTapi Configuration, DNS Configuration, SSH/FTPs Configuration, Network Time Protocol (NTP), Date/Time Settings and Daylight-Savings Time.

This PDU supports IPv4 and IPV6 with full featured network management and alerting capabilities. After you select your Internet protocol option, you will be able to communicate via HTTP, HTTPS, SNMP, FTPS and SSH and Email for network communications.

1. Click on the **Settings** icon to dropdown the Settings menu.
2. Select the **Network Settings** to view the information.



Network Settings

Ethernet-1 IP Configuration

Network Mode	IPv4/IPv6 Dual
Boot Mode	DHCP
Boot Mode IPv6	Autoconfig
IPv4 Address	10.10.106.188
Network Mask	255.255.252.0
Default Gateway	10.10.104.254
IPv6 Link Local Address	fe80::ca45:44ff:feb5:8ef
IPv6 Global Configured Address	2001:c0a8:aa01::dc8

Domain Name System

Manually Override Servers	✗
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Edit Hostname/Domain	✗
Host Name	
Domain Name(IPv4/IPv6)	

Web/ RESTapi Access Configuration

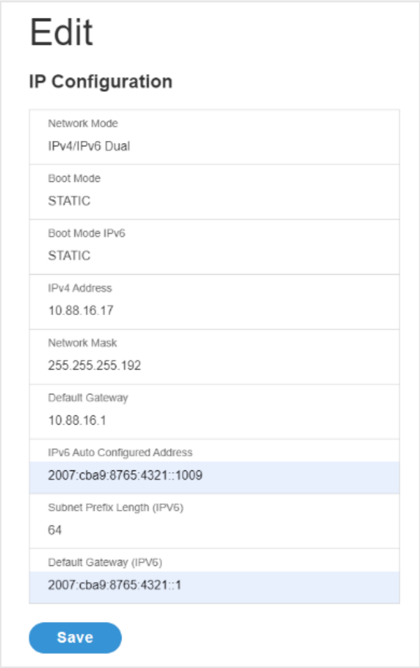
Web Access	https
Web Port	443
RESTapi Access	✗
Certificate	View Certificate

SSH/FTPs Configuration

SSH Access	✓
SSH Port	22
FTPs Access	✓
FTPs Port	21

3. Click on the ✎ icon to edit/change the **IP Configuration** information below:

- **Network Mode**
- **Boot Mode**
- **Boot Mode Ipv6**
- **IPv4 Address**
- **Network Mask**
- **Default Gateway**
- **IPv6 Auto Configured Address**
- **Subnet Prefix Length (Ipv6)**
- **Default Gateway (Ipv6)**
- Click **Save** button to complete setting.



Edit

IP Configuration

Network Mode
IPv4/IPv6 Dual

Boot Mode
STATIC

Boot Mode IPv6
STATIC

IPv4 Address
10.88.16.17

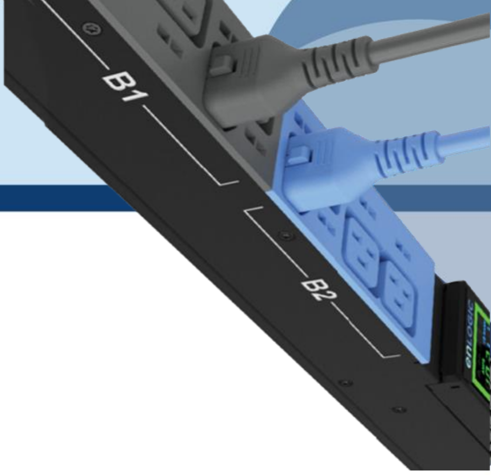
Network Mask
255.255.255.192

Default Gateway
10.88.16.1

IPv6 Auto Configured Address
2007:cba9:8765:4321::1009

Subnet Prefix Length (IPV6)
64

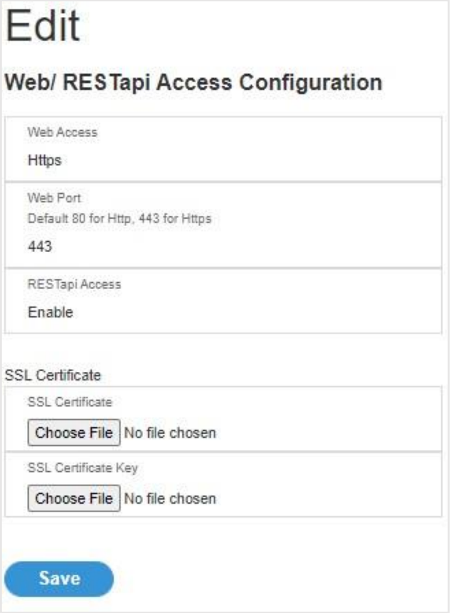
Default Gateway (IPV6)
2007:cba9:8765:4321::1



4. By default, accessing the PDU uses HTTPS port setting.

Click the ✎ icon to edit/change the **Web/RESTapi Access Configuration** information below:

- **Web Access** (**HTTP** or **HTTPS**).
- **Web *Port*** (Default 80 for HTTP, and 443 for HTTPS).
- Enable **RESTapi Access**.
- To access the HTTPS settings, upload the **SSL Certificate** and **SSL Certificate Key** provided by Enlogic.
- Click Save button to complete the settings.



Edit

Web/ RESTapi Access Configuration

Web Access
Https

Web Port
Default 80 for Http, 443 for Https
443

RESTapi Access
Enable

SSL Certificate

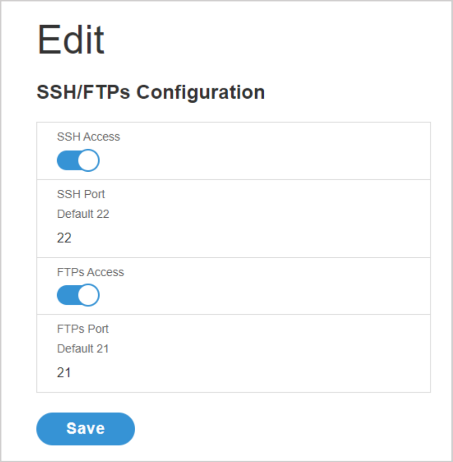
SSL Certificate
Choose File No file chosen

SSL Certificate Key
Choose File No file chosen

5. Edit the SSH/FTPS configuration Settings information below:

Click the ✎ icon to edit/change the **SSH/FTPs Configuration** information below:

- Enable **SSH Access.**
- **SSH Port** (Default 22).
- Enable **FTPs Access.**
- **FTPs Port** (Default 21).
- Click Save button to complete the settings.



Edit

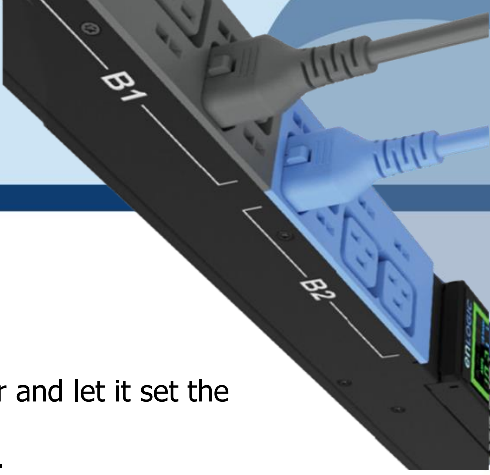
SSH/FTPs Configuration

SSH Access
●

SSH Port
Default 22
22

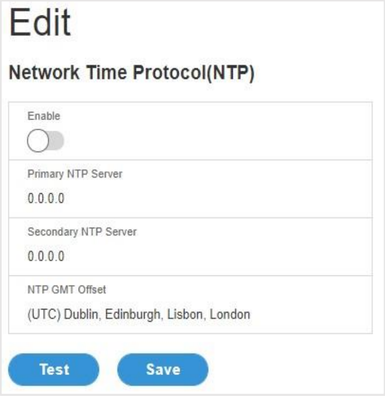
FTPs Access
●

FTPs Port
Default 21
21



6. You can link the PDU to a **Network Time Protocol (NTP)** server and let it set the date and time.
Click the icon ✎ to edit/change the NTP Setting information below:

- **Enable** the NTP settings.
- To synchronize the PDU time with a selected server.
- Type the valid **Primary** NTP server address.
- Type the valid **Secondary** NTP server address.
- **The user has an option to configure only the primary IP, the secondary one is not mandatory.**
- Select the desired **NTP GMT offset** time from the dropdown list.
- Click **Test** button to check if the network is valid or not.
- Click **Save** button to complete setting.



Edit

Network Time Protocol(NTP)

Enable

○

Primary NTP Server

0.0.0.0

Secondary NTP Server

0.0.0.0

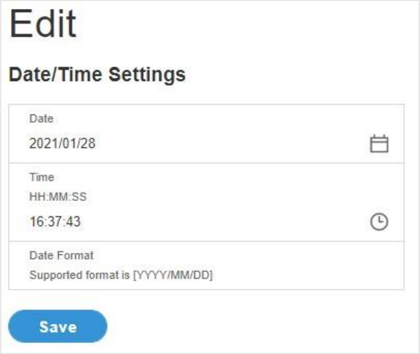
NTP GMT Offset

(UTC) Dublin, Edinburgh, Lisbon, London

7. You can manually set the internal clock on the PDU.

Click the ✎ icon to edit/change the **Date/Time Setting** information below:

- Type the **Date** in YYYY/MM/DD format or use the calendar icon.
- Type the **Time** in HH: MM: SS format and time is measured in 24-hour format.
- Click **Save** button to complete setting.



Edit

Date/Time Settings

Date

2021/01/28

Time

HH:MM:SS

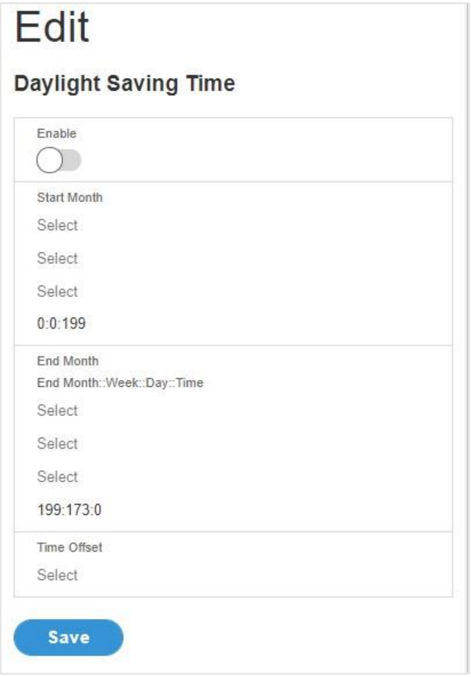
16:37:43

Date Format

Supported format is [YYYY/MM/DD]

8. Click on the ✎ icon to edit/change the Daylight-Saving Time information below:

- **Enable** the Daylight-Saving Time.
- Select the specifics of the **Start Month**:
  - Month
  - Week
  - Day
  - Time
- Select the specifics of the **End Month**:
  - Month
  - Week
  - Day
  - Time
  - Assign the **Time Offset.**
- Click **Save** button to complete setting.



Edit

Daylight Saving Time

Enable

○

Start Month

Select

Select

Select

0:0:199

End Month

End Month::Week::Day::Time

Select

Select

Select

199:173:0

Time Offset

Select

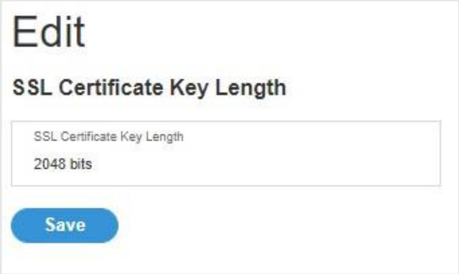
Save

9. On the top-right side of the Network Settings page, Click the below options as required:

Set Certificate Key

Below are the steps to edit SSL Certificate Key Length.

- Click **Set Certificate Key** button.
- Select **bits** (**1024/2048)** from dropdown menu.
- Click **Save** button to complete setting.



Edit

SSL Certificate Key Length

SSL Certificate Key Length

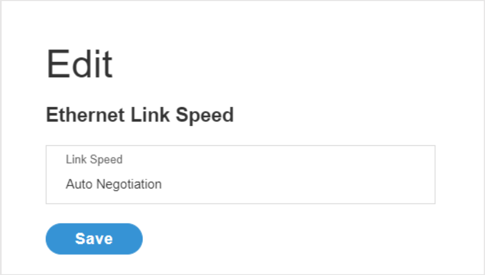
2048 bits

Save

Change Link Speed

Below are the steps to change the Ethernet link speed.

- Click **Change Link Speed** button.
- Select speed (as required below) from dropdown menu.
  - – **Auto Negotiation**
  - – **10/100 Mbps**
  - – **1 Gbps**
- Click **Save** button to complete setting.



Edit

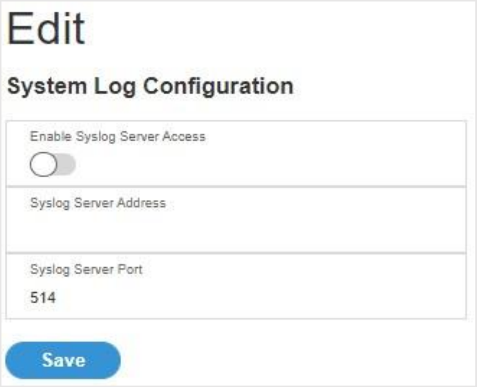
Ethernet Link Speed

Link Speed: Auto Negotiation

Syslog Configuration

Below are the steps to configure the Syslog.

- Click **Syslog Configuration** button.
- Enable the **Enable Syslog Server Access**.
- Type the **Syslog Server Address**.
- Select **Syslog Server Port** number.
- Click **Save** button to complete setting.



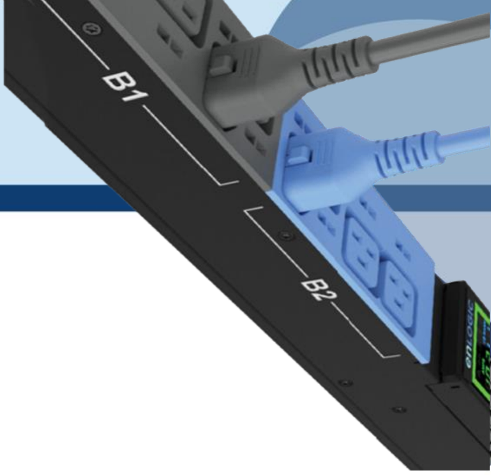
Edit

System Log Configuration

Enable Syslog Server Access: ○

Syslog Server Address:

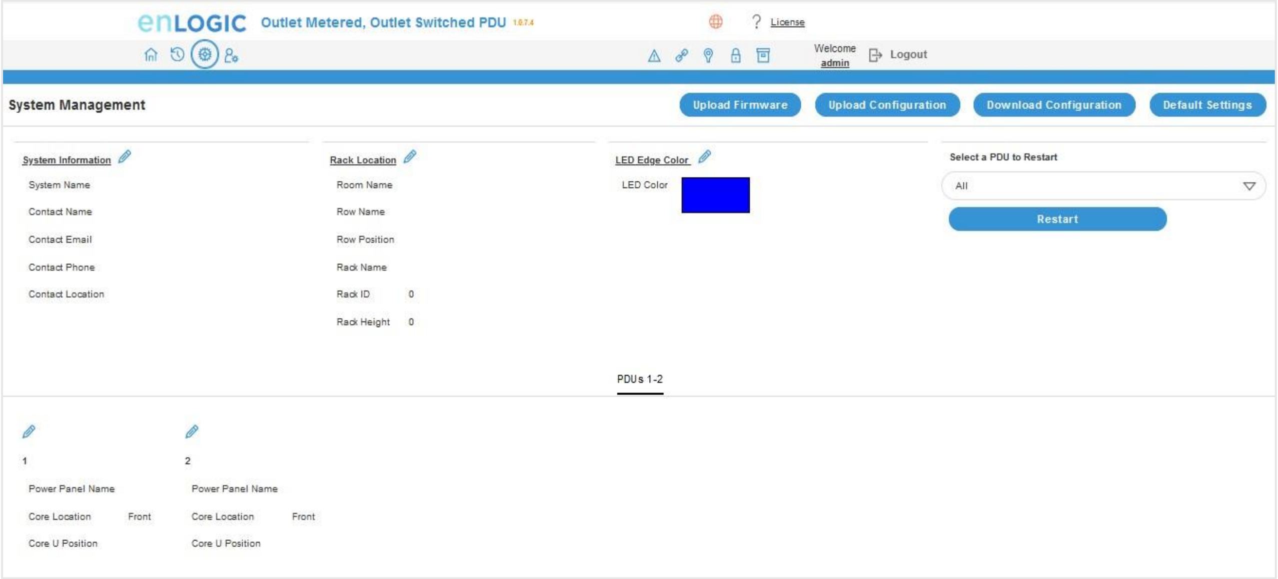
Syslog Server Port: 514



System Management

This page allows the user to perform functions like, **Uploading Firmware**, **Uploading Configuration**, **Downloading Configuration** and setting the PDU to its **Default Settings**. It also allows the user to **Restart** the PDU.

1. Click on the **Settings** icon to dropdown the Settings menu.
2. Select the **System Management** to view the information.



System Management

System Information
System Name
Contact Name
Contact Email
Contact Phone
Contact Location

Rack Location
Room Name
Row Name
Row Position
Rack Name
Rack ID 0
Rack Height 0

LED Edge Color
LED Color

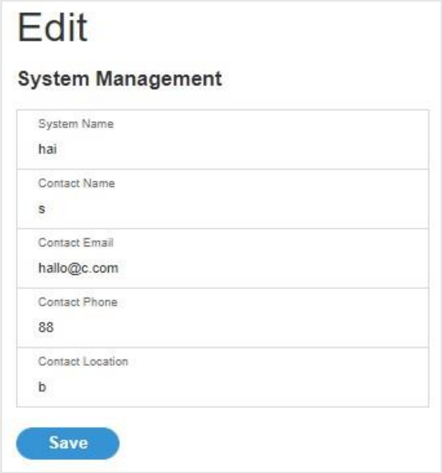
Select a PDU to Restart
All

1
Power Panel Name
Core Location Front
Core U Position

2
Power Panel Name
Core Location Front
Core U Position

3. Click on ✎ the icon to edit/change the System Information below.

- Enter the **System Name** of the PDU for identification
- Enter the **Contact Name** of the contact person.
- Enter the **Contact Email** of the contact person.
- Enter the **Contact Phone** of the contact person.
- Enter the **Contact Location** of the contact person.
- Click **Save** button to complete setting.



Edit

System Management

System Name
hai

Contact Name
s

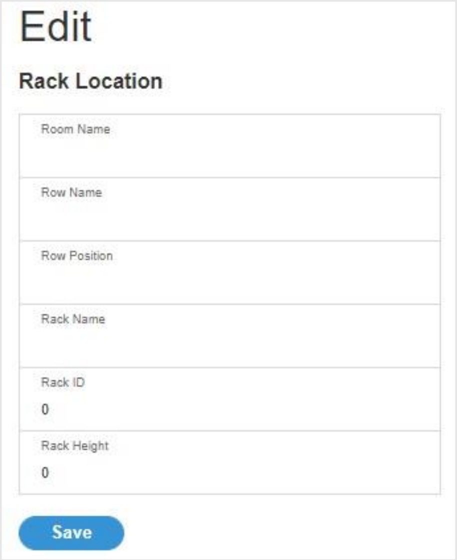
Contact Email
hallo@c.com

Contact Phone
88

Contact Location
b

4. Click on the icon ✎ to edit the Rack Location Information below:

- Enter the **Room Name** to identify the cabinet or room where the PDU is located.
- Enter the **Row Name** where the PDU is located on the rack.
- Enter the **Row Position** where the PDU is located on the rack.
- Enter the **Rack Name** where the PDU is located.
- Enter the **Rack ID** for identification of rack.
- Enter the **Rack Height** where the PDU is located on the rack**.**
- Click **Save** button to complete setting.



Edit

Rack Location

Room Name

Row Name

Row Position

Rack Name

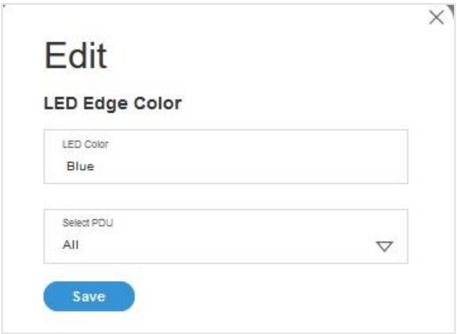
Rack ID
0

Rack Height
0

4. The LED Edge Color can be configured into 7 different colors for the easy identification. The colors are red, blue, white, yellow, green, cyan, and pink.

Click the ✎ icon to edit/change the **LED Edge Color** information below:

- Select the **LED Color**.
- Select **PDU.**

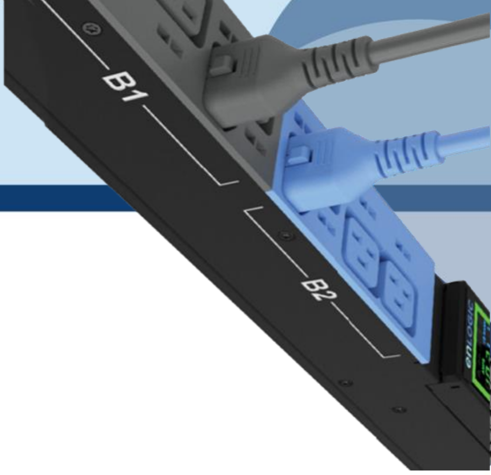


Edit

LED Edge Color

LED Color
Blue

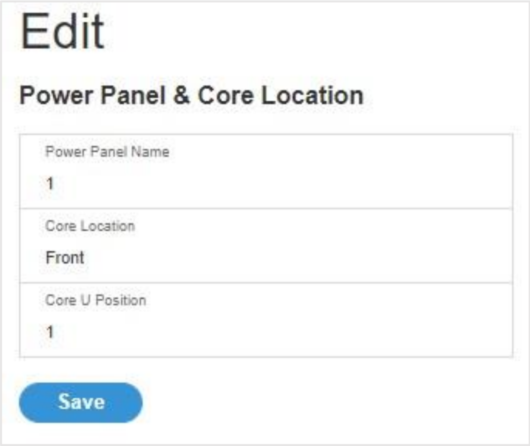
Select PDU
All



5. Click the ✎ icon to edit/change the

   Power Panel & Core Location information below:

   - Enter the **Power Panel Name** to identify the PDU.
   - Select **Core Location** to identify which side the PDU is located **Front** or **Back**
   - Enter **Core U Position** to identify the rack location.
   - Click **Save** button to complete setting.



Edit

Power Panel & Core Location

Power Panel Name
1

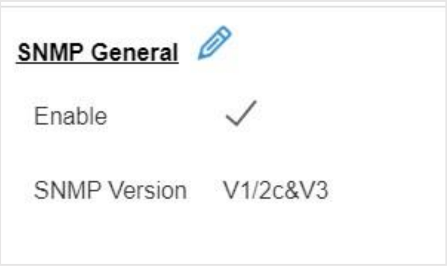
Core Location
Front

Core U Position
1

SNMP Management

This page allows the user to manage the transfer of data from the PDU to the MIB Browser. Simple Network Management Protocol (SNMP) is used to manage the Advantage Secure PDU(s) remotely. SNMP allows the user to monitor and detect PDU faults and to even configure variable data in the PDU.

1. Click on the **Settings** icon to dropdown the Settings menu.
2. Select the **SNMP Manager** to view the information.
3. To access the PDU data inside a MIB Browser.



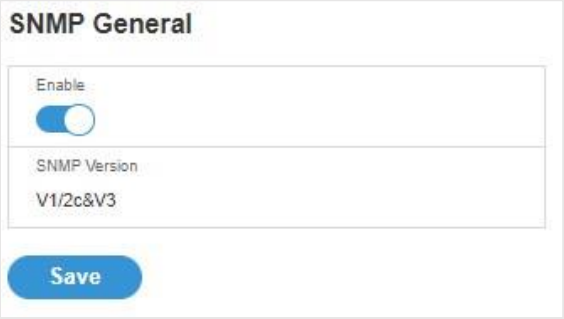
SNMP General ✎

Enable ✓

SNMP Version V1/2c&V3

- Enable the SNMP General

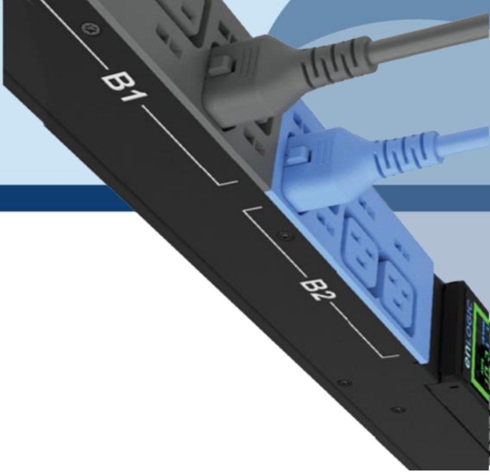
4. Click Save button to complete the settings.



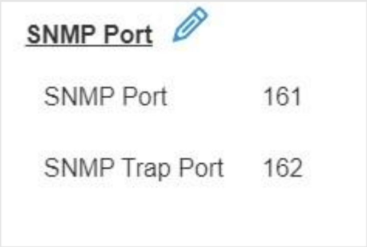
SNMP General

Enable
●

SNMP Version
V1/2c&V3



5. To secure the link between the PDU and the MIB Browser.

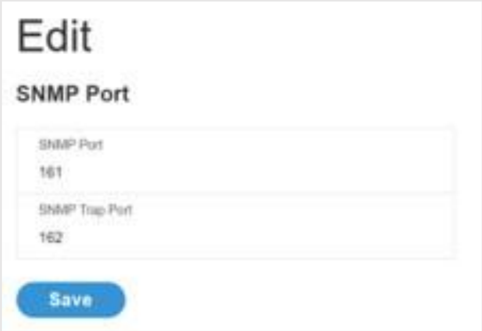


SNMP Port ✎

SNMP Port	161
SNMP Trap Port	162

6. Click the ✎ icon to edit/change the SNMP Port below:

- Enter the **SNMP Port** number.
- Enter the **SNMP Trap Port** number.
- Click **Save** button to complete setting.



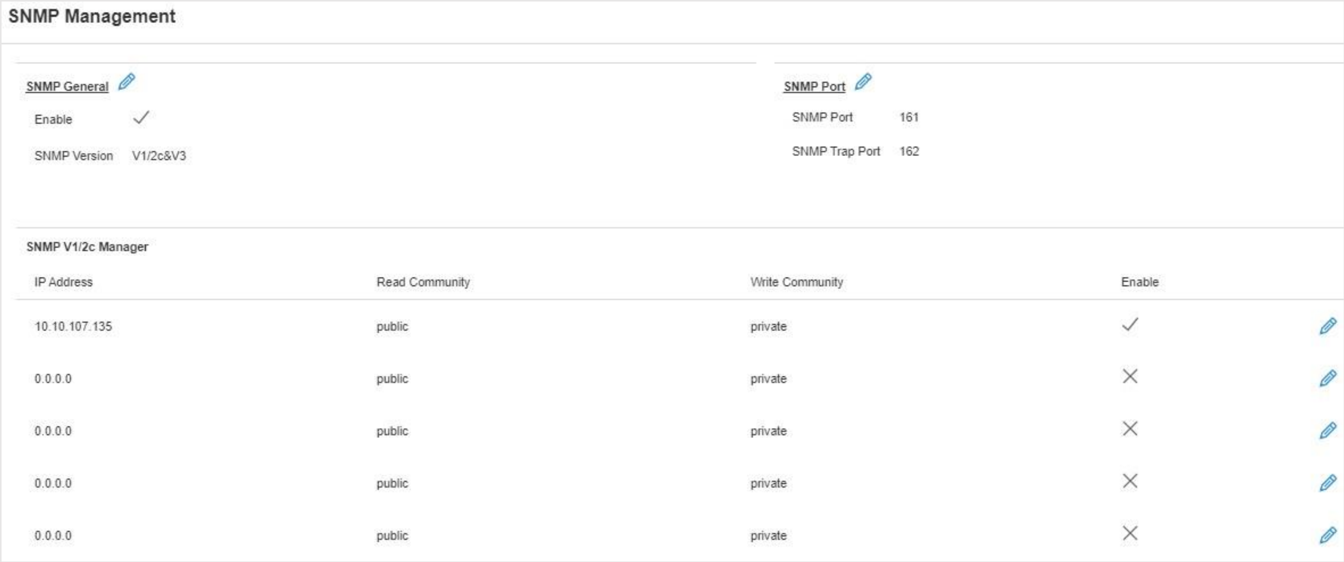
Edit

SNMP Port

SNMP Port
161

SNMP Trap Port
162

7. Configuring Users for SNMP V1/V2c. Click on the icon ✎ to edit/change the SNMP V1/2c Manager below:



SNMP Management

SNMP General ✎

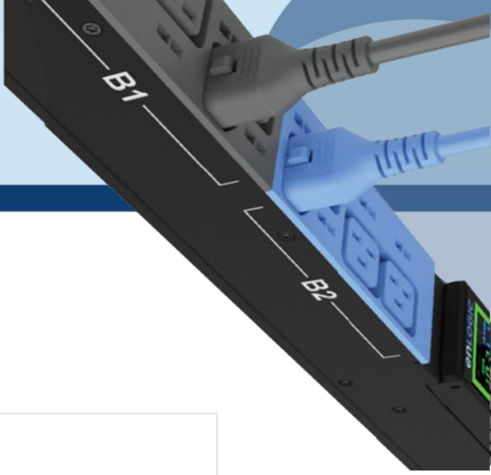
Enable	✓
SNMP Version	V1/2c&V3

SNMP Port ✎

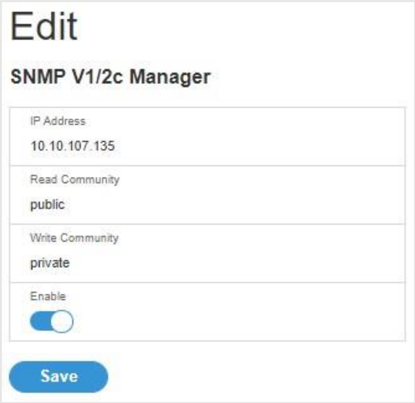
SNMP Port	161
SNMP Trap Port	162

SNMP V1/2c Manager

IP Address	Read Community	Write Community	Enable	
10.10.107.135	public	private	✓	✎
0.0.0.0	public	private	✕	✎
0.0.0.0	public	private	✕	✎
0.0.0.0	public	private	✕	✎
0.0.0.0	public	private	✕	✎



- Enter the **IP Address**.
- Define the security to **public** or **private** in the
  - **Read Community**
  - **Write Community**
- **Enable** the SNMP V1/V2c.
- Click **Save** button to complete setting.



Edit

SNMP V1/2c Manager

IP Address: 10.10.107.135

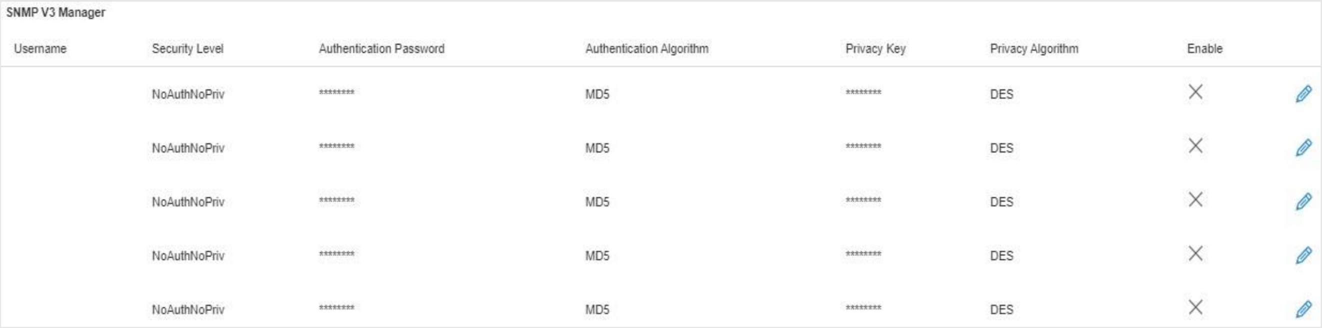
Read Community: public

Write Community: private

Enable: ●

8. Configuring users for SNMP V3 to ensure higher security of data transfer, to the MIB browser.

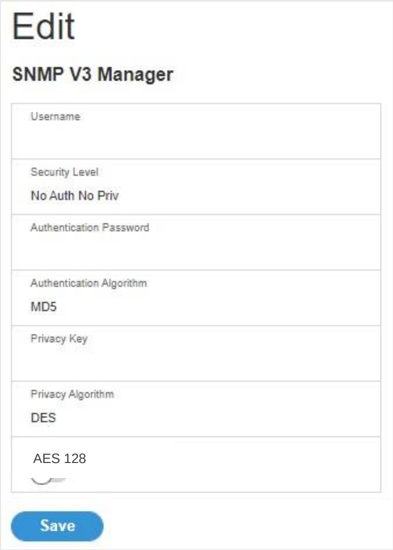
Click on the ✎ icon to edit/change the **SNMP V3 Manager** below:



SNMP V3 Manager

Username	Security Level	Authentication Password	Authentication Algorithm	Privacy Key	Privacy Algorithm	Enable	
	NoAuthNoPriv	********	MD5	********	DES	×	✎
	NoAuthNoPriv	********	MD5	********	DES	×	✎
	NoAuthNoPriv	********	MD5	********	DES	×	✎
	NoAuthNoPriv	********	MD5	********	DES	×	✎
	NoAuthNoPriv	********	MD5	********	DES	×	✎

- **AuthPriv**: Authentication and privacy.
- Type a new unique password as the **Authentication Password**.
- Select the **Authentication Algorithm**.
- **MD5**
- **SHA**
- Type a new unique password as the **Privacy Key**
- Select the **Privacy Algorithm.**
  - **DES**
  - **AES-128**
  - **AES-192**
  - **AES-256**
- **Enable** the SNMP V3.
- Click **Save** button to complete setting.



Edit

SNMP V3 Manager

Username:

Security Level: No Auth No Priv

Authentication Password:

Authentication Algorithm: MD5

Privacy Key:

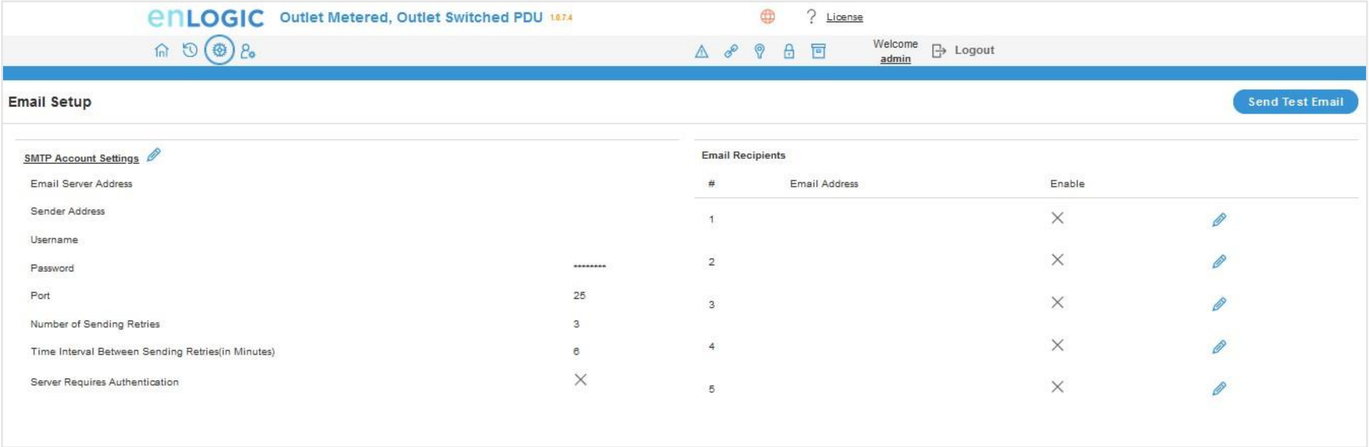
Privacy Algorithm: DES

AES 128 ○

Email Setup

In this page, the user can configure the PDU to send alerts or event messages via email. To do this, the information about the Simple Mail Transfer Protocol (SMTP) server needs to be configured.

1. Click on the **Settings** icon to dropdown the Settings menu.
2. Select the **Email Setup** to view the information.



Email Setup

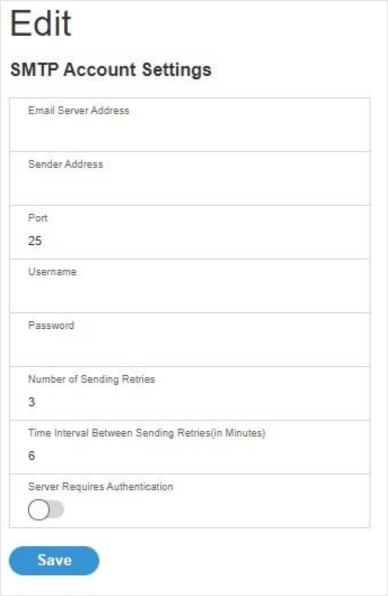
SMTP Account Settings ✎

Email Server Address	
Sender Address	
Username	
Password	********
Port	25
Number of Sending Retries	3
Time Interval Between Sending Retries(in Minutes)	6
Server Requires Authentication	✕

Email Recipients

#	Email Address	Enable	
1		✕	✎
2		✕	✎
3		✕	✎
4		✕	✎
5		✕	✎

3. To set the SMTP server settings to receive Emails and notifications.
   Click the ✎ icon to edit/change the **SMTP Account Settings** below:



Edit

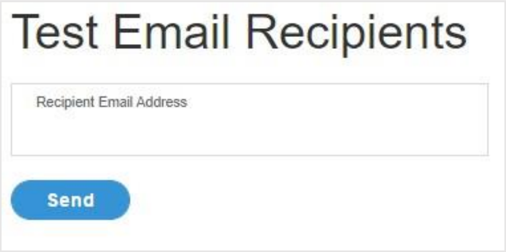
SMTP Account Settings

Email Server Address	
Sender Address	
Port	25
Username	
Password	
Number of Sending Retries	3
Time Interval Between Sending Retries(in Minutes)	6
Server Requires Authentication	○

- Enter the **Email Server Address**, which is the IP address or Fully qualified Domain Name of the SMTP server to route the emails to the recipient.
- Enter the **Sender Address**, which is the email address that the email is sent **From**.
- Configure the **Port** number, which is the communication endpoint on the server. The default is **25**.
- Enter the **Username** for SMTP security.
- Enter the **Password** for SMTP security.
- Assign the **Number of Sending Retries**, which is the number of times the PDU will attempt to resend a message if the message fails. The default is **3**.
- Type the **Time Interval Between Sending Retries** (in minutes). The default is **6** minutes.
- Enable the **Server Requires Authentication** to password protect the SMTP.
- Click **Save** button to complete setting.

On the top- right side of the Email Setup page, Click the below options as required:

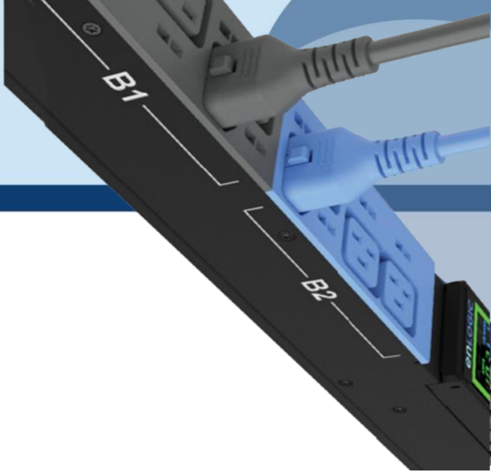
Send Test Email



Test Email Recipients

This button allows us to send a test mail to check if the feature is active or not.

- Enter the **Recipient Email Address**.
- Click the **Send** button to send the Email.



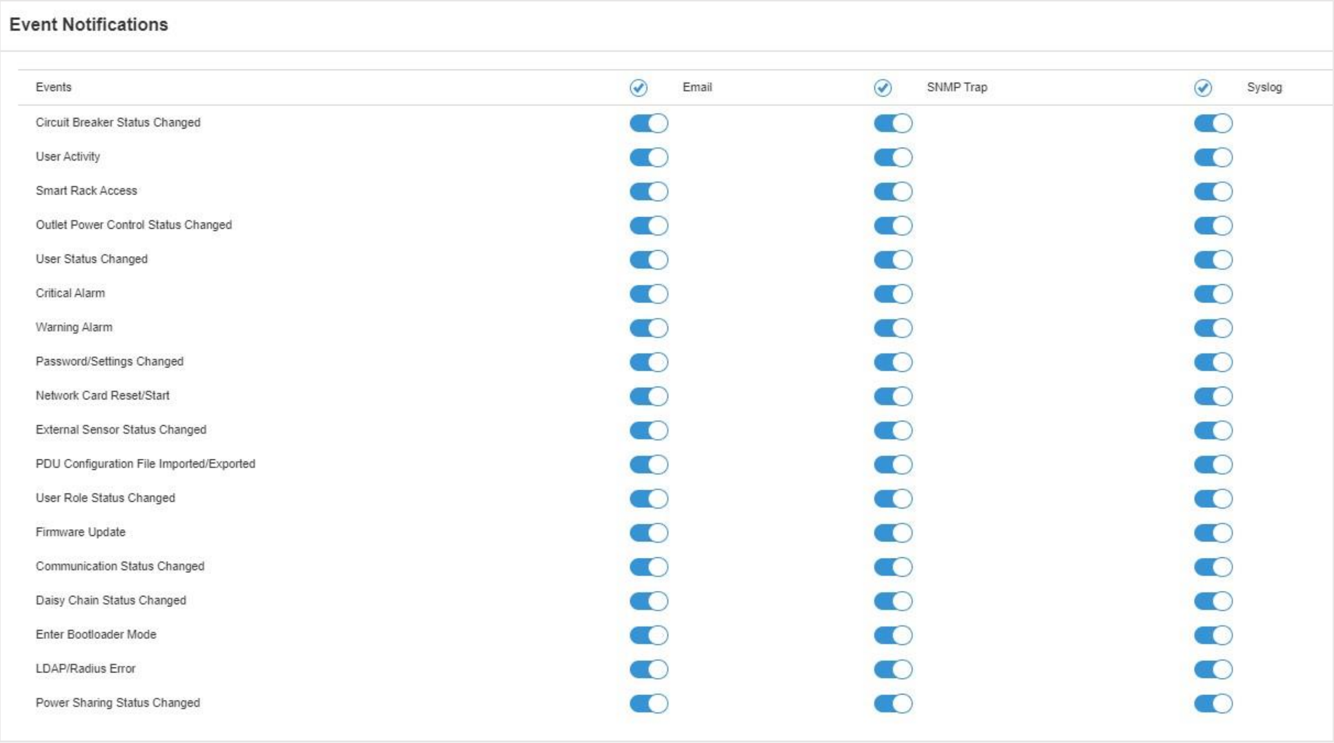
Event Notifications

In this page the user can assign the Event notifications from the PDU to the Syslog, SNMP Trap, and Email.

An event notification has two parts:

- Event: the situation where the PDU meets certain condition (i.e., temperature sensor exceeds the warning limit. Or circuit breaker status is changed).
- Action: the response to the event (i.e., send an SMTP message and SNMP trap).

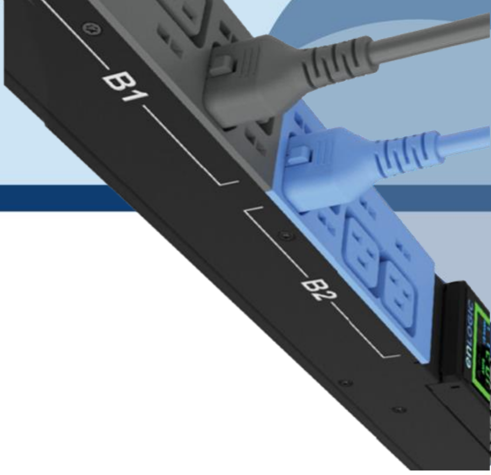
1. Click on the **Settings** icon to dropdown the Settings menu.
2. Select **Event Notifications** to view information.
3. **Enable** the **Email**, **SNMP Trap** and **Syslog** to the respective Events to receive notification.



Event Notifications

Events	✓ Email	✓ SNMP Trap	✓ Syslog
Circuit Breaker Status Changed	●	●	●
User Activity	●	●	●
Smart Rack Access	●	●	●
Outlet Power Control Status Changed	●	●	●
User Status Changed	●	●	●
Critical Alarm	●	●	●
Warning Alarm	●	●	●
Password/Settings Changed	●	●	●
Network Card Reset/Start	●	●	●
External Sensor Status Changed	●	●	●
PDU Configuration File Imported/Exported	●	●	●
User Role Status Changed	●	●	●
Firmware Update	●	●	●
Communication Status Changed	●	●	●
Daisy Chain Status Changed	●	●	●
Enter Bootloader Mode	●	●	●
LDAP/Radius Error	●	●	●
Power Sharing Status Changed	●	●	●

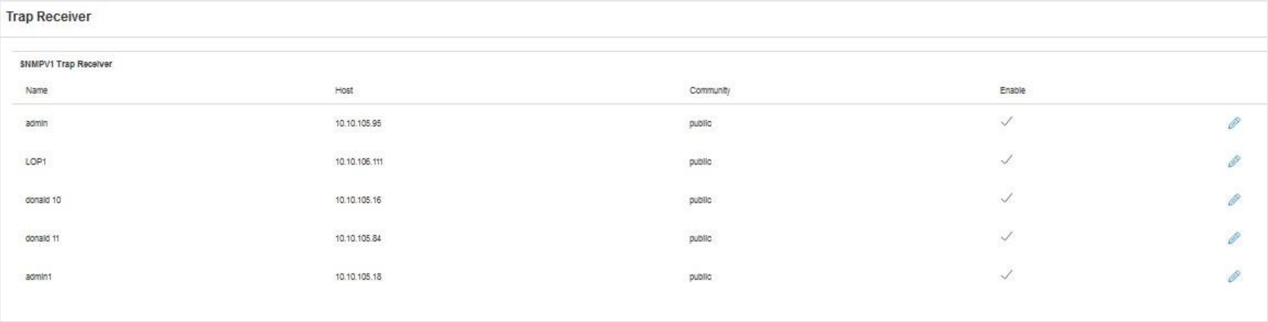
The Critical and Warning Alarms are enabled at the SNMP Trap, as default. The notifications for these default events enabled, can only be received after the configuration of **Traps Receiver**.



Trap Receiver

This page allows us to configure the Trap receiver by typing in name, host, and community. Typically, the Read Community and Write Community are public.

1. Click on the **Settings** icon to dropdown the Settings menu.
2. Select **Trap Receiver** to view information.
3. Configuring users for SNMP V1 Trap Settings that allows the communication to the MIB browser.



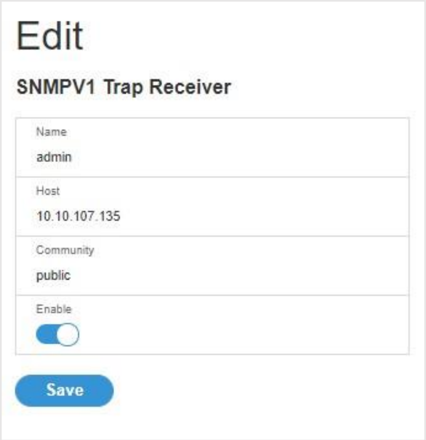
Trap Receiver

SNMPV1 Trap Receiver

Name	Host	Community	Enable	
admin	10.10.105.95	public	✓	✎
LOP1	10.10.106.111	public	✓	✎
donald 10	10.10.105.16	public	✓	✎
donald 11	10.10.105.84	public	✓	✎
admin1	10.10.105.18	public	✓	✎

Click on the ✎ icon to edit/change the **SNMP V1 Trap Receiver** settings below:

- Enter the **Name**, which allows us to identify the different receivers.
- Enter the **Host** IP address to which the traps are sent.
- Assign the **Community** to **public** or **private** security.
- **Enable** the SNMP V1.
- Click **Save** to complete the settings.



Edit

SNMPV1 Trap Receiver

Name: admin

Host: 10.10.107.135

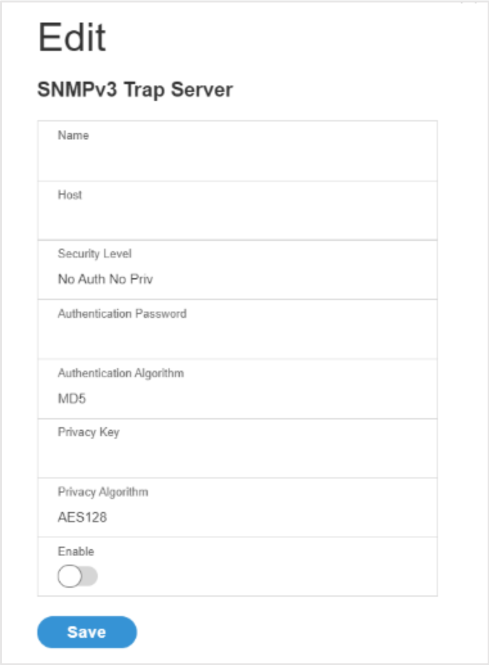
Community: public

Enable: ●

4. Configuring users for SNMP V3 Trap Settings that allows for encrypted communication to the MIB browser.

Click the ✎ icon to edit/change the **SNMP V3 Trap Server** settings below,

- Enter the **Name**, which allows us to identify the different receivers.
- Enter the **Host** IP address to which the traps are sent.
- Assign the **Security Level** from the dropdown menu.
- **NoAuthNoPriv**: No authentication and no privacy. This is the default.
- **AuthNoPriv**: Authentication and no privacy.
- **AuthPriv**: Authentication and privacy.
- Type a new unique password as the **Authentication Password**.
- Select the **Authentication Algorithm**.
    - **MD5**
    - **SHA**
- Type a new unique password as the **Privacy Key**.
- Select the **Privacy Algorithm.**
    - DES
    - AES-128
    - AES-192
    - AES-256
- **Enable** the SNMP V3
- **Click Save button to complete settings.**



Edit

SNMPv3 Trap Server

Name

Host

Security Level
No Auth No Priv

Authentication Password

Authentication Algorithm
MD5

Privacy Key

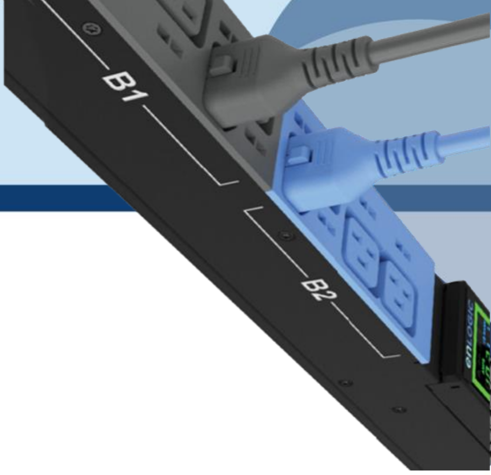
Privacy Algorithm
AES128

Enable
○

Save

On the top-right side of the Email Setup page, Click the below options as required:

- **Send Test Trap -** This button allows us to send a test Trap to check if the feature is active or not.



Defining Thresholds

The Thresholds are limits, defined by the user over parameters like power, phase, circuit breaker and sensor to send alert notifications when the value crosses above or below the limit.

To access the PDU Thresholds page,

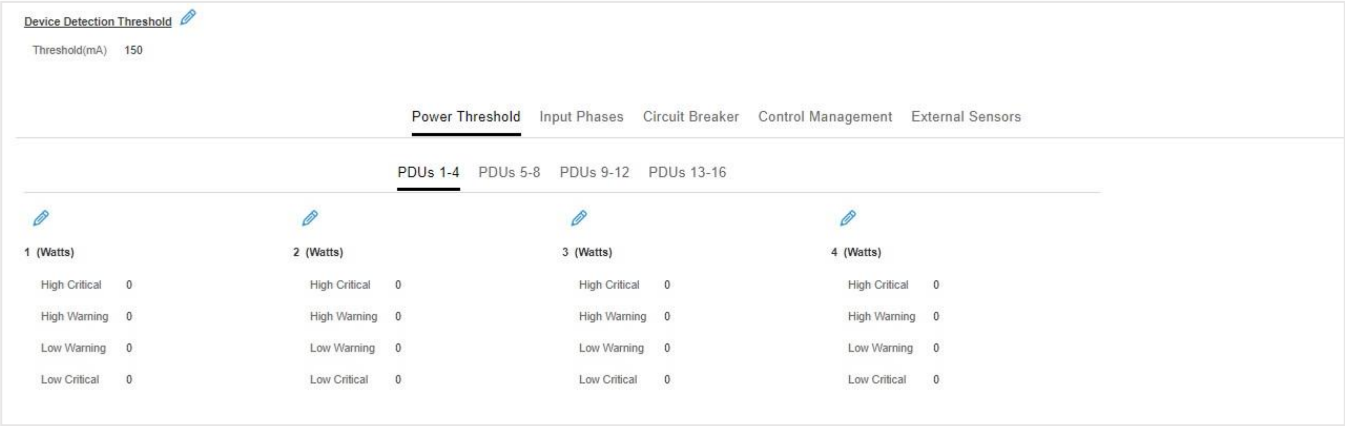
1. Click on the **Settings** icon to dropdown the Settings menu.
2. Select **Thresholds** to view information.

Power Thresholds

The PDU will send alert notifications when a power threshold wattage crosses above or below the settings you specify in the Power Threshold.

Below are the steps to change the Power Thresholds settings and alarm notifications,

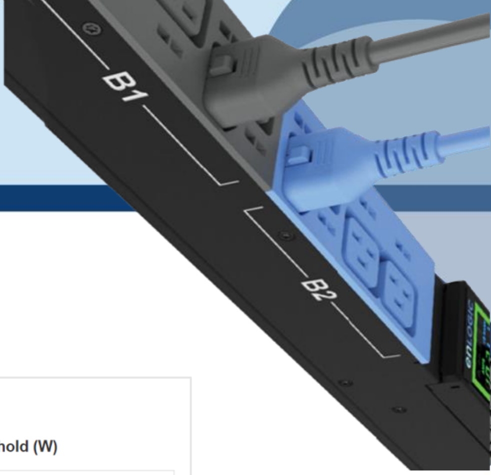
1. Choose **Power Threshold** tab in the PDU Threshold page.
2. Click ✎ icon edit/change the Power Threshold Setting.



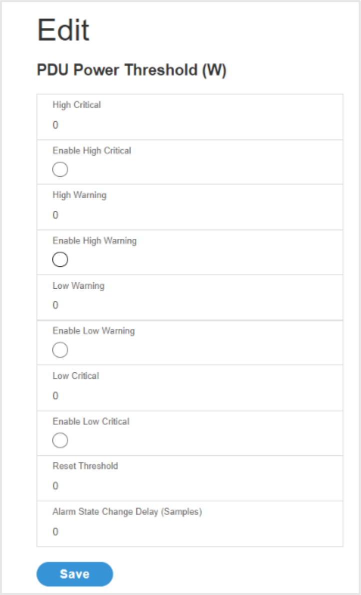
Device Detection Threshold ✎

Threshold(mA) 150

1 (Watts)		2 (Watts)		3 (Watts)		4 (Watts)	
High Critical	0	High Critical	0	High Critical	0	High Critical	0
High Warning	0	High Warning	0	High Warning	0	High Warning	0
Low Warning	0	Low Warning	0	Low Warning	0	Low Warning	0
Low Critical	0	Low Critical	0	Low Critical	0	Low Critical	0



3. In the **PDU Power Threshold Setting** dialog boxes, change the fields as needed:
    a. Low Critical (W)
    b. Low Warning (W)
    c. High Warning (W)
    d. High Critical (W)
    e. Reset Threshold (W)
    f. Alarm State Change Delay (samples)
4. Click **Save** button to complete the setting.
5. Repeat the steps for all PDUs.



Edit

PDU Power Threshold (W)

High Critical
0

Enable High Critical
○

High Warning
0

Enable High Warning
○

Low Warning
0

Enable Low Warning
○

Low Critical
0

Enable Low Critical
○

Reset Threshold
0

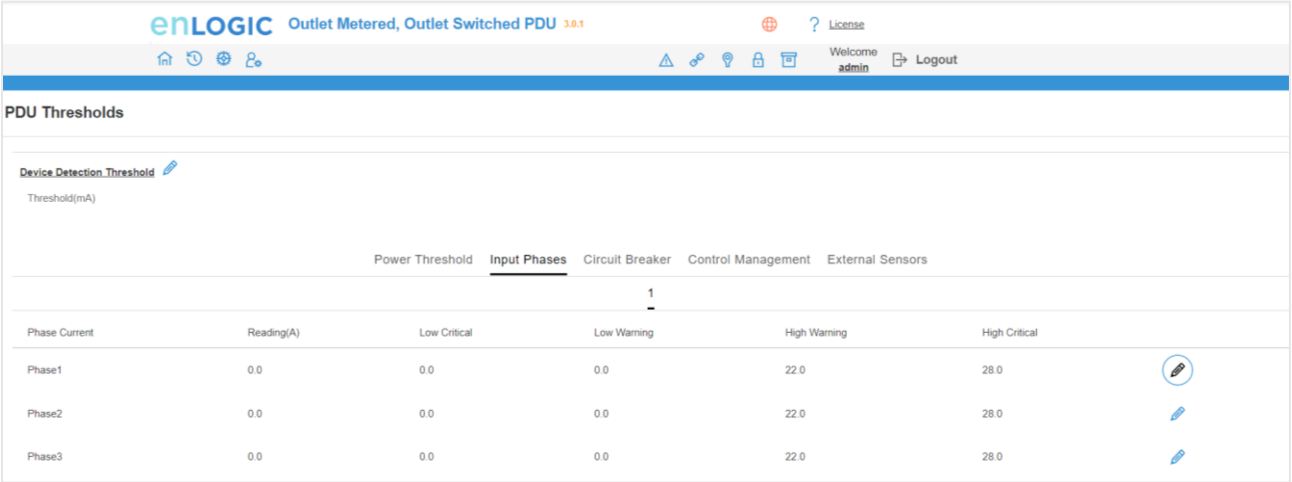
Alarm State Change Delay (Samples)
0

Input Phases

The PDU will send alert notifications when a phase current and voltage alarm crosses above or below the settings you specify in the Input Phase Threshold.

Below are the steps to change the Input Phase Settings and alarm notifications,

1. Choose the **Input Phases** tab in the PDU Threshold page.
2. Click ✎ icon to edit/change the Phase Current Settings.



PDU Thresholds

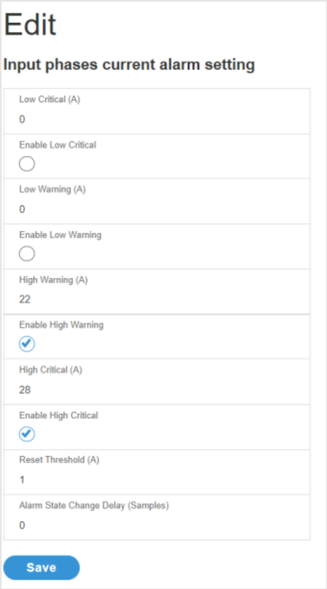
Device Detection Threshold ✎

Threshold(mA)

Phase Current	Reading(A)	Low Critical	Low Warning	High Warning	High Critical	
Phase1	0.0	0.0	0.0	22.0	28.0	✎
Phase2	0.0	0.0	0.0	22.0	28.0	✎
Phase3	0.0	0.0	0.0	22.0	28.0	✎

3. In the **Input Phase Current Alarm Setting** dialog boxes, change the fields as needed:
   - Low Critical (A)
   - Low Warning (A)
   - High Warning (A)
   - High Critical (A)
   - Reset Threshold (A)
   - Alarm State Change Delay (samples)

4. Click **Save** button to complete the setting
5. Repeat Steps 1 to 4 for all PDUs
6. Click on the ✎ icon to edit/change the Phase Voltage Settings



Edit

Input phases current alarm setting

Low Critical (A)
0

Enable Low Critical
○

Low Warning (A)
0

Enable Low Warning
○

High Warning (A)
22

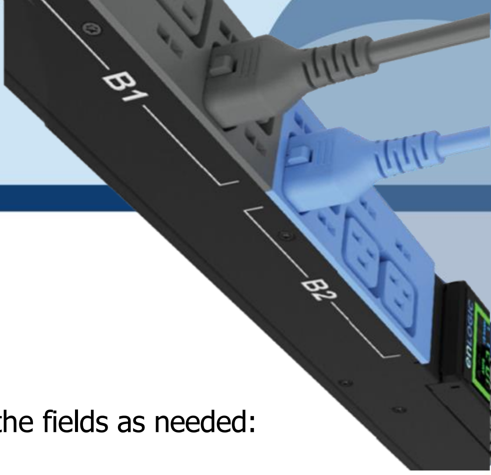
Enable High Warning
✓

High Critical (A)
28

Enable High Critical
✓

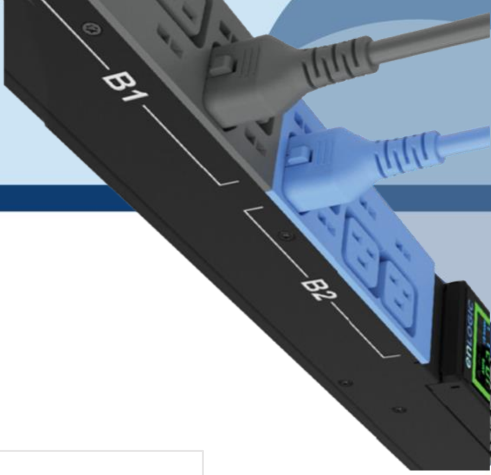
Reset Threshold (A)
1

Alarm State Change Delay (Samples)
0



7. In the **Input Phase Voltage Alarm Setting** dialog boxes, change the fields as needed:
   - Low Critical (V)
   - Low Warning (V)
   - High Warning (V)
   - High Critical (V)
   - Reset Threshold (V)
   - Alarm State Change Delay (samples)

8. Click **Save** button to complete the setting.
9. Repeat the steps for all PDUs.

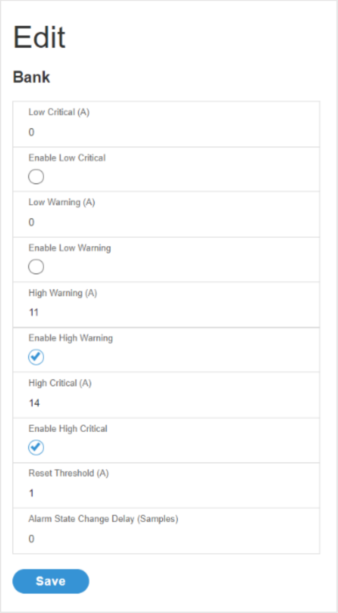


Circuit Breaker

The PDU will send alert notifications when a circuit breaker amperage crosses above or below the settings you specify in the Circuit Breaker Threshold.

Below are the steps to change the Circuit Breaker Settings and alarm notifications,

1. Choose the **Circuit Breaker** tab in the PDU Threshold page.
   - Low Critical (A)
   - Warning Thresholds
   - High Warning (A)
   - High Critical (A)
   - Reset Threshold (A)
   - Alarm State Change Delay (samples)



Edit

Bank

Low Critical (A)
0

Enable Low Critical
○

Low Warning (A)
0

Enable Low Warning
○

High Warning (A)
11

Enable High Warning
✓

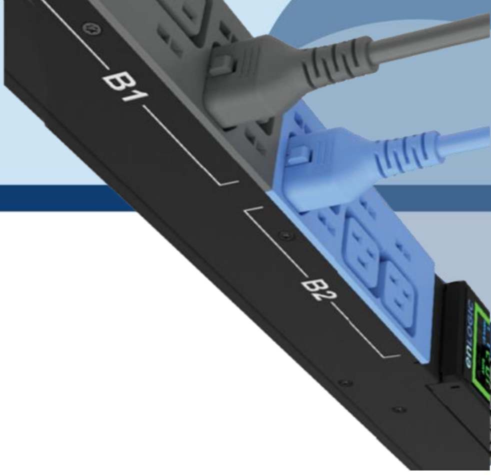
High Critical (A)
14

Enable High Critical
✓

Reset Threshold (A)
1

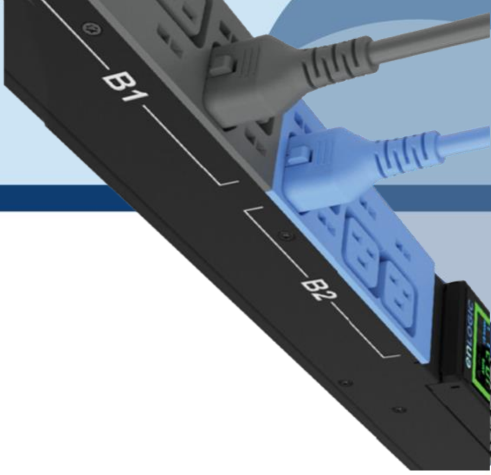
Alarm State Change Delay (Samples)
0

2. Click **Save** button to complete the setting.
3. Repeat the steps for all PDUs.



Circuit Breaker List

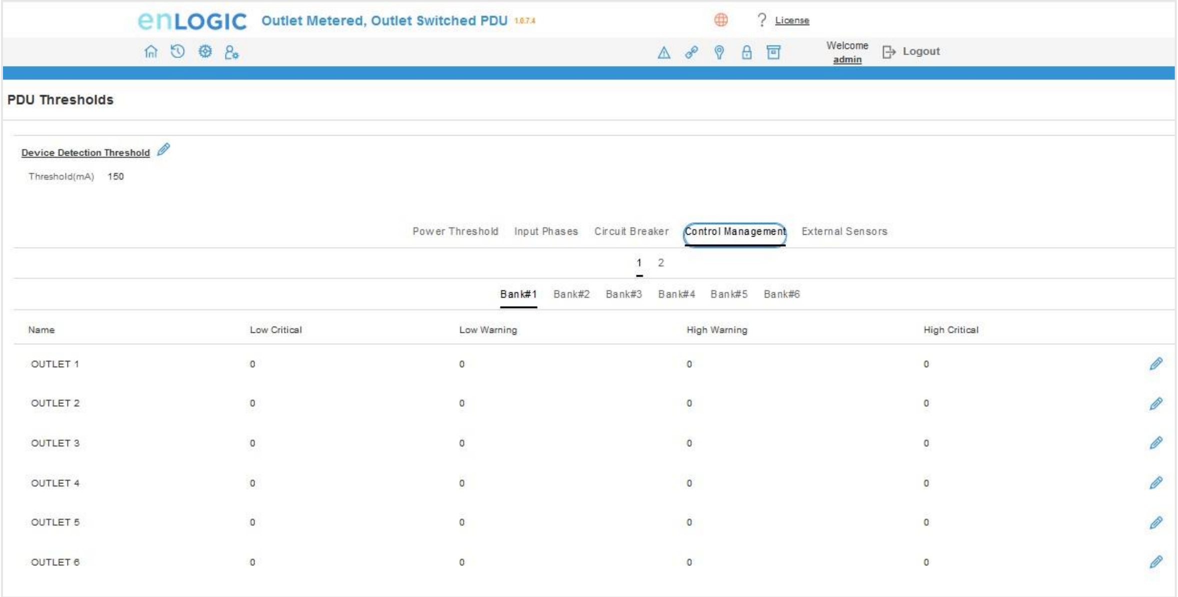
PN	Manufacturer	Manufacturer Part Number	Amperage	AIC	Application
810-00975	BSB	B3D1-16.0-240-1500B-A2-C1-G-K	16A,1P	5KA	Vertical
810-00977	BSB	B3D1-20.0-240-1500B-A2-C1-G-K	20A,1P	5KA	Vertical
810-00976	BSB	B3D1-20.0-240-2520B-A2-C1-G-K	20A,2P	5KA	Vertical
810-00980	BSB	B2R1-16.0-250-1200B-A2-F2-K-C	16A,1P	5KA	Horizontal
810-00978	BSB	B2R1-16.0-250-1300B-A2-F2-K-C	16A,1P	5KA	Vertical
810-00981	BSB	B2R1-20.0-250-1200B-A2-F2-K-C	20A,1P	5KA	Horizontal
810-01151	BSB	B2R6-20.0/127-1300B-A2-F1-K-K	20A,1P	5KA	Vertical
810-00982	BSB	B2R1-20.0-250-2220B-A2-F2-K-C	20A,2P	5KA	Horizontal
810-00979	BSB	B2R1-20.0-250-2320B-A2-F2-K-C	20A,2P	5KA	Vertical
810-01203	BSB	B3H3-20.0/240-1100B-A2-F2-G-K	20A,1P	10KA	Vertical
810-01204	BSB	B3H3-20.0/240S-2100B-A2-F2-G-K	20A,2P	10KA	Vertical
810-01205	BSB	B3H3-16.0/240-1100B-A2-F2-G-K	16A,1P	10KA	Vertical
810-01206	BSB	B2HR6-16.0/240-1A00B-A2-F1-K-K	16A,1P	10KA	Vertical
810-01207	BSB	B2HR6-20.0/240-1A00B-A2-F1-K-K	20A,1P	10KA	Vertical
810-01208	BSB	B2HR6-20.0/240-2A20B-A2-F1-K-K	20A,2P	10KA	Vertical
810-01209	BSB	B2HE4-16.0/240-1200B-A2-F1-K-K	16A,1P	10KA	Horizontal
810-01210	BSB	B2HE4-20.0/240-1200B-A2-F1-K-K	20A,1P	10KA	Horizontal
810-01211	BSB	B2HE4-20.0/240-2230B-A2-F1-K-K	20A,2P	10KA	Horizontal



Control Management

The PDU will send alert notifications when an outlet wattage crosses above or below the settings you specify in the Control Management Threshold.

1. Choose the **Control Management** tab in the PDU Threshold page.



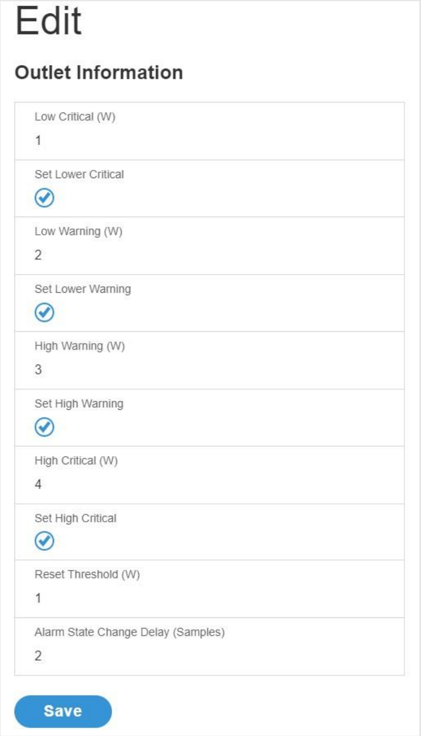
PDU Thresholds

Device Detection Threshold

Threshold(mA) 150

Name	Low Critical	Low Warning	High Warning	High Critical
OUTLET 1	0	0	0	0
OUTLET 2	0	0	0	0
OUTLET 3	0	0	0	0
OUTLET 4	0	0	0	0
OUTLET 5	0	0	0	0
OUTLET 6	0	0	0	0

2. Click ✎ icon to edit/change the Control Management Settings,
   - Low Critical (W)
   - Low Warning (W)
   - High Warning (W)
   - High Critical (W)
   - Reset Threshold (W)
   - Alarm State Change Delay (samples)
3. Click **Save** button to complete the setting.
4. Repeat the steps for all PDUs.



Edit

Outlet Information

Low Critical (W)
1

Set Lower Critical
✓

Low Warning (W)
2

Set Lower Warning
✓

High Warning (W)
3

Set High Warning
✓

High Critical (W)
4

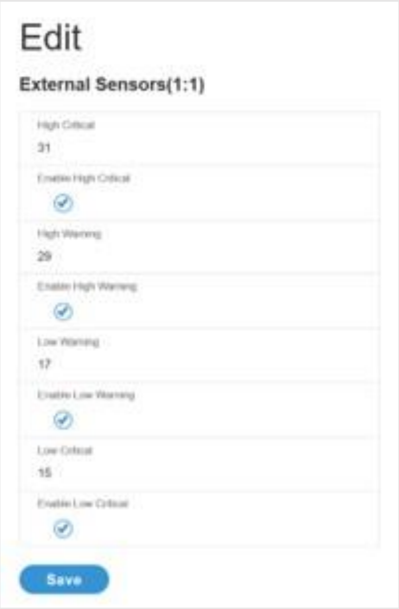
Set High Critical
✓

Reset Threshold (W)
1

Alarm State Change Delay (Samples)
2

The PDU will communicate about the sensor location, alarms, notifications, and details. The External Sensors section displays the connected sensors on the PDU. Choose the External Sensors tab PDU Threshold page.

1. Choose the **External Sensors** tab in the PDU Threshold page
2. Click ✎ icon to edit/change the External Sensors Settings,
   - Low Critical
   - Low Warning
   - High Warning
   - High Critical
3. Click **Save** button to complete the setting.
4. Repeat the steps for all PDUs.



Edit

External Sensors(1:1)

High Critical
31

Enable High Critical
☑

High Warning
29

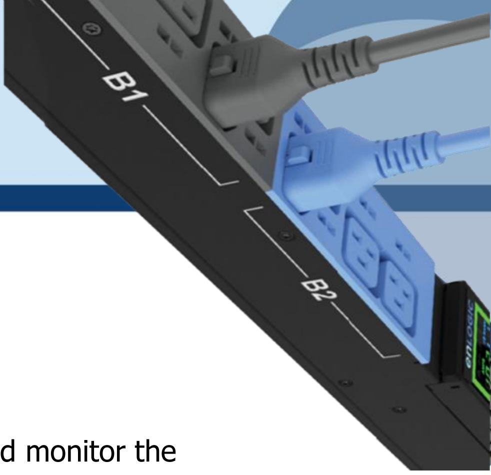
Enable High Warning
☑

Low Warning
17

Enable Low Warning
☑

Low Critical
15

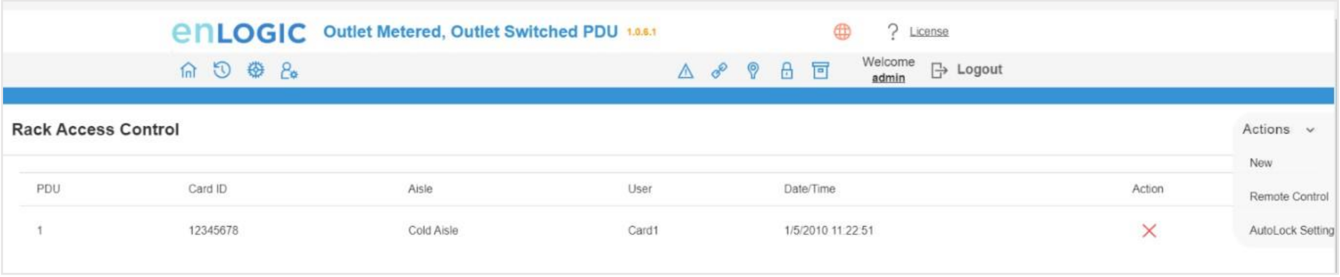
Enable Low Critical
☑



Rack Access Control

This page allows you to configure the Rack Access functions to control and monitor the Racks.

1. Click on the **Settings** icon to dropdown the Settings menu.
2. Select **Rack Access Control** to view information.



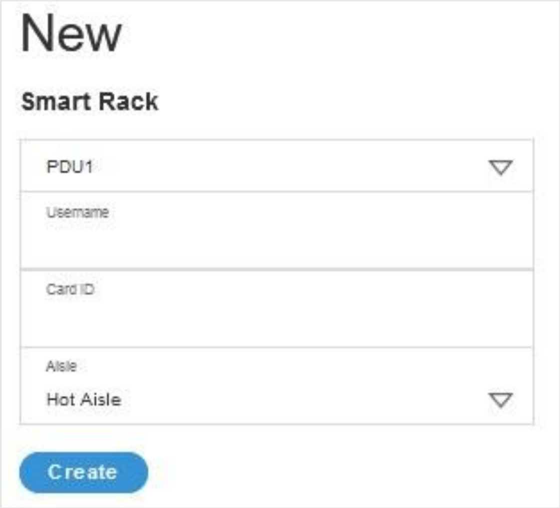
Rack Access Control

PDU	Card ID	Aisle	User	Date/Time	Action
1	12345678	Cold Aisle	Card1	1/5/2010 11:22:51	✕

On the top- right side of the Rack Access Control page, Click the below options as required:

- **Actions**
- **New**

To Assign new Rack Access to the PDU



New

Smart Rack

PDU1

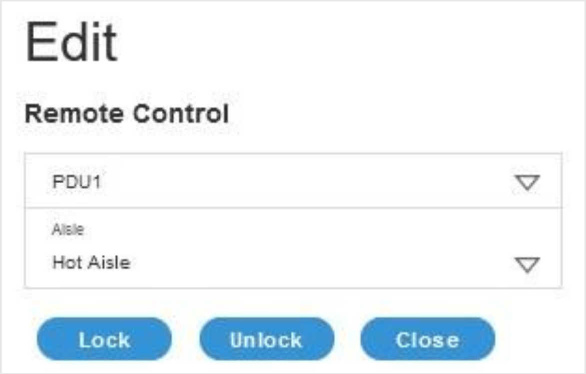
Username

Card ID

Aisle: Hot Aisle

Remote Control

Used to perform Lock, Unlock and Close functions.



Edit

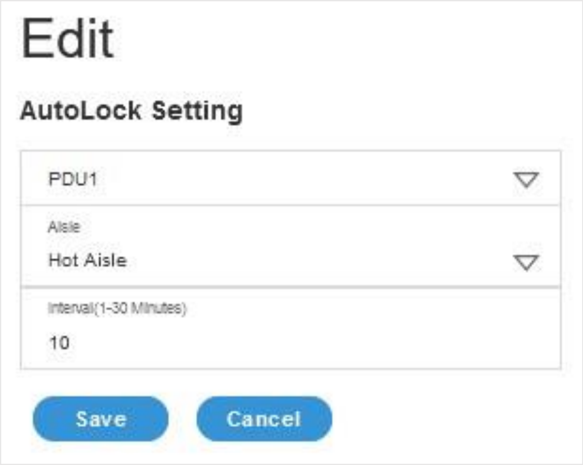
Remote Control

PDU1

Aisle: Hot Aisle

AutoLock Settings

To assign Automatic locking functions within a time limit to the PDU



Edit

AutoLock Setting

PDU1

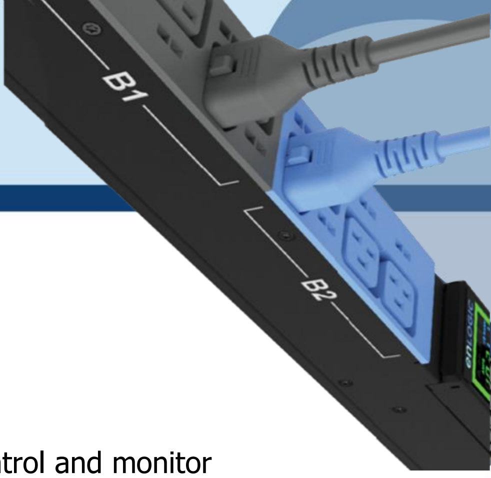
Aisle: Hot Aisle

Interval(1-30 Minutes): 10

Handle and Compatible Card Types

Below are the card lists which are supported on the different swing handle,

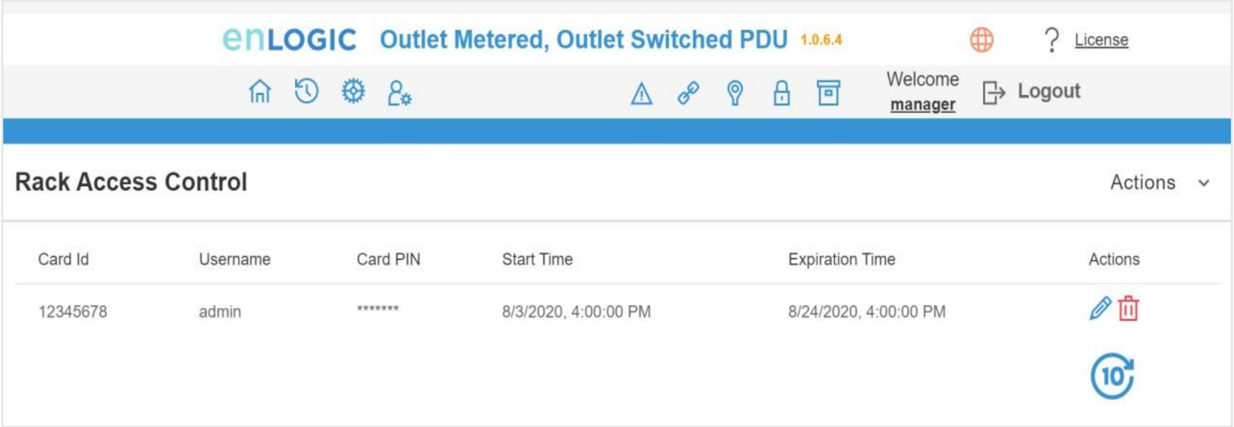
1. MYFARE® Classic 4K
2. MYFARE® Plus 2K
3. MYFARE® DESFire 4K
4. HID® iCLASS



Smart Rack Control

This page allows you to configure the Smart Rack Access functions to control and monitor the Racks. It is used to set up the access control server door Handle (above 4 Handles and Compatible Cards). So, the user can use the editing option to modify the data as required. A total of 200 cards are compatible with the smart rack control.

1. Click on the **Settings** icon to dropdown the Settings menu.
2. Select **Smart Rack Control** to view information.

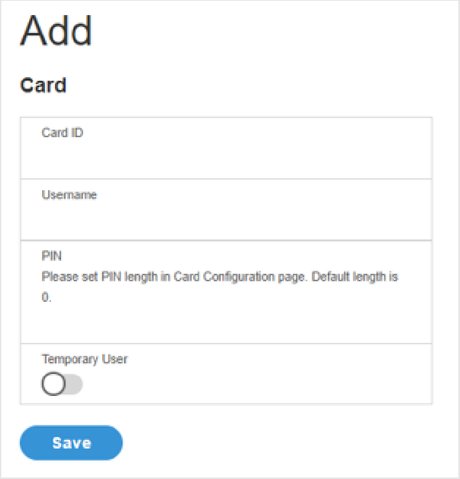


Rack Access Control

Card Id	Username	Card PIN	Start Time	Expiration Time	Actions
12345678	admin	*******	8/3/2020, 4:00:00 PM	8/24/2020, 4:00:00 PM	

3. Click icon to edit/change the Rack Access Control Settings

- Enter the **Card ID** to ensure security and restrictive access.
- Enter **Username** of the card holder.
- Enter **PIN** (as set in card configuration page).
- Enable or Disable **Temporary User** as per user status
- Click **Save** button to complete setting.


Add

Card

Card ID

Username

PIN
Please set PIN length in Card Configuration page. Default length is 0.

Temporary User

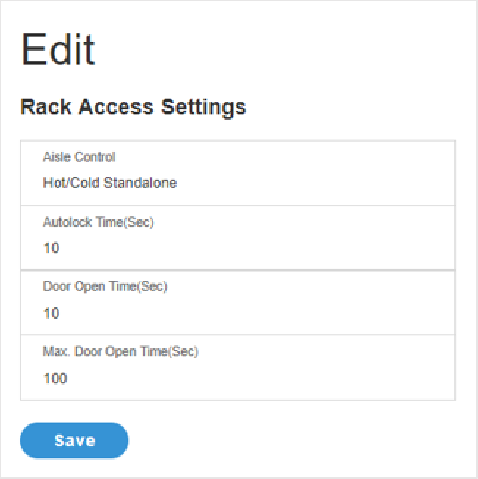
4. On the top-right side of the Rack Access Control page, Click the below options as required:

Action

5. On the top-right side of the Rack Access Control page, click the below options as required. Click on the Actions, Edit button

6. To add card details, select **Add Card**.
    - Enter the **Card ID**
    - Enter **Username** of the card holder.
    - Enter **PIN** (as set in card configuration page)
    - Enable or Disable **Temporary User** as per user status
    - Click **Save** button to complete setting.

7. To edit rack access details, select **Rack Access Settings**.
    - Select **Aisle Control** to **Standalone** or **Combined** as per rack.
    - Set **Autolock Time**.
    - Set **Door Open Time**.
    - Set **Max Door Open Time**.
    - Select the access type in **Work Mode**.
    - Click **Save** button to complete setting.



Edit

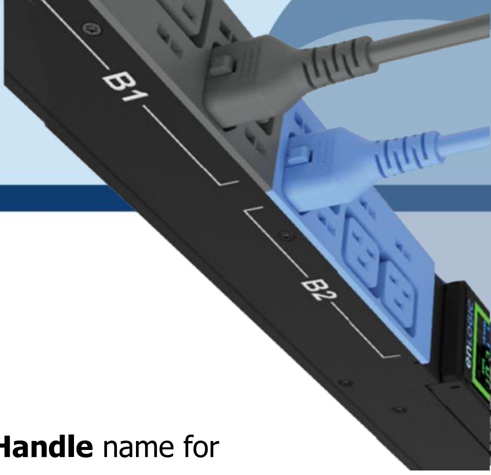
Rack Access Settings

Aisle Control
Hot/Cold Standalone

Autolock Time(Sec)
10

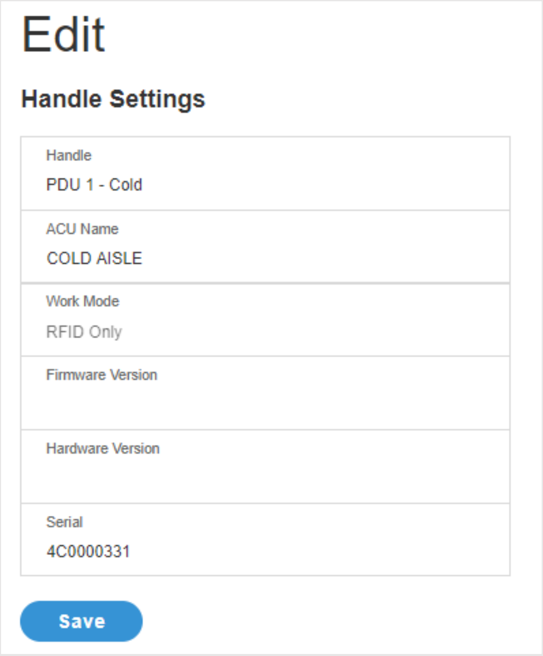
Door Open Time(Sec)
10

Max. Door Open Time(Sec)
100



8. To edit handle settings, select **Rack Access Settings**. – Enter **Handle** name for identification.

- Enter **ACU Name** for identification.
- The **Firmware Version** and **Hardware Version** are non-editable fields and are filled by default in their respective Versions.
- Enter **Serial** number of the handle. Click **Save** button to complete setting.



Edit

Handle Settings

Handle: PDU 1 - Cold

ACU Name: COLD AISLE

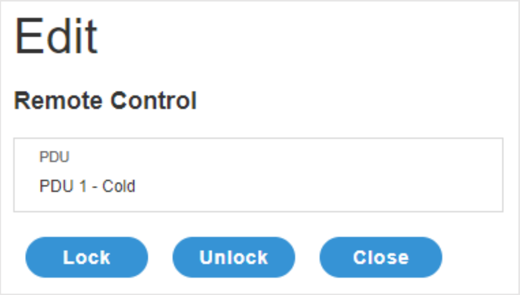
Work Mode: RFID Only

Firmware Version:

Hardware Version:

Serial: 4C0000331

9. Select **Remote Control** to perform **Lock**, **Unlock** and **Close** functions.

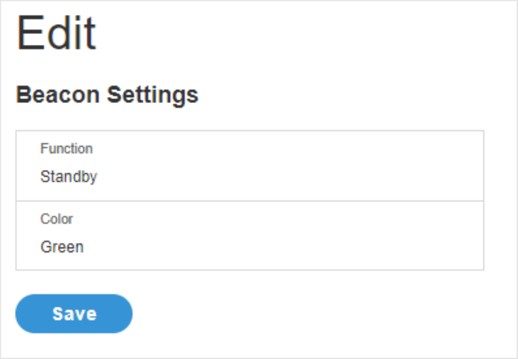


Edit

Remote Control

PDU: PDU 1 - Cold

10. Select **Beacon Settings** to **Enable Beacon** Lock and **Color**. Click **Save** button to complete setting.

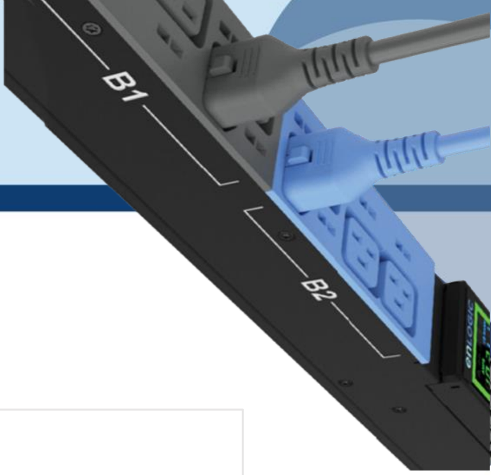


Edit

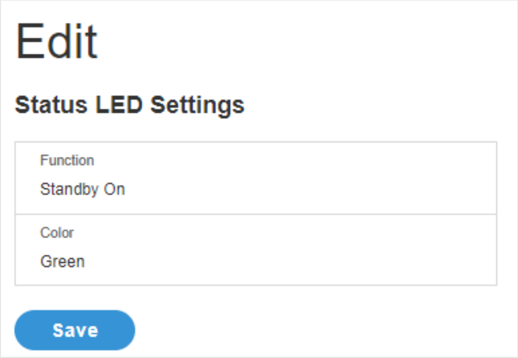
Beacon Settings

Function: Standby

Color: Green



11. Select **Status LED Settings** to configure **Function** and **Color** of the LED. Click **Save** button to complete setting.



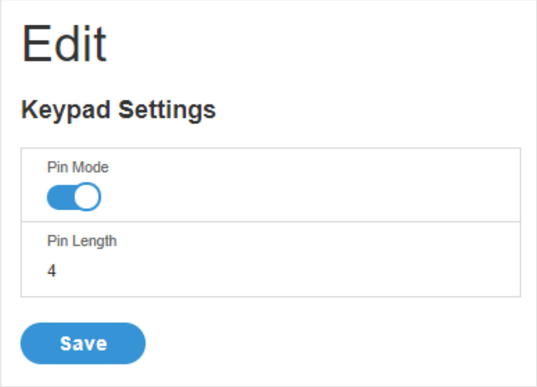
Edit

Status LED Settings

Function
Standby On

Color
Green

12. Select **Sensor Harness Configuration** to configure the sensor harness. Click **Save** button to complete setting.

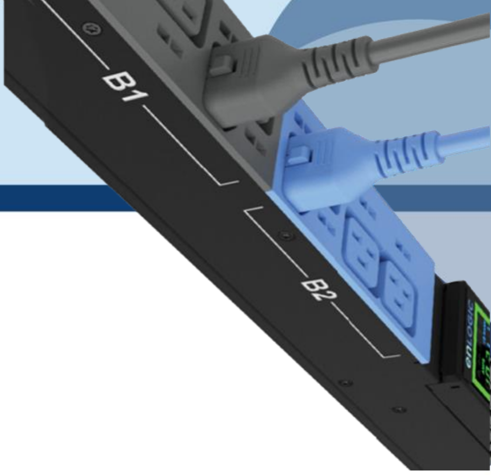


Edit

Keypad Settings

Pin Mode
●

Pin Length
4



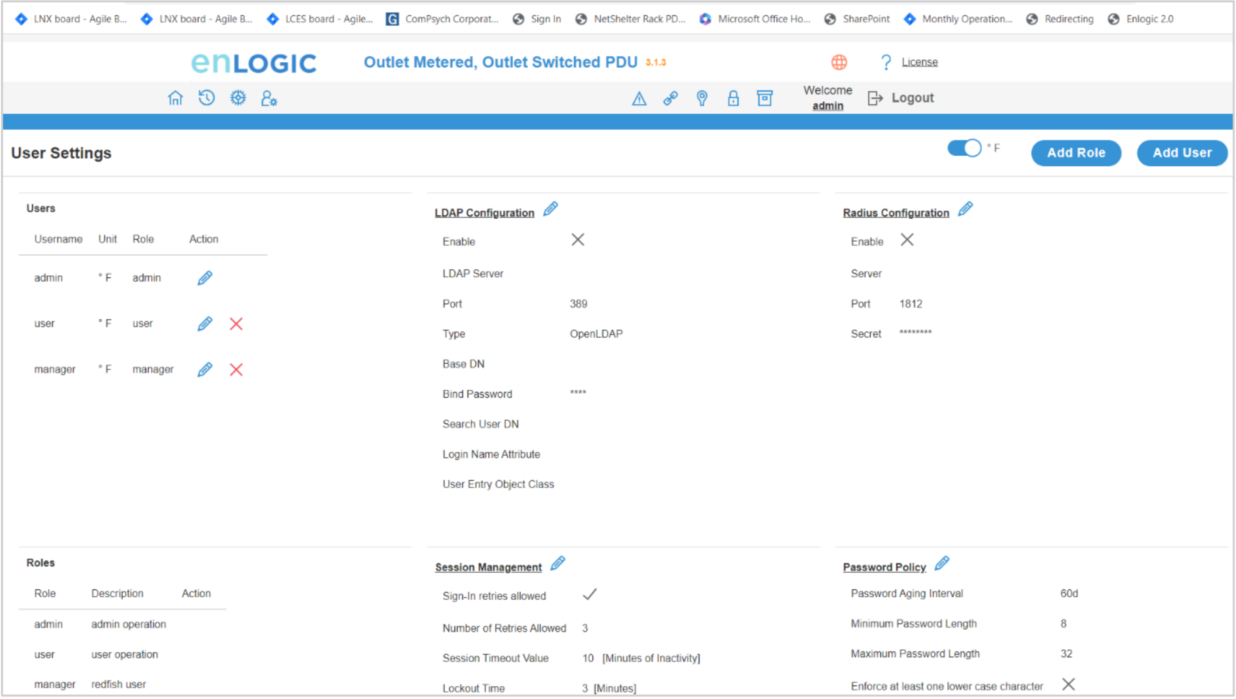
User Settings

The Advantage Secure PDU comes with a standard **Admin** profile and a standard **User** profile.

- The Admin profile is typically the system administrator, and it has the “Admin Role” with full operating permissions.
- The default User profile includes the default “User Role” permissions. The Admin user must add all other user privileges. Users are defined by their unique login credentials and by their user role.

Before setting up the user profile, determine the roles required. Each user must be given a Role. These Roles define the permissions which are granted to the user.

1. Click on the **User Settings** icon to dropdown the User Settings menu.



User Settings

Users

Username	Unit	Role	Action
admin	°F	admin	
user	°F	user	
manager	°F	manager	

LDAP Configuration

Enable	✕
LDAP Server	
Port	389
Type	OpenLDAP
Base DN	
Bind Password	****
Search User DN	
Login Name Attribute	
User Entry Object Class	

Radius Configuration

Enable	✕
Server	
Port	1812
Secret	********

Roles

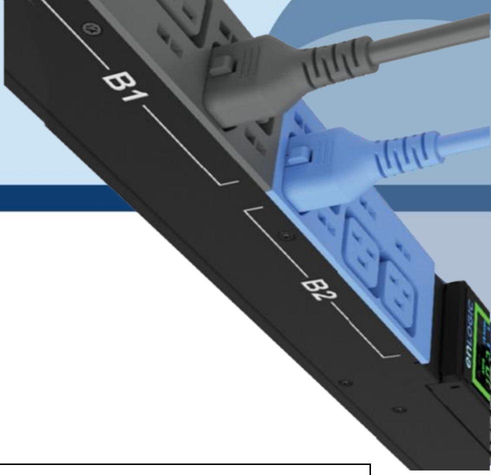
Role	Description	Action
admin	admin operation	
user	user operation	
manager	redfish user	

Session Management

Sign-In retries allowed	✓
Number of Retries Allowed	3
Session Timeout Value	10 [Minutes of Inactivity]
Lockout Time	3 [Minutes]

Password Policy

Password Aging Interval	60d
Minimum Password Length	8
Maximum Password Length	32
Enforce at least one lower case character	✕



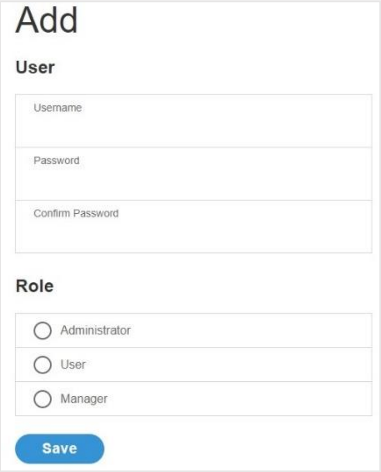
Role	Default Permissions
Admin	Complete system permissions (that cannot be modified or deleted)
User	Limited permissions that can be modified or deleted. By default, these permissions are: Change own Password
Manager	Complete system permissions (that cannot be modified or deleted)

On the top- right side of the User Settings page, Click the below options as required

Add Users

To create a new user profile:

1. Click on the **User Settings**, the user settings page opens.
2. Click **on** Add User the icon, to create a new user profile.
3. The add user window opens, enter the information:
   - Username
   - Password
   - Confirm Password
4. In the add user window assign role to set admin, user, or manager privileges.
5. Select **Save** to save the new user profile.



Add

User

Username

Password

Confirm Password

Role

○ Administrator

○ User

○ Manager

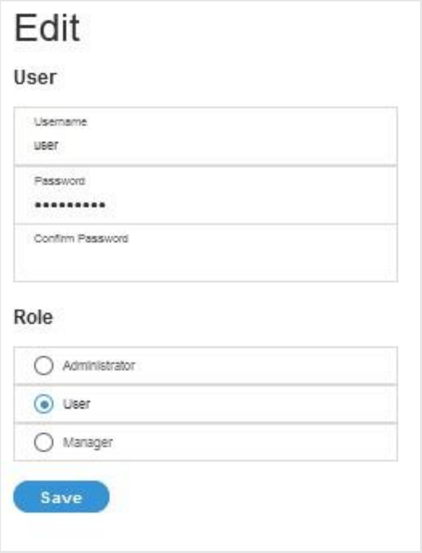
Save

Modify

To edit the existing user profile,

1 In **User Settings** select the Edit next to the username to modify.

2 Update the user profile and select **Save** to save the new user profile.



Edit

User

Username: user

Password: •••••••••

Confirm Password

Role

○ Administrator

● User

○ Manager

Save

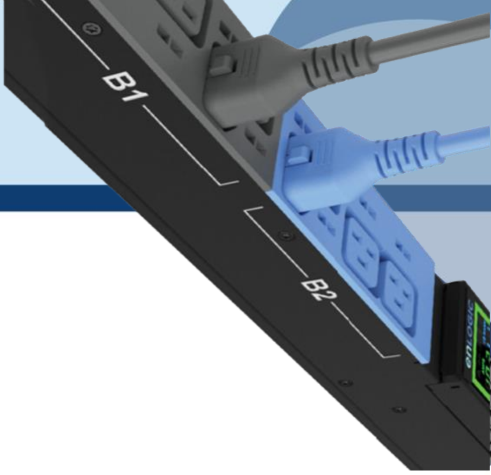
Delete:

To delete the existing user profile,

1 Go to User Settings.

2 Go to the username.

3 Select the X next to the username to delete.



LDAP Server Settings

To setup LDAP to access the Active Directory (AD) and provide authentication when logging into the PDU via the Web Interface:

1 In **User Setting,** go to LDAP Configuration.

2 Select the LDAP Enable.

3 From the **Type** (Type of LDAP Server) drop down menu, select **Open LDAP**.

4 Type Port number.
***Note**: For Microsoft, this is typically 389.*

5 Type Password in the Bind Password box

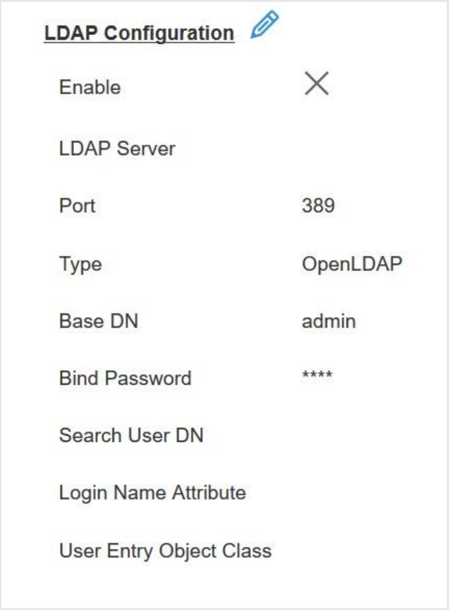
6 In the Base DN field, type in the account.
Example - CN=myuser, CN=Users, DC=EMEA, DC=mydomain, DC=com

7 Search User DN.

8 Type SAMAccountName (typically) in the Login Name Attribute field.

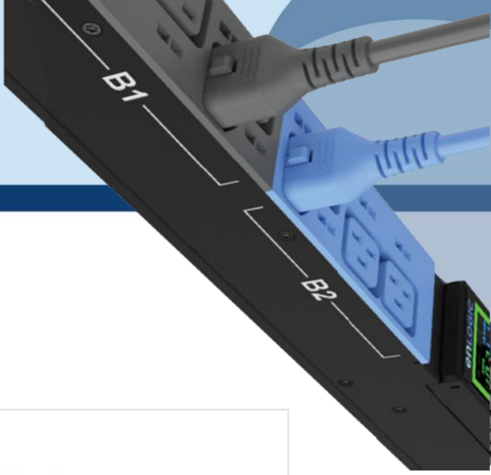
9 Type Person Name in the User Entry Object Class field.

10 With these LDAP settings configured, the Bind is complete.

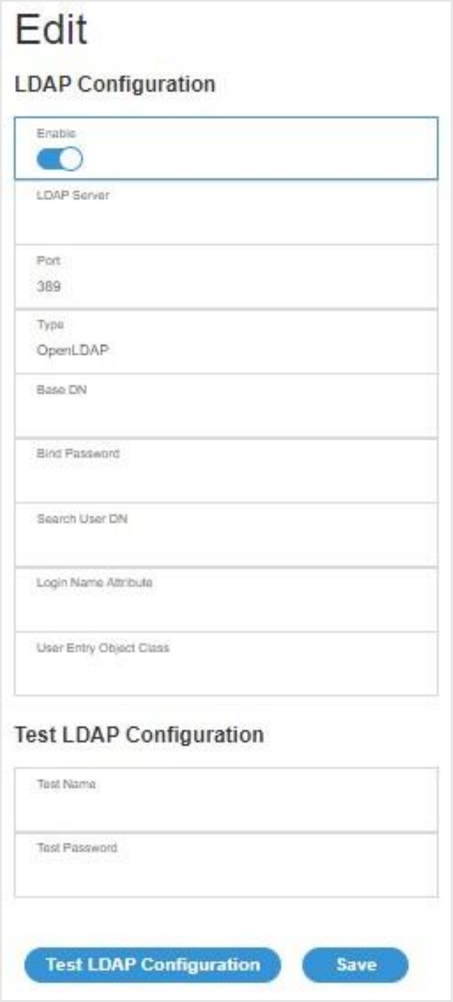


LDAP Configuration

Enable	✕
LDAP Server	
Port	389
Type	OpenLDAP
Base DN	admin
Bind Password	****
Search User DN	
Login Name Attribute	
User Entry Object Class	



11 Once the LDAP is configured, the PDU must understand for which group authentication occurs. A role must be created on the PDU to reference a group within Active Directory (AD).



Edit

LDAP Configuration

Enable: ●

LDAP Server

Port: 389

Type: OpenLDAP

Base DN

Bind Password

Search User DN

Login Name Attribute

User Entry Object Class

Test LDAP Configuration

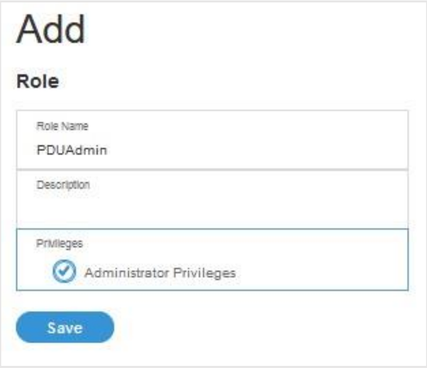
Test Name

Test Password

12 Within the Web Interface, go to **User Settings**, click on the **Add Role** button

13 Type **Role Name,** which was created in AD *i.e., PDUAdmin.*

14 Administrator privileges must be enabled



Add

Role

Role Name: PDUAdmin

Description

Privileges: ✓ Administrator Privileges

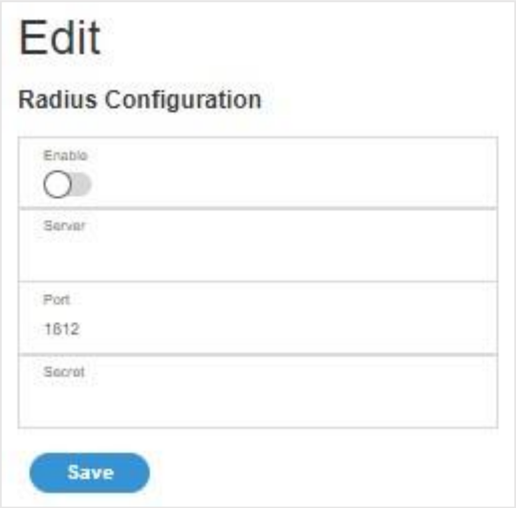
15 Once LDAP authentication is ready to use.

16 To test this, click **save**, then click “**LDAP Configuration**” again and type **Active Directory username/password** into the test box.

17 Click **Test LDAP Configuration**. If a box pops up with all green “SUCCEEDED” (no X’s), the LDAP is successfully configured.

Radius Configuration

1. In the **User Settings** go to **Radius Configuration** and click the edit pencil.
2. Select the Enable button.
   - Type **Server IP address**, **Port number**, and **Secret** in the corresponding field.
   - Click **save** button to complete the Radius authentication.



Edit

Radius Configuration

Enable

Server

Port

1612

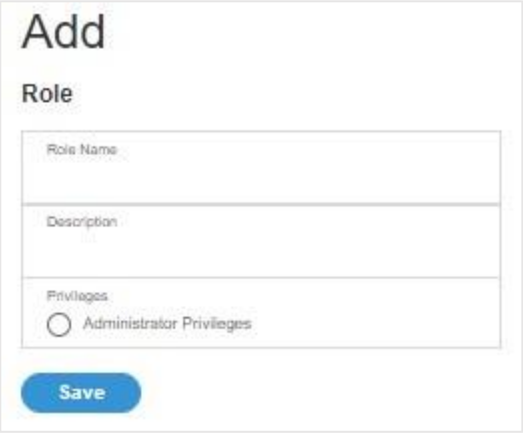
Secret

Roles

In the **User Settings,** go to **Roles** to change user roles, privileges, and settings.

To create a new role:

1. Click **Add Role** button on the top right corner.
2. type the **Role Name** and **Description**.
3. In the Privileges tab, click Edit.
4. Select the privileges to add to that user role. Set parameters if necessary.
5. Click **OK**.
6. Click **Save**.



Add

Role

Role Name

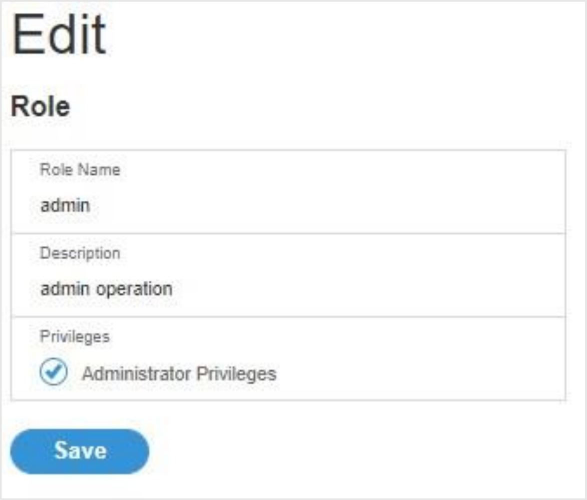
Description

Privileges

○ Administrator Privileges

To modify a custom user role:

1. Select the role.
2. click Edit Button.
3. Edit the role name and privileges as needed. click **Save**.



Edit

Role

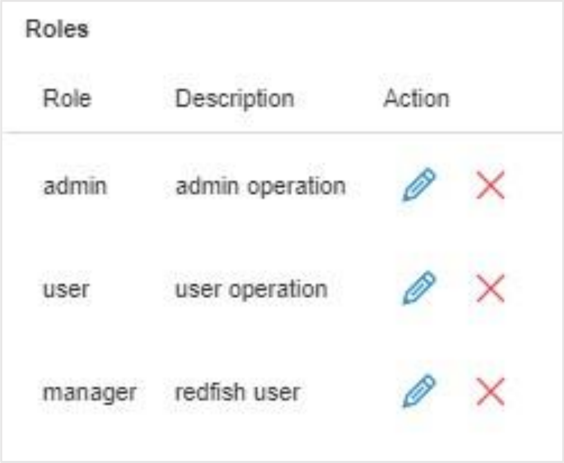
Role Name
admin

Description
admin operation

Privileges
✓ Administrator Privileges

To delete a user role:

1. Select the role.
2. Click **Delete** Button.
3. click **Yes** to confirm the change.



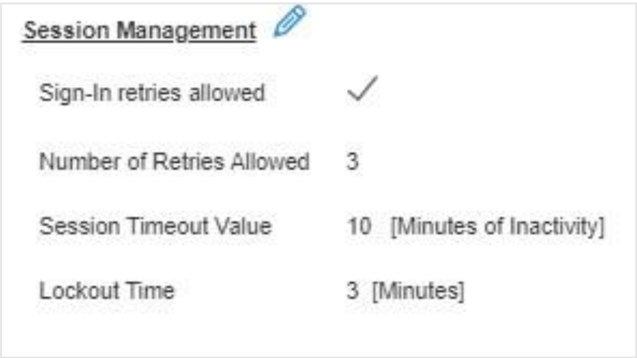
Roles

Role	Description	Action
admin	admin operation	✎ ✕
user	user operation	✎ ✕
manager	redfish user	✎ ✕

Session Management

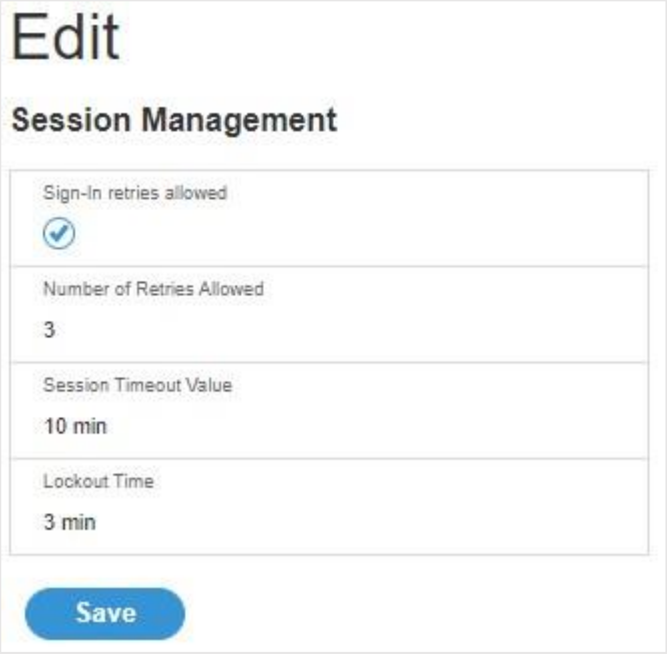
Session management supports the users to manage the Sign-In retries, number of retries allowed session timeout value and lockout time.

1. Click on the ✎ icon to edit/change the Session Management settings.
2. Add the required data and click on **Save** button to update the new settings.



Session Management ✎

Sign-In retries allowed	✓
Number of Retries Allowed	3
Session Timeout Value	10 [Minutes of Inactivity]
Lockout Time	3 [Minutes]



Edit

Session Management

Sign-In retries allowed
☑

Number of Retries Allowed
3

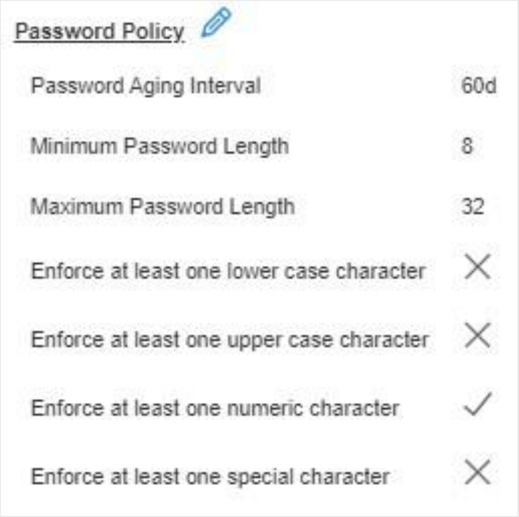
Session Timeout Value
10 min

Lockout Time
3 min

Password Policy

You can set a requirement for users to change their password at set intervals using the Password Aging Interval policy. You can also specify criteria for passwords to ensure that your users enter strong passwords.

1. Go to User Setting, click on **Password Policy**.
2. If desired, choose a password aging interval from the Password Interval dropdown menu.
3. If you wish to specify password criteria, enable the **Strong Password** radio button.



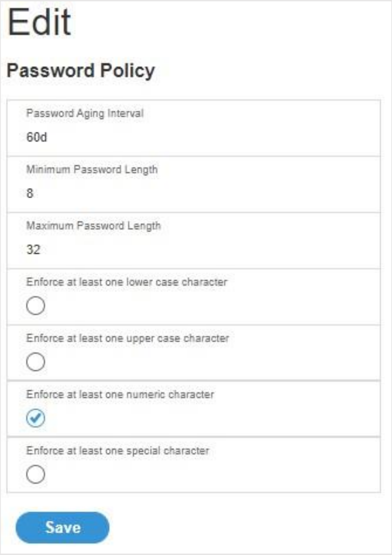
Password Policy

Password Aging Interval	60d
Minimum Password Length	8
Maximum Password Length	32
Enforce at least one lower case character	✗
Enforce at least one upper case character	✗
Enforce at least one numeric character	✓
Enforce at least one special character	✗

4. Set the Minimum Password Length and Maximum Password Length from the dropdown menus.

***Note**: Minimum password length cannot be below 8 characters and the maximum allowed up to 32.*

5. Enable the **checkboxes** to force the users to use specific types of characters within the password.
6. Click Save button to complete the settings.



Edit

Password Policy

Password Aging Interval
60d

Minimum Password Length
8

Maximum Password Length
32

Enforce at least one lower case character
○

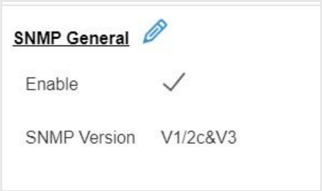
Enforce at least one upper case character
○

Enforce at least one numeric character
☑

Enforce at least one special character
○

SNMP

Simple Network Management Protocol (SNMP) is used to manage the Advantage Secure PDU(s) remotely. SNMP allows the user to monitor and detect network faults and to even configure variable data in the PDU.



SNMP General

Enable ✓

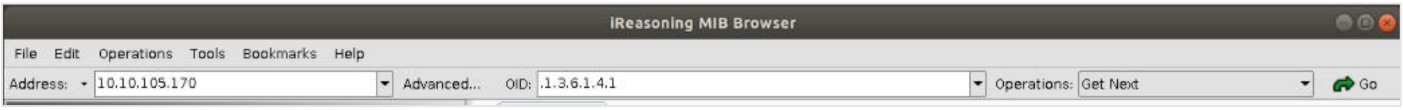
SNMP Version V1/2c&V3

Enable the SNMP in the Web UI (Refer SNMP Management)

Working with MIB Browser

Download the MIB browser and install it.

1. Open the **MIB browse and** Type the IP address of the PDU.



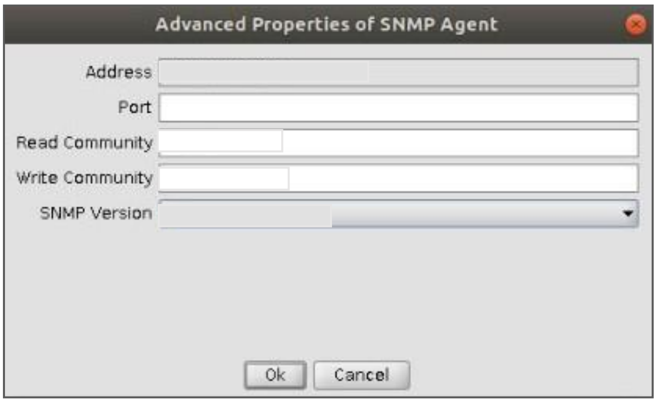
iReasoning MIB Browser

Address: 10.10.105.170

OID: .1.3.6.1.4.1

Operations: Get Next

2. Click the Advanced button, in the **Advanced Properties of SNMP Agent** window , enter the respective Port, Read Community and Write Community information.
3. Select the SNMP manager version- **1** / **2** / **3**.



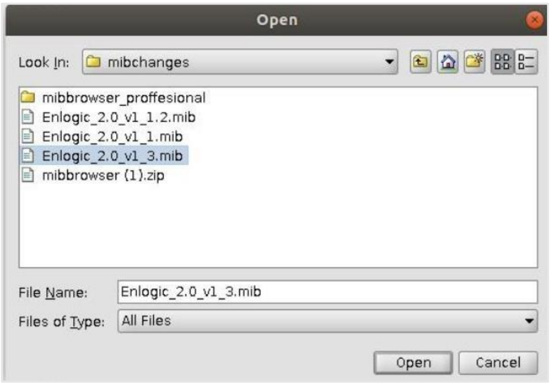
Advanced Properties of SNMP Agent

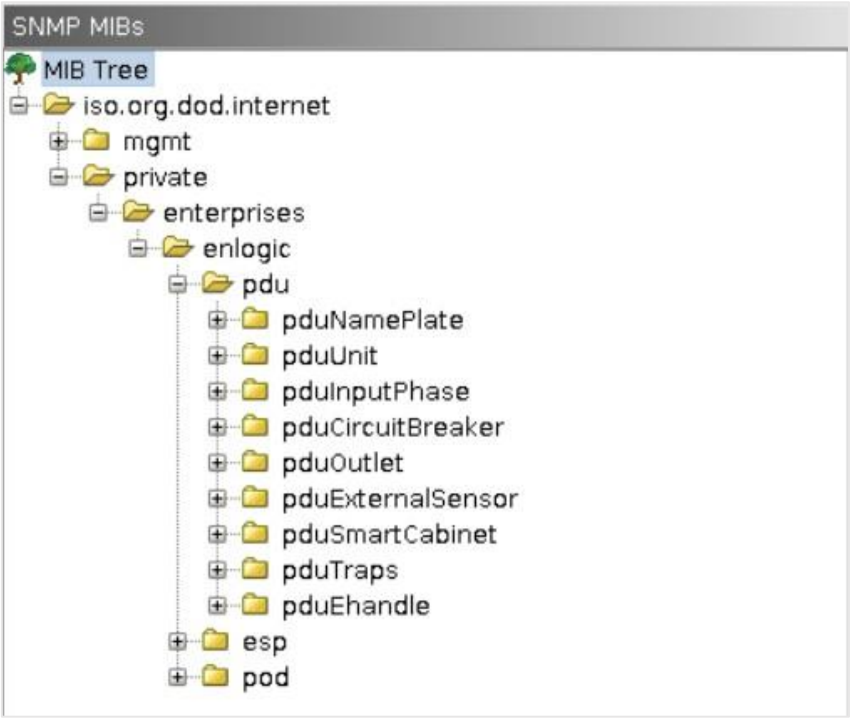
Loading the MIB file

Click on **File** and select **Load MIBs**

The **Open** window comes to view:

1. Select the latest version of the **mib file**
2. Click **Open**-> The **mib file** gets loaded.
3. The **MIB Tree** comes to view on the SNMP MIBs-> Expand the MIB Tree and select the **iso.org.dod.internet**
4. Right click on the **iso.org.dod.internet** and select **walk** to monitor the PDU data.

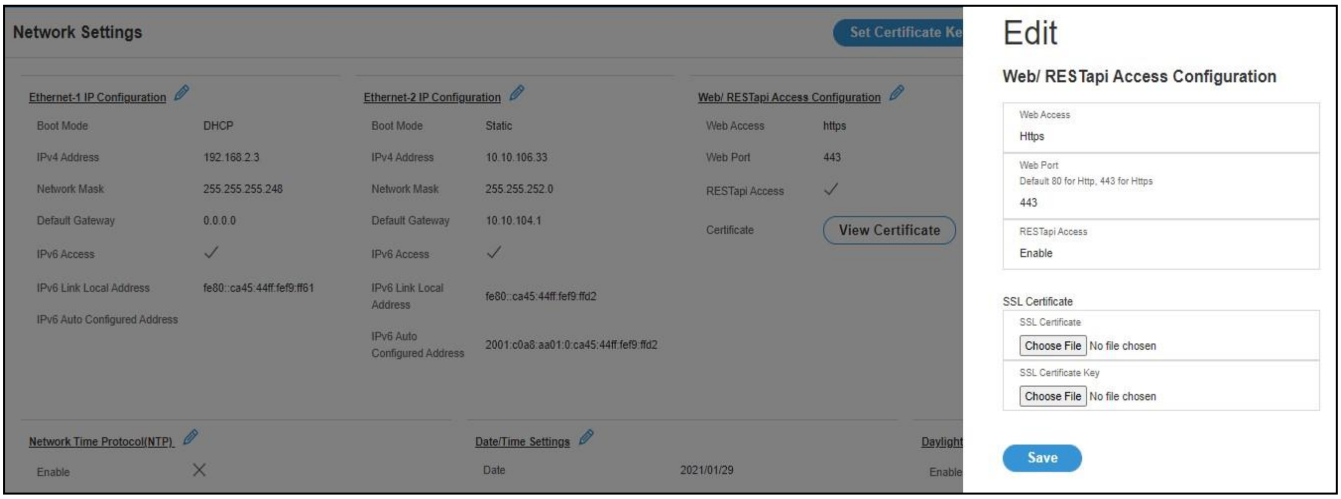




Redfish

Redfish API is tested using POSTMAN, which is a Google Chrome extension app for GET, POST and DELETE method requests.

1. To setup the **Redfish access**, type the PDU IP in chrome browser and login to the PDU using the credentials.
2. Go to **Network Settings** and enable **RESTapi Access** Configuration.



Network Settings

Ethernet-1 IP Configuration

Boot Mode	DHCP
IPv4 Address	192.168.2.3
Network Mask	255.255.255.248
Default Gateway	0.0.0.0
IPv6 Access	✓
IPv6 Link Local Address	fe80::ca45:44ff:fef9:ff61
IPv6 Auto Configured Address	

Ethernet-2 IP Configuration

Boot Mode	Static
IPv4 Address	10.10.106.33
Network Mask	255.255.252.0
Default Gateway	10.10.104.1
IPv6 Access	✓
IPv6 Link Local Address	fe80::ca45:44ff:fef9:ffd2
IPv6 Auto Configured Address	2001:c0a8:aa01:0:ca45:44ff:fef9:ffd2

Web/ RESTapi Access Configuration

Web Access	https
Web Port	443
RESTapi Access	✓
Certificate	View Certificate

Network Time Protocol(NTP)

Enable	✗

Date/Time Settings

Date	2021/01/29

Daylight

Enable

Edit

Web/ RESTapi Access Configuration

Web Access
Https

Web Port
Default 80 for Http, 443 for Https
443

RESTapi Access
Enable

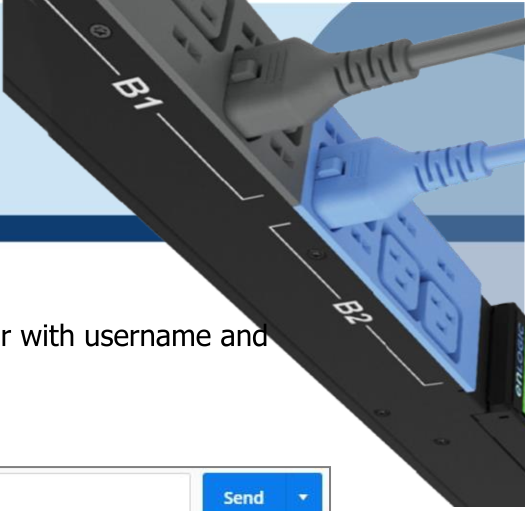
SSL Certificate

SSL Certificate
Choose File No file chosen

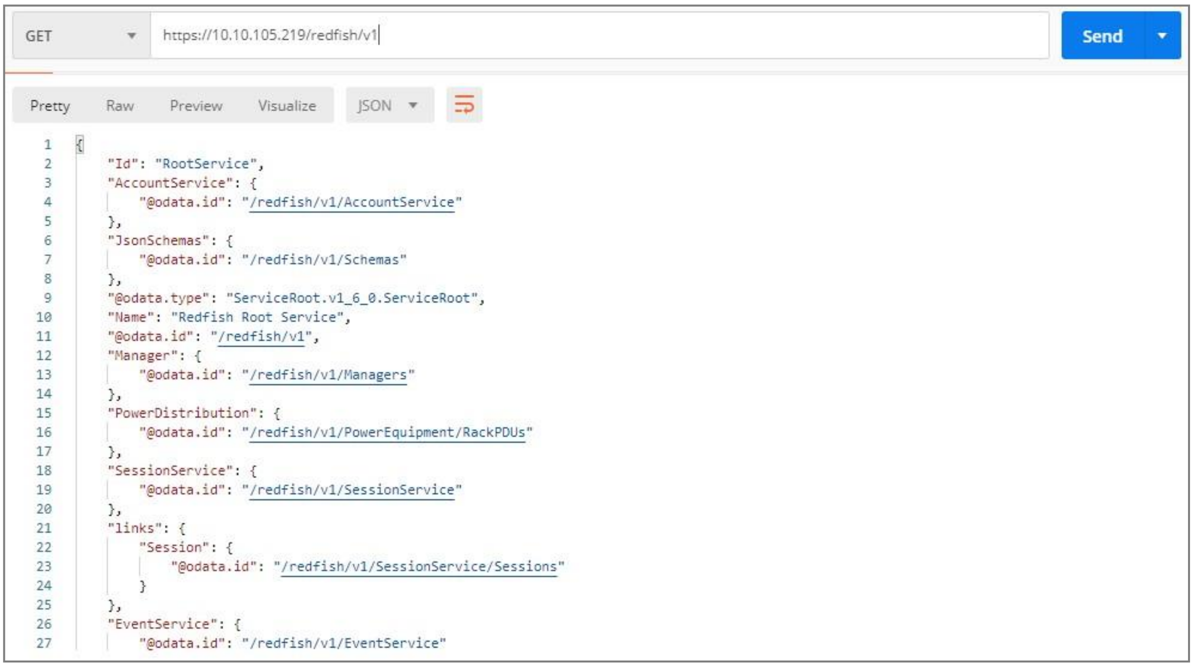
SSL Certificate Key
Choose File No file chosen

Save

3. Click **Save**, **Confirm,** and apply changes. The PDU will reboot
4. Open **POSTMAN** app. Add the basic authentication header, which is required for all the query requests.



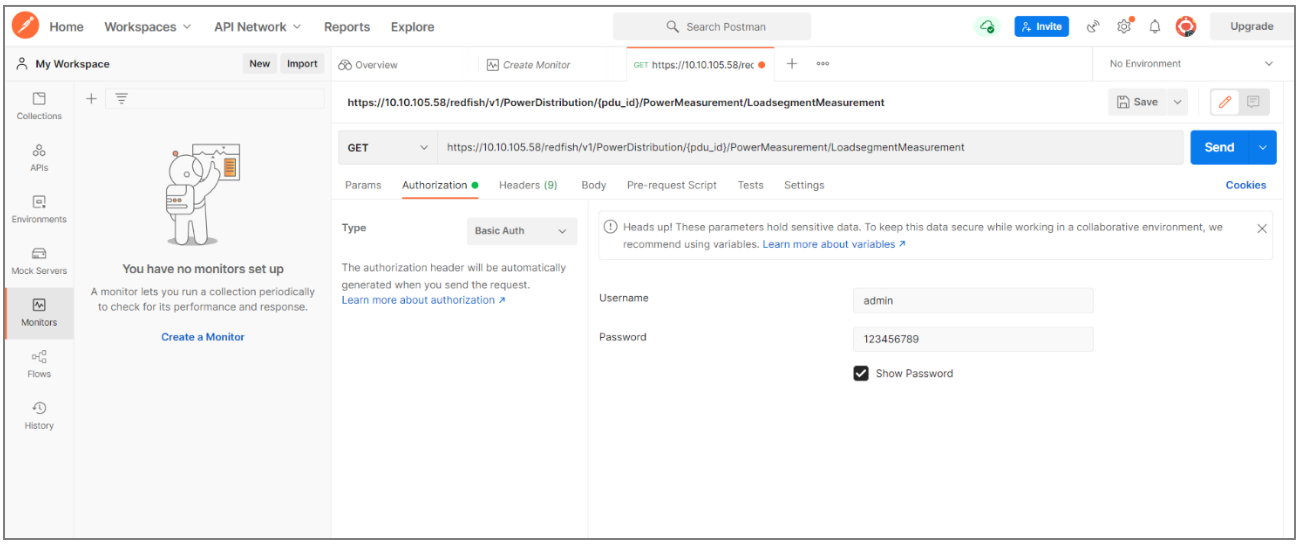
For **GET** request, type the URL request, basic authentication header with username and password and query the request.



https://10.10.105.219/redfish/v1

```
{
    "Id": "RootService",
    "AccountService": {
        "@odata.id": "/redfish/v1/AccountService"
    },
    "JsonSchemas": {
        "@odata.id": "/redfish/v1/Schemas"
    },
    "@odata.type": "ServiceRoot.v1_6_0.ServiceRoot",
    "Name": "Redfish Root Service",
    "@odata.id": "/redfish/v1",
    "Manager": {
        "@odata.id": "/redfish/v1/Managers"
    },
    "PowerDistribution": {
        "@odata.id": "/redfish/v1/PowerEquipment/RackPDUs"
    },
    "SessionService": {
        "@odata.id": "/redfish/v1/SessionService"
    },
    "links": {
        "Session": {
            "@odata.id": "/redfish/v1/SessionService/Sessions"
        }
    },
    "EventService": {
        "@odata.id": "/redfish/v1/EventService"
```

For **POST** request, include the json object type along with the basic authentication header. Create a session using POST method:



https://10.10.105.58/redfish/v1/PowerDistribution/{pdu_id}/PowerMeasurement/LoadsegmentMeasurement

GET https://10.10.105.58/redfish/v1/PowerDistribution/{pdu_id}/PowerMeasurement/LoadsegmentMeasurement

Type: Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization ↗

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about variables ↗

Username: admin

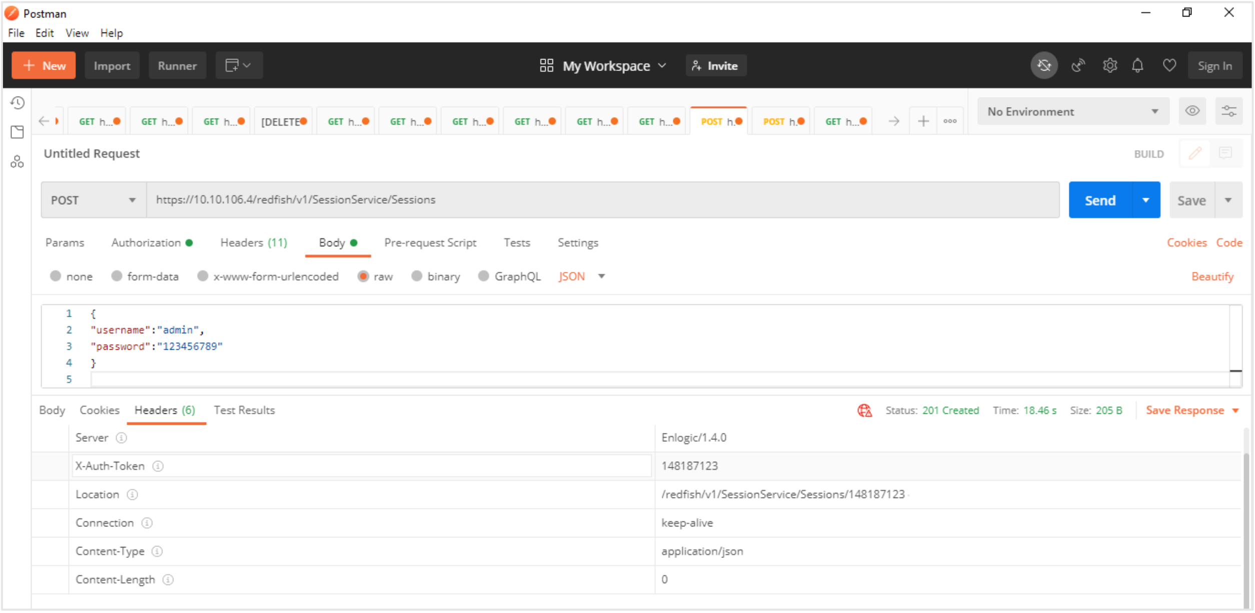
Password: 123456789

☑ Show Password

POST query the URL **http://{pdu_ip}/redfish/v1/SessionService/Sessions** along with the two headers (basic auth and json object type) and the body:

1. https://{pdu_ip}/redfish/v1/SessionService/Sessions

```
{
"username":"admin",
"password":"123456789"
}
```



POST https://10.10.106.4/redfish/v1/SessionService/Sessions

○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

```
{
"username":"admin",
"password":"123456789"
}
```

Status: 201 Created Time: 18.46 s Size: 205 B

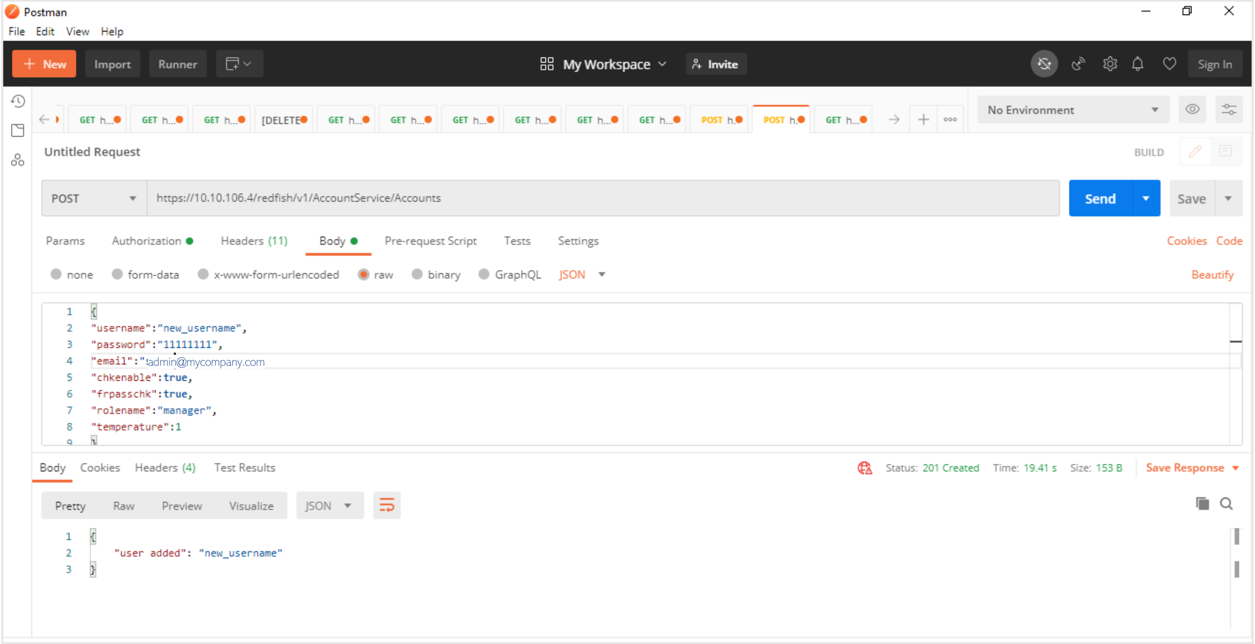
Server	Enlogic/1.4.0
X-Auth-Token	148187123
Location	/redfish/v1/SessionService/Sessions/148187123
Connection	keep-alive
Content-Type	application/json
Content-Length	0

2. https://{pdu_ip}/redfish/v1/SessionService/Sessions

```
{
"username":"admin",
"password":"123456789"
}
```

3. https://{pdu_ip}/redfish/v1/AccountService/Accounts

```
{
"username":"new_user",
"password":"11223344",
"email":" admin@mycompany.com",
"chkenable":true,
"frpasschk":true,
"rolename":"manager",
"temperature":1
}
```



POST https://10.10.106.4/redfish/v1/AccountService/Accounts

○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

```
{
"username":"new_username",
"password":"11111111",
"email":"admin@mycompany.com
"chkenable":true,
"frpasschk":true,
"rolename":"manager",
"temperature":1
}
```

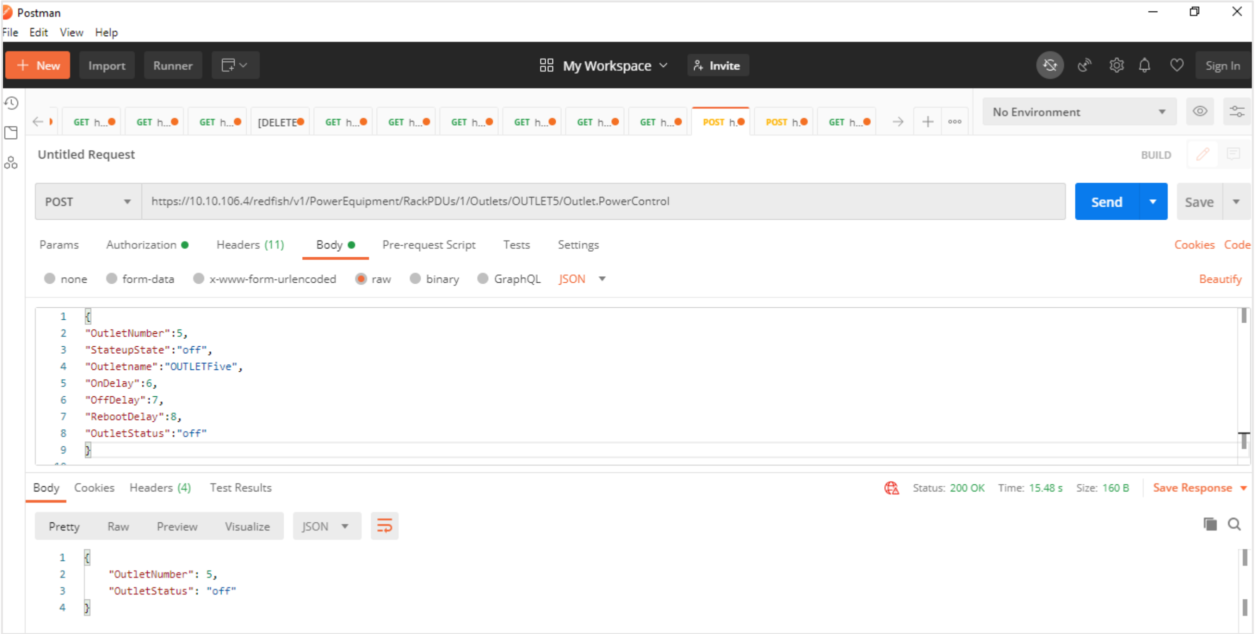
Status: 201 Created Time: 19.41 s Size: 153 B

```
{
    "user added": "new_username"
}
```

4. PDU1 – Outlet Control

https://{pdu_ip}/redfish/v1/PowerEquipment/RackPDUs/1/Outlets/OUTLET5/Outlet.PowerControl

```
{
"OutletNumber":6,
"StartupState":"off",
"Outletname":"OUTLETFive",
"OnDelay":5,
"OffDelay":6,
"RebootDelay":7,
"OutletStatus":"off"
}
```



Untitled Request

POST https://10.10.106.4/redfish/v1/PowerEquipment/RackPDUs/1/Outlets/OUTLET5/Outlet.PowerControl

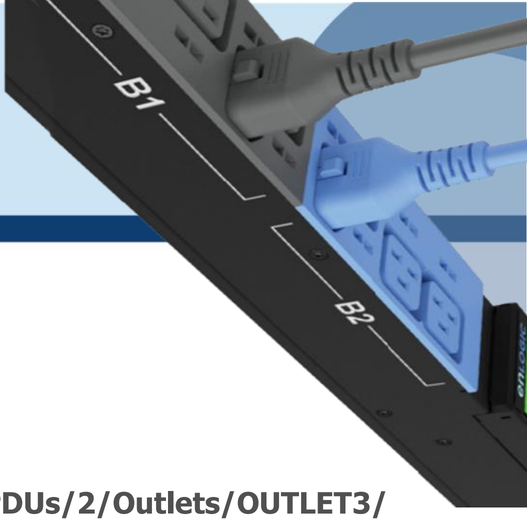
Body: ○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

```
{
"OutletNumber":5,
"StateupState":"off",
"Outletname":"OUTLETFive",
"OnDelay":6,
"OffDelay":7,
"RebootDelay":8,
"OutletStatus":"off"
}
```

Status: 200 OK Time: 15.48 s Size: 160 B

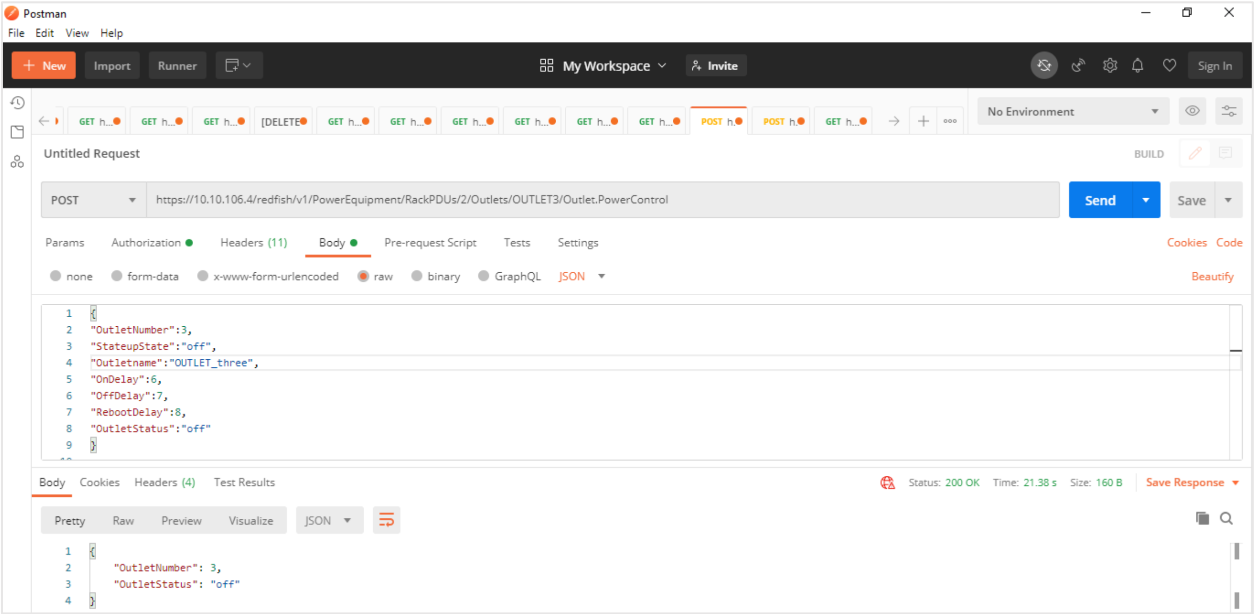
Body: Pretty, JSON

```
{
    "OutletNumber": 5,
    "OutletStatus": "off"
}
```



5. PDU2 – Outlet Control

https://{pdu_ip}/redfish/v1/PowerEquipment/RackPDUs/2/Outlets/OUTLET3/Outlet.PowerControl



POST https://10.10.106.4/redfish/v1/PowerEquipment/RackPDUs/2/Outlets/OUTLET3/Outlet.PowerControl

Body: ○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

```
{
"OutletNumber":3,
"StateupState":"off",
"Outletname":"OUTLET_three",
"OnDelay":6,
"OffDelay":7,
"RebootDelay":8,
"OutletStatus":"off"
}
```

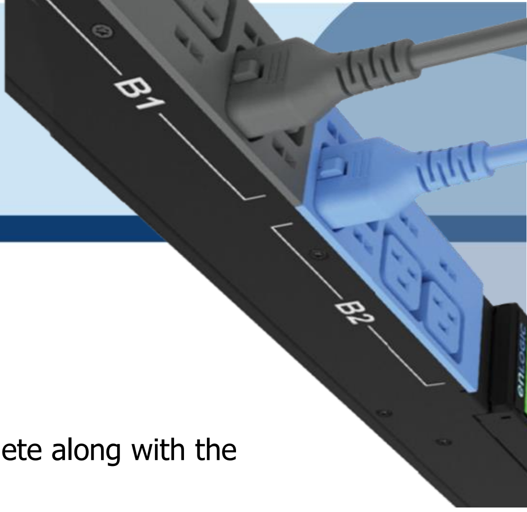
Status: 200 OK Time: 21.38 s Size: 160 B

Body JSON

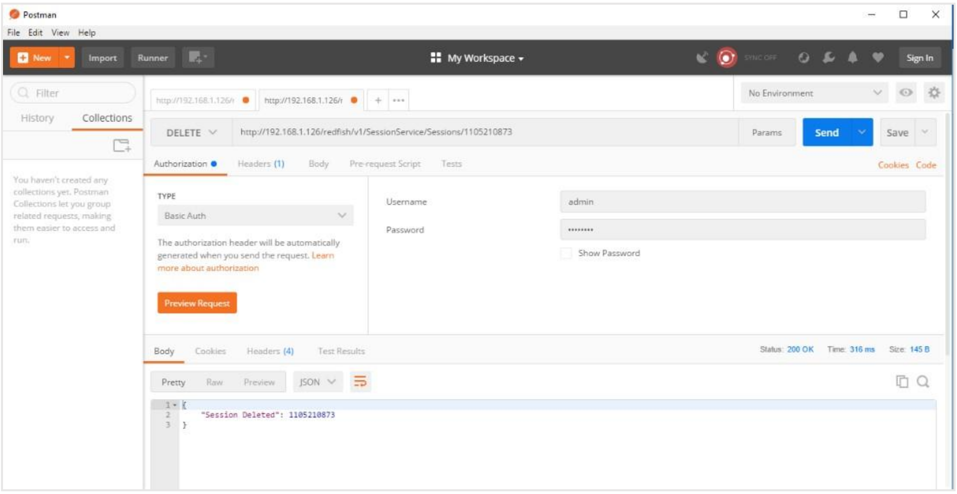
```
{
    "OutletNumber": 3,
    "OutletStatus": "off"
}
```

Note : Every highlighted text must be provided in the body section as shown in captured screenshots

Along with authorization & X-Auth-Token generated



For **DELETE** request, type the URL for session or users want to delete along with the basic authentication and send



Postman

DELETE http://192.168.1.126/redfish/v1/SessionService/Sessions/1105210873

Authorization: TYPE Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

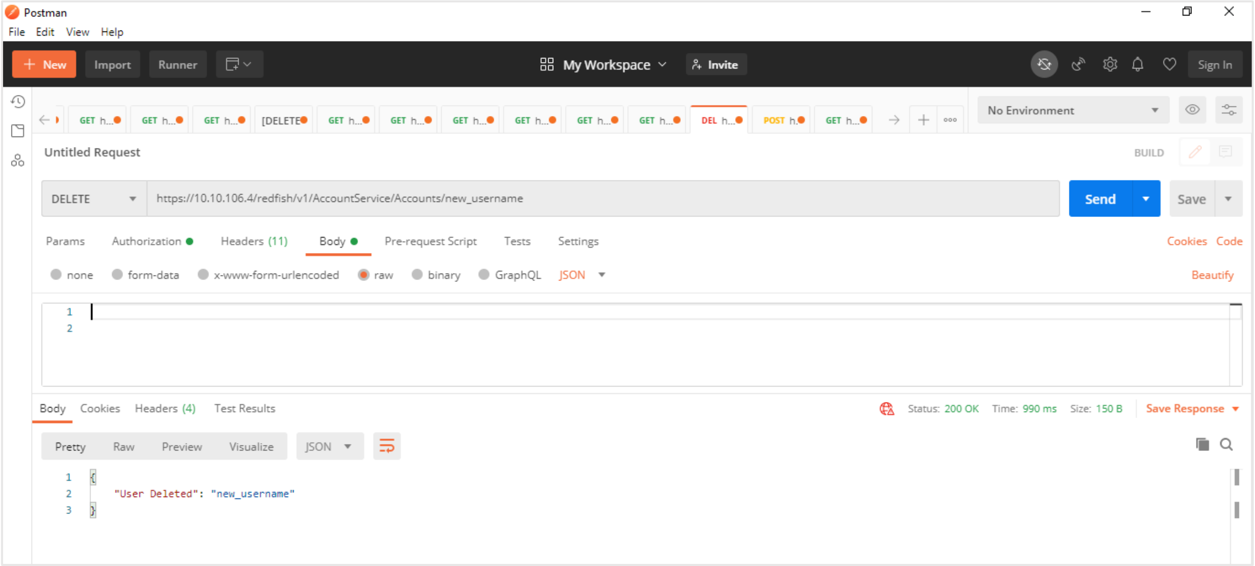
Username: admin

Password: ••••••••

Status: 200 OK Time: 316 ms Size: 145 B

```
{
    "Session Deleted": 1105210873
}
```

1. **https://{pdu_ip}/redfish/v1/AccountService/Accounts/{username}**



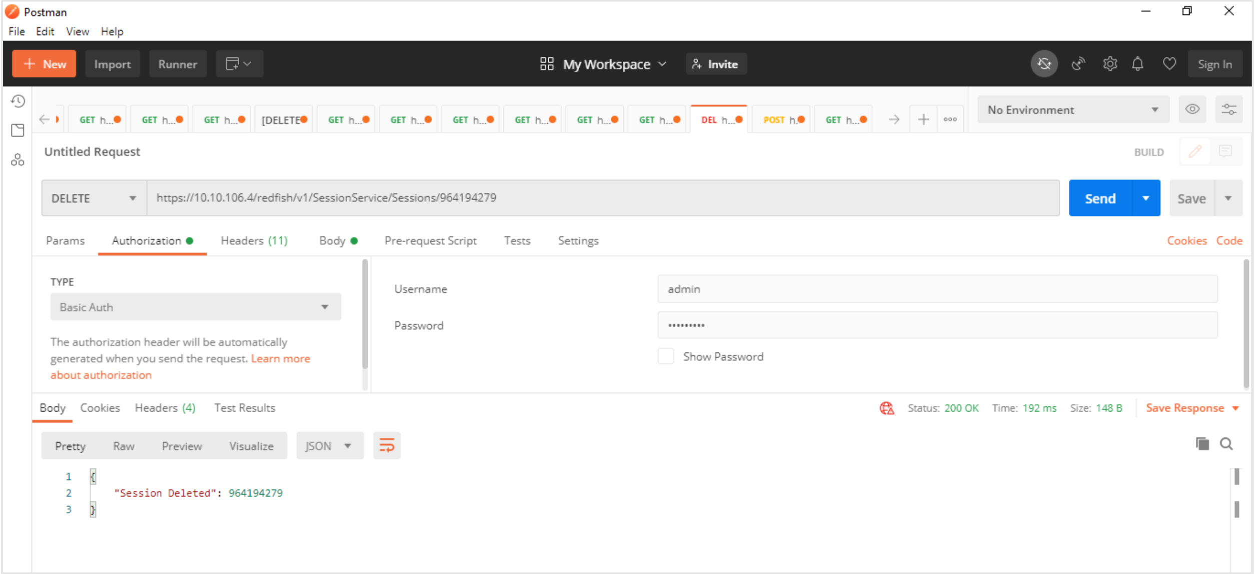
Untitled Request

DELETE https://10.10.106.4/redfish/v1/AccountService/Accounts/new_username

Status: 200 OK Time: 990 ms Size: 150 B

```
{
    "User Deleted": "new_username"
}
```

2. **https://{pdu_ip}/redfish/v1/SessionService/Sessions/{session_id}**



Postman

File Edit View Help

New Import Runner My Workspace Invite Sign In

No Environment

Untitled Request

DELETE https://10.10.106.4/redfish/v1/SessionService/Sessions/964194279

Send Save

Params Authorization ● Headers (11) Body ● Pre-request Script Tests Settings Cookies Code

TYPE

Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

Username: admin

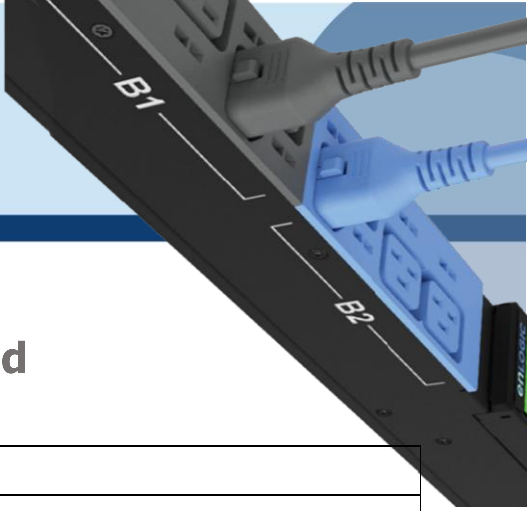
Password: •••••••••

□ Show Password

Body Cookies Headers (4) Test Results Status: 200 OK Time: 192 ms Size: 148 B Save Response

Pretty Raw Preview Visualize JSON

```
{
    "Session Deleted": 964194279
}
```



Redfish URLs Supported with GET Method

Session Service

S.No	URL
1	https://<ip_addr>/redfish/v1
2	/redfish/v1/SessionService
3	/redfish/v1/SessionService/Sessions
4	/redfish/v1/SessionService/Sessions/{session_ids}

Account Service

S.No	URL
1	/redfish/v1/AccountService
2	/redfish/v1/AccountService/Accounts
3	/redfish/v1/AccountService/Accounts/{userid}
4	/redfish/v1/AccountService/Roles
5	/redfish/v1/AccountService/Roles/{rolename}

Managers

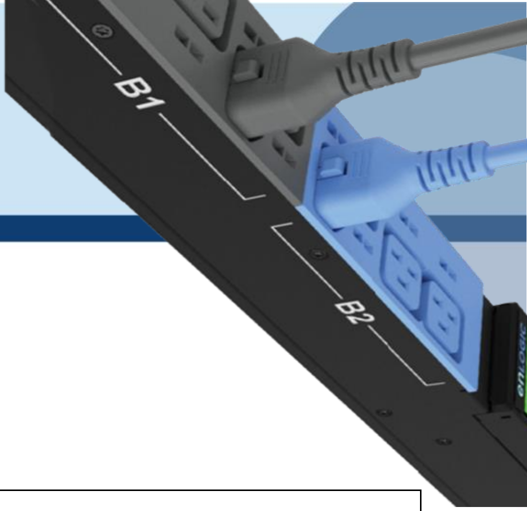
S.No	URL
1	/redfish/v1/Managers
2	/redfish/v1/Managers/manager
3	/redfish/v1//Managers/manager/NetworkProtocol
4	/redfish/v1//Managers/1/LogServices
5	/redfish/v1//Managers/1/LogServices/Log
6	/redfish/v1//Managers/1/LogServices/Log/Entries

Metrics

S.No	URL
1	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Metrics

Power Equipment

S.No	URL
1	/redfish/v1/PowerEquipment
2	/redfish/v1/PowerEquipment/RackPDUs
3	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}



Branches

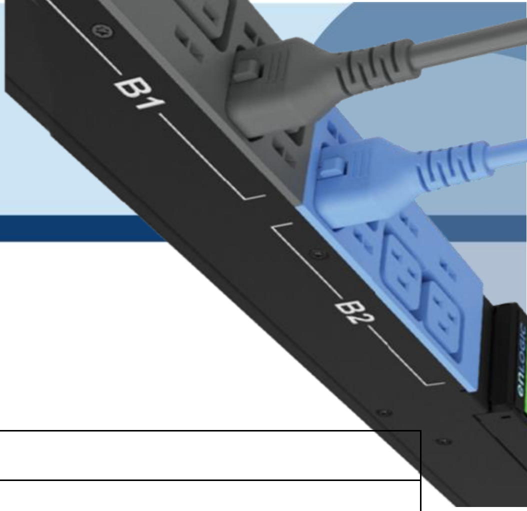
S.No	URL
1	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Branches
2	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id} /Branches/#cbnumber
3	/redfish/v1/PowerEquipment/RackPDUs/{pdu id}/Branches/A
4	/redfish/v1/PowerEquipment/RackPDUs/{pdu id}/Branches/B
5	/redfish/v1/PowerEquipment/RackPDUs/{pdu id}/Branches/C
6	/redfish/v1/PowerEquipment/RackPDUs/{pdu id}/Branches/D
7	/redfish/v1/PowerEquipment/RackPDUs/{pdu id}/Branches/E
8	/redfish/v1/PowerEquipment/RackPDUs/{pdu id}/Branches/F

Outlets

S.No	URL
1	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Outlets
2	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Outlets/#outletnumber

Sensors

S.No	URL
1	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors
2	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/Power{cbnum#}
3	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/Current{cbnum#}
4	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/Voltage{cbnum#}
5	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/CurrentOUTLET#
6	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/VoltageOUTLET#
7	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/PowerOUTLET#
8	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/EnergyOUTLET#
9	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/PowerMains1-6 (for WYE type PDUs) /redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/PowerMains1-3 (for DELTA type PDUs)
10	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/CurrentMains1-3
11	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/VoltageMains1-6 (for WYE type PDUs) /redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/VoltageMains1-3 (for DELTA type PDUs)
12	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/FreqMains
13	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Sensors/PDUPower



Mains

S.No	URL
1	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Mains
2	/redfish/v1/PowerEquipment/RackPDUs/{pdu_id}/Mains/AC1

Redfish URLs Supported with POST Method

S.No	URL
1	/redfish/v1/SessionService/Sessions
2	/redfish/v1/AccountService/Accounts
3	/redfish/v1/PowerEquipment/RackPDUs/{pduid}/Outlets/OUTLET#/Outlet.PowerControl
4	/redfish/v1/PowerEquipment/RackPDUs/{pduid}/Outlets/OUTLET#/Outlet.PowerControl
5	/redfish/v1/PowerEquipment/RackPDUs/4/Outlets/OUTLET24/Outlet.PowerControl

Redfish URLs Supported with DELETE Method

S.No	URL
1	/redfish/v1/AccountService/Accounts/{username}
2	/redfish/v1/SessionService/Sessions/{session_id}

RESTAPI – CURL Commands

Getting Started

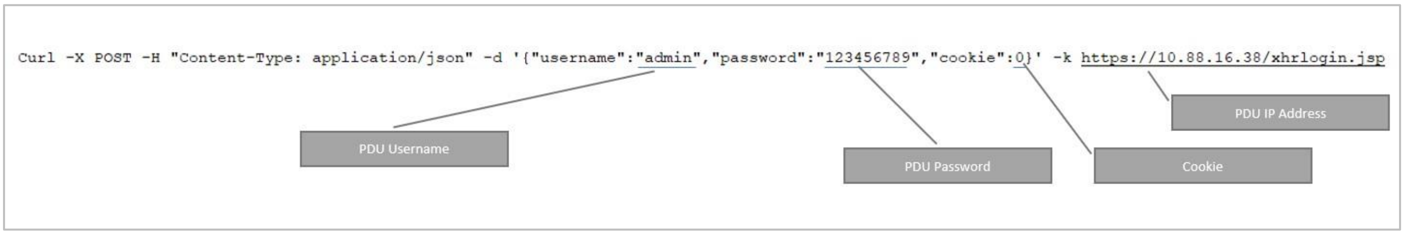
- The curl commands in this document utilize the username 'admin' and password '123456789'. Update these commands in relation to the setup.
- The IP address used for illustrations is https://10.88.0.82/***. Update it in accordance with the setting.
- Check for 'Web Access' HTTP or HTTPS. Based on the context. The curl commands must be changed for the 'k' option.
- The curl command requires a 'cookie ID' to function properly. To post any curl method, the user would need to acquire a cookie ID and utilize it in subsequent curl operations.

Note - Cookie IDs will be active till the PDU times out or reboots.

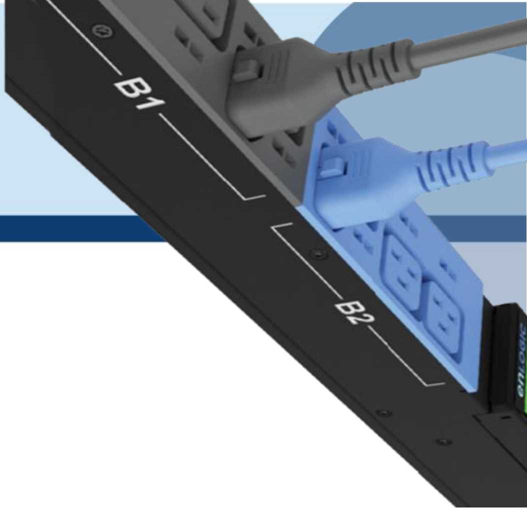
Understanding the Syntax

Command Syntax

```
curl -X POST -H "Content-Type: application/json" -d '{"username":"admin","password":"123456789","cookie":0}' -k
https://10.88.16.38/xhrlogin.jsp
```



```
Curl -X POST -H "Content-Type: application/json" -d '{"username":"admin","password":"123456789","cookie":0}' -k https://10.88.16.38/xhrlogin.jsp
```

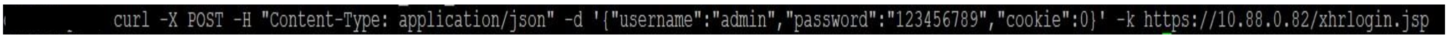


1. **Session ID: To Create a Session ID**

Curl Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"username":"admin","password":"123456789","cookie":0}' -k
https://10.88.0.82/xhrlogin.jsp
```

Screen capture from LINUX box.

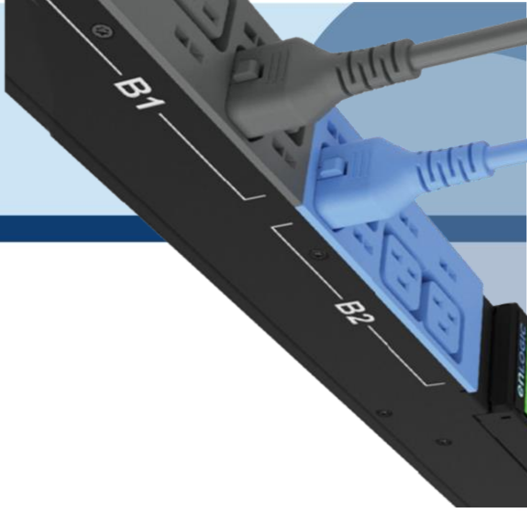


```
curl -X POST -H "Content-Type: application/json" -d '{"username":"admin","password":"123456789","cookie":0}' -k https://10.88.0.82/xhrlogin.jsp
```

Note *- the cookie generated in the response "{"cookie": 1107747442," this is the cookie ID which needs to be used for next subsequent commands.*

Curl Command formatted:

```
curl -X POST \
 -H "Content-Type: application/json" \
 -d '{
        "username":"admin",
        "password":"123456789",
        "cookie":0
        }' \
 -k https://10.88.0.82/xhrlogin.jsp
```

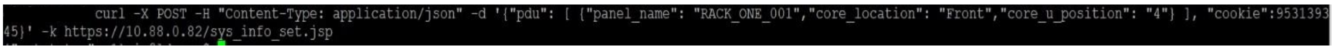


2. **PDU NAME:**

Curl Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"pdu": [ {"panel_name": " RACK_ONE_001","core_location":
"Front","core_u_position": "4"} ], "cookie": 1107747442}' -k https://10.88.0.82/sys_info_set.jsp
```

Screen capture from LINUX box.

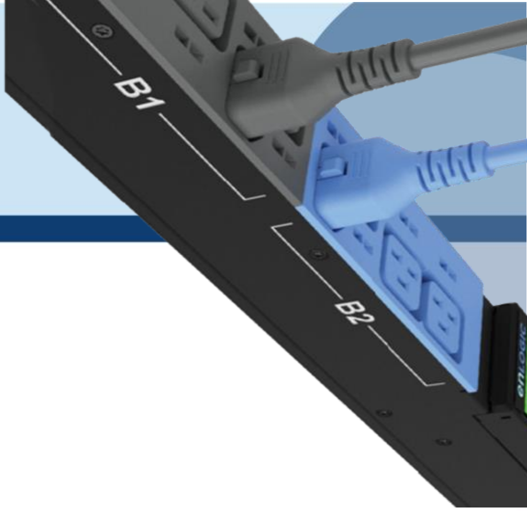


```
        curl -X POST -H "Content-Type: application/json" -d '{"pdu": [ {"panel_name": "RACK_ONE_001","core_location": "Front","core_u_position": "4"} ], "cookie":9531393
45}' -k https://10.88.0.82/sys_info_set.jsp
```

***Note** - the response {"upstatus":1} – This response confirms the command executed gracefully.*

Curl Command formatted:

```
curl -X POST \
 -H "Content-Type: application/json" \
 -d '{
        "username": "add_new_user",
        "password": "newuser123",
        "email": "",
        "chkenable": true,
        "frpasschk": true,
        "rolename": "admin",
        "temperature": 0, "roles": "admin", "cookie": 1107747442}' \
 -k https://10.88.0.82/xhrnewusersset.jsp
```

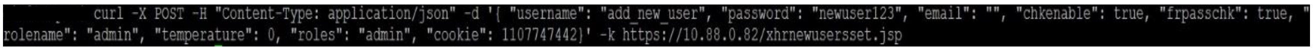


3. ADD USER & PASSWORD:

Curl Command:

```
curl -X POST -H "Content-Type: application/json" -d '{ "username": "add_new_user", "password": "newuser123", "email": "", "chkenable": true, "frpasschk": true, "rolename": "admin", "temperature": 0, "roles": "admin", "cookie": 1107747442}' -k https://10.88.0.82/xhrnewusersset.jsp
```

Screen capture from LINUX box.



```
        curl -X POST -H "Content-Type: application/json" -d '{ "username": "add_new_user", "password": "newuser123", "email": "", "chkenable": true, "frpasschk": true, "
rolename": "admin", "temperature": 0, "roles": "admin", "cookie": 1107747442}' -k https://10.88.0.82/xhrnewusersset.jsp
```

***Note** - the response {"upstatus":1} – This response confirms the command executed gracefully.*

Curl Command formatted:

```
curl -X POST \
 -H "Content-Type: application/json" \
 -d '{
        "pdu": [ {
                "panel_name": " RACK_ONE_001",
                "core_location": "Front",
                "core_u_position": "4"} ],
            "cookie": 1107747442}' \
 -k https://10.88.0.82/sys_info_set.jsp
```

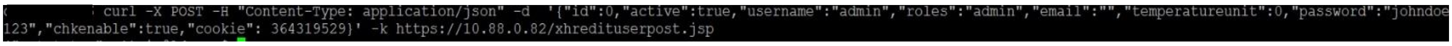
4. EDIT USER & PASSWORD:

Curl Command to edit the User and Manager User Password:

ADMIN USER:

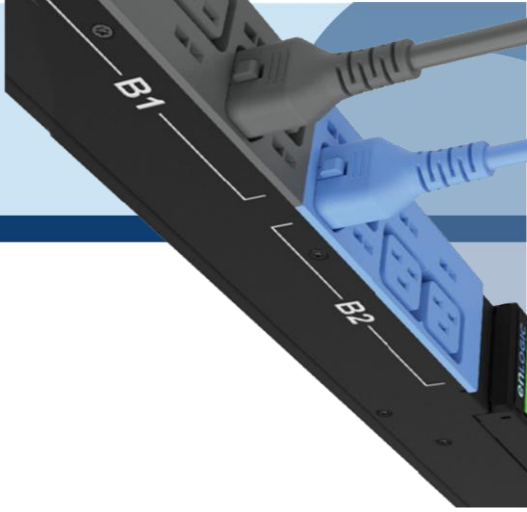
```
curl -X POST -H "Content-Type: application/json" -d
{"id":0,"active":true,"username":"admin","roles":"admin","email":"","temperatureunit":0,"password":"johndoe123" ,"chkenable":true,"cookie": 364319529}' -k https://10.88.0.82/xhredituserpost.jsp
```

Screen capture from LINUX box.



```
        curl -X POST -H "Content-Type: application/json" -d  '{"id":0,"active":true,"username":"admin","roles":"admin","email":"","temperatureunit":0,"password":"johndoe
123","chkenable":true,"cookie": 364319529}' -k https://10.88.0.82/xhredituserpost.jsp
```

***Note** - the response {"upstatus":1} – This response confirms the command executed gracefully.*



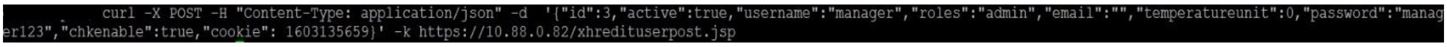
Curl Command formatted:

```
curl -X POST \
 -H "Content-Type: application/json"
-d  '{
        "id":0,
        "active":true,
        "username":"admin",
        "roles":"admin",
        "email":"",
        "temperatureunit":0,
        "password":"johndoe123",
        "chkenable":true,
        "cookie": 364319529}' \
-k https://10.88.0.82/xhredituserpost.jsp
```

MANAGER USER:

```
curl -X POST -H "Content-Type: application/json" -d
'{"id":3,"active":true,"username":"manager","roles":"admin","email":"","temperatureunit":0,"password":"manager12
3","chkenable":true,"cookie": 1107747442}' -k https://10.88.0.82/xhredituserpost.jsp
```

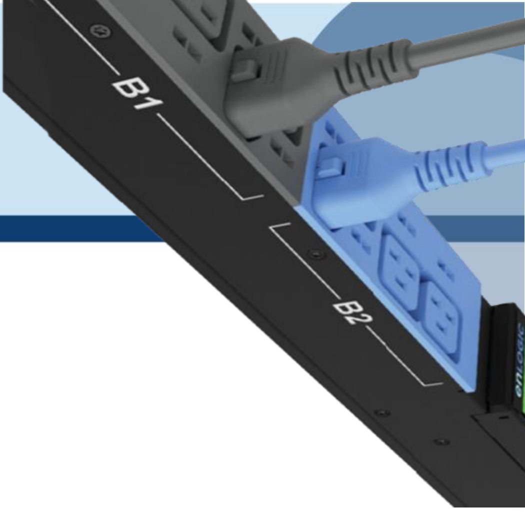
Screen capture from LINUX box.



```
       curl -X POST -H "Content-Type: application/json" -d  '{"id":3,"active":true,"username":"manager","roles":"admin","email":"","temperatureunit":0,"password":"manag
er123","chkenable":true,"cookie": 1603135659}' -k https://10.88.0.82/xhredituserpost.jsp
```

Curl Command formatted:

```
curl -X POST \
 -H "Content-Type: application/json" \
 -d '{
        "id":3,
        "active":true,
        "username":"manager",
        "roles":"admin",
        "email":"",
        "temperatureunit":0,
        "password":"manager123",
        "chkenable":true,
        "cookie": 1107747442}' \
 -k https://10.88.0.82/xhredituserpost.jsp
```

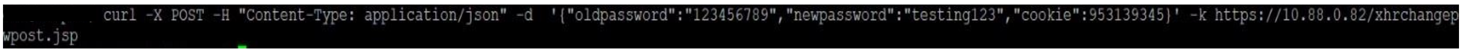


5. **CHANGE ADMIN & PASSWORD:**

Curl Command:

```
curl -X POST -H "Content-Type: application/json" -d
'{"oldpassword":"123456789","newpassword":"testing123","cookie": 1107747442}' -k
https://10.88.0.82/xhrchangepwpost.jsp
```

Screen capture from LINUX box.



```
curl -X POST -H "Content-Type: application/json" -d  '{"oldpassword":"123456789","newpassword":"testing123","cookie":953139345}' -k https://10.88.0.82/xhrchangep
wpost.jsp
```

Note *- the response {"upstatus":1} – This response confirms the command executed gracefully.*

Curl Command formatted:

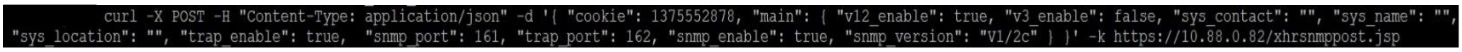
```
curl -X POST \
 -H "Content-Type: application/json" \
 -d  '{
        "oldpassword":"123456789",
        "newpassword":"testing123",
        "cookie": 1107747442}' \
 -k https://10.88.0.82/xhrchangepwpost.jsp
```

6. **SNMP VERSION:**

Curl Command TO SET V1/V2:

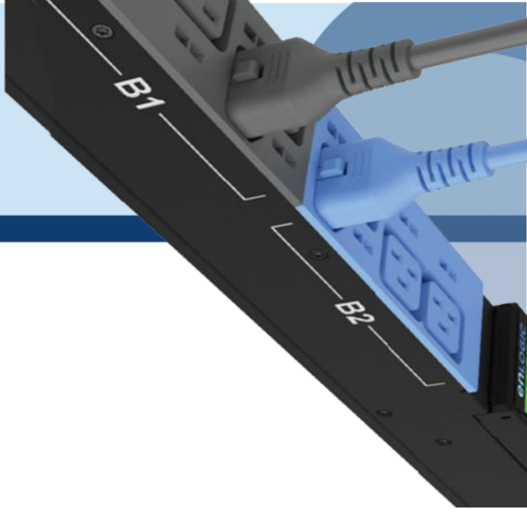
```
curl -X POST -H "Content-Type: application/json" -d '{ "cookie": 1375552878, "main": { "v12_enable": true,
"v3_enable": false, "sys_contact": "", "sys_name": "", "sys_location": "", "trap_enable": true,  "snmp_port": 161,
"trap_port": 162, "snmp_enable": true, "snmp_version": "V1/2c" } }' -k https://10.88.0.82/xhrsnmppost.jsp
```

Screen capture from LINUX box.



```
curl -X POST -H "Content-Type: application/json" -d '{ "cookie": 1375552878, "main": { "v12_enable": true, "v3_enable": false, "sys_contact": "", "sys_name": "",
"sys_location": "", "trap_enable": true,  "snmp_port": 161, "trap_port": 162, "snmp_enable": true, "snmp_version": "V1/2c" } }' -k https://10.88.0.82/xhrsnmppost.jsp
```

Note *- the response {"upstatus":1} – This response confirms the command executed gracefully.*



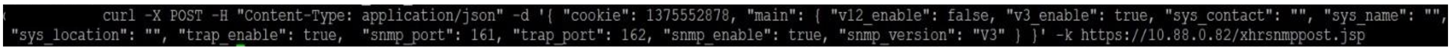
Curl Command formatted:

```
curl -X POST \
 -H \"Content-Type: application/json" \
 -d '{
        "cookie": 1375552878,
        "main":
        {
              "v12_enable": true,
              "v3_enable": false,
              "sys_contact": "",
              "sys_name": "",
              "sys_location": "",
              "trap_enable": true,
              "snmp_port": 161,
              "trap_port": 162,
              "snmp_enable": true,
              "snmp_version": "V1/2c"
        } }'
 -k https://10.88.0.82/xhrsnmppost.jsp
```

Curl Command TO SET V3 ONLY:

```
curl -X POST -H "Content-Type: application/json" -d '{ "cookie": 1375552878, "main": { "v12_enable": false,
"v3_enable": true, "sys_contact": "", "sys_name": "", "sys_location": "", "trap_enable": true,  "snmp_port": 161,
"trap_port": 162, "snmp_enable": true, "snmp_version": "V3" } }' -k https://10.88.0.82/xhrsnmppost.jsp
```

Screen capture from LINUX box.

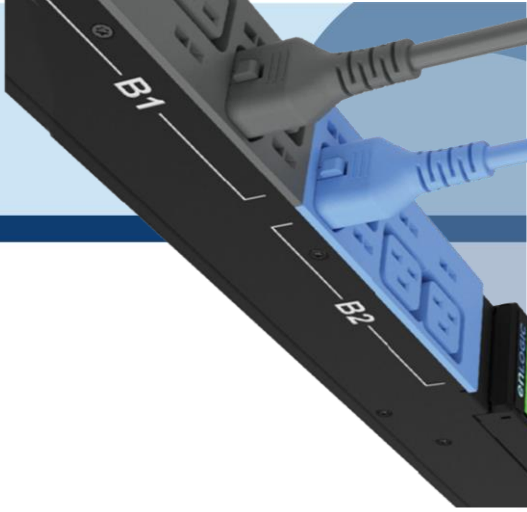


```
          curl -X POST -H "Content-Type: application/json" -d '{ "cookie": 1375552878, "main": { "v12_enable": false, "v3_enable": true, "sys_contact": "", "sys_name": "",
"sys_location": "", "trap_enable": true,  "snmp_port": 161, "trap_port": 162, "snmp_enable": true, "snmp_version": "V3" } }' -k https://10.88.0.82/xhrsnmppost.jsp
```

Note *- the response {"upstatus":1} – This response confirms the command executed gracefully.*

Curl Command formatted:

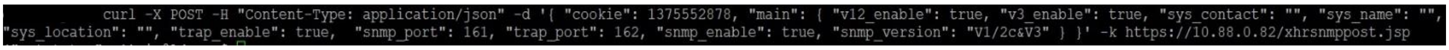
```
curl -X POST \
 -H \"Content-Type: application/json" \
 -d '{
        "cookie": 1375552878,
        "main":
        {
                "v12_enable": false,
                "v3_enable": true,
                "sys_contact": "",
                "sys_name": "",
                "sys_location": "",
                "trap_enable": true,
                "snmp_port": 161,
                "trap_port": 162,
                "snmp_enable": true,
                "snmp_version": "V3"
        } }'
 -k https://10.88.0.82/xhrsnmppost.jsp
```



Curl Command TO SET V1/V2 & V3:

curl -X POST -H "Content-Type: application/json" -d '{ "cookie": 1375552878, "main": { "v12_enable": true, "v3_enable": true, "sys_contact": "", "sys_name": "", "sys_location": "", "trap_enable": true, "snmp_port": 161, "trap_port": 162, "snmp_enable": true, "snmp_version": "V1/2c&V3" } }' -k https://10.88.0.82/xhrsnmppost.jsp

Screen capture from LINUX box.

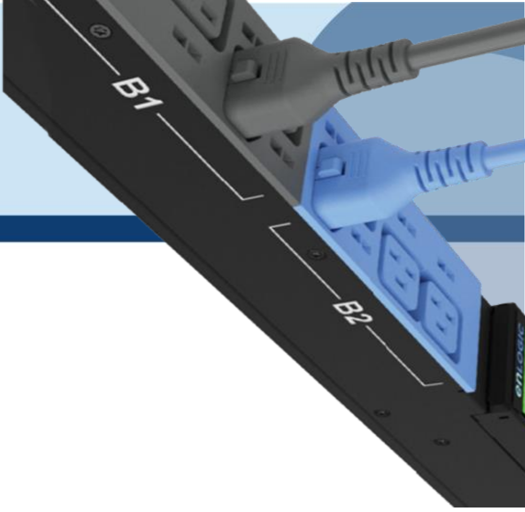


```
         curl -X POST -H "Content-Type: application/json" -d '{ "cookie": 1375552878, "main": { "v12_enable": true, "v3_enable": true, "sys_contact": "", "sys_name": "",
"sys_location": "", "trap_enable": true,  "snmp_port": 161, "trap_port": 162, "snmp_enable": true, "snmp_version": "V1/2c&V3" } }' -k https://10.88.0.82/xhrsnmppost.jsp
```

Note *- the response {"upstatus":1} – This response confirms the command executed gracefully.*

Curl Command formatted:

```
curl -X POST \
 -H "Content-Type: application/json" \
 -d '{
        "cookie": 1375552878,
        "main":
        {
               "v12_enable": true,
               "v3_enable": true,
               "sys_contact": "",
               "sys_name": "",
               "sys_location": "",
               "trap_enable": true,
               "snmp_port": 161,
               "trap_port": 162,
               "snmp_enable": true,
               "snmp_version": "V1/2c&V3"
} }' \
 -k https://10.88.0.82/xhrsnmppost.jsp
```

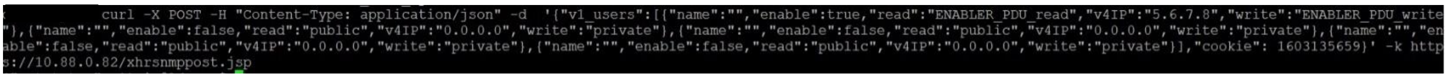


7. SNMP COMMUNITY STRING [READ/WRITE]:

Curl Command:

```
curl -X POST -H "Content-Type: application/json" -d
'{"v1_users":[{"name":"","enable":true,"read":"ENABLER_PDU_read","v4IP":"5.6.7.8","write":"ENABLER_PDU_write"},
{ "name":"","enable":false,"read":"public","v4IP":"0.0.0.0","write":"private"},{"name":"","enable":false,"read":"p
ublic","v4IP":"0.0.0.0","write":"private"},{"name":"","enable":false,"read":"public","v4IP":"0.0.0.0","write":"p
rivate"},{"name":"","enable":false,"read":"public","v4IP":"0.0.0.0","write":"private"}],"cookie": 1603135659}' k
https://10.88.0.82/xhrsnmppost.jsp
```

Screen capture from LINUX box.

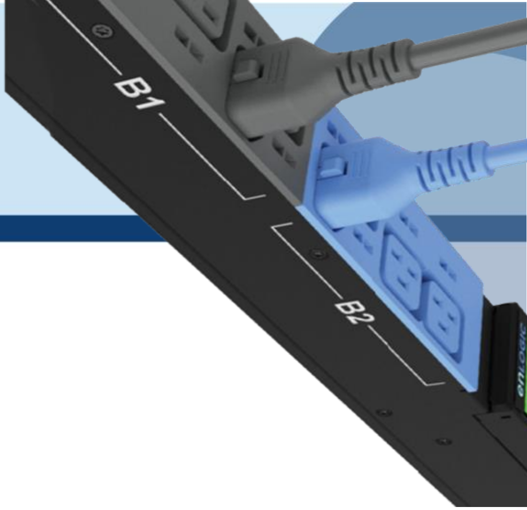


```
[redacted]  curl -X POST -H "Content-Type: application/json" -d  '{"v1_users":[{"name":"","enable":true,"read":"ENABLER_PDU_read","v4IP":"5.6.7.8","write":"ENABLER_PDU_write
"},{"name":"","enable":false,"read":"public","v4IP":"0.0.0.0","write":"private"},{"name":"","enable":false,"read":"public","v4IP":"0.0.0.0","write":"private"},{"name":"","en
able":false,"read":"public","v4IP":"0.0.0.0","write":"private"},{"name":"","enable":false,"read":"public","v4IP":"0.0.0.0","write":"private"}],"cookie": 1603135659}' -k http
s://10.88.0.82/xhrsnmppost.jsp
```

***Note** - the response {"upstatus":1} – This response confirms the command executed gracefully.*

Curl Command formatted:

```
curl -X POST \
 -H "Content-Type: application/json" \
 -d  '{
        "v1_users":
        [
               {
                      "name":"",
                      "enable":true,
                      "read":"ENABLER_PDU_read",
                      "v4IP":"5.6.7.8",
                      "write":"ENABLER_PDU_write"
               },
               {
                      "name":"",
                      "enable":false,
                      "read":"public",
                      "v4IP":"0.0.0.0",
                      "write":"private"
               },
               {
                      "name":"",
                      "enable":false,
                      "read":"public",
                      "v4IP":"0.0.0.0",
                      "write":"private"
               },
               {
                      "name":"",
                      "enable":false,
                      "read":"public",
                      "v4IP":"0.0.0.0",
                      "write":"private"
               },
               {
                      "name":"",
                      "enable":false,
                      "read":"public",
                      "v4IP":"0.0.0.0",
                      "write":"private"
               }
               ],
               "cookie": 1603135659}' \
 -k https://10.88.0.82/xhrsnmppost.jsp
```



8. CHANGE DHCP/IP SETTINGS:

FROM DHCP TO STATIC

First set the IP Configuration from STATIC to DHCP and follow it by a Reset command.

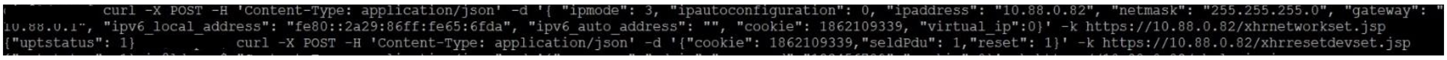
Curl Command:

```
curl -X POST -H 'Content-Type: application/json' -d '{ "ipmode": 3, "ipautoconfiguration": 0, "ipaddress": "10.88.0.82",
"netmask": "255.255.255.0", "gateway": "10.88.0.1", "ipv6_local_address": "fe80::2a29:86ff:fe65:6fda",
"ipv6_auto_address": "", "cookie": 1862109339, "virtual_ip":0}' -k https://10.88.0.82/xhrnetworkset.jsp

curl -X POST -H 'Content-Type: application/json' -d '{"cookie": 1862109339,"seldPdu": 1,"reset": 1}' -k
https://10.88.0.82/xhrresetdevset.jsp
```

Note:

- For Static `ipautoconfiguration` needs to be set as 0
- For DHCP `ipautoconfiguration` needs to be set as 1

Screen capture from LINUX box.



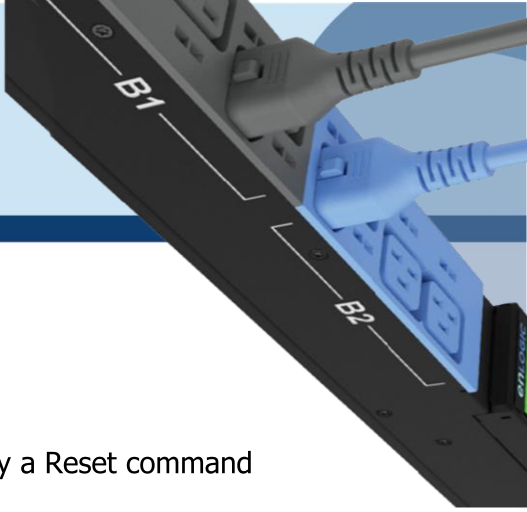
```
[redacted] curl -X POST -H 'Content-Type: application/json' -d '{ "ipmode": 3, "ipautoconfiguration": 0, "ipaddress": "10.88.0.82", "netmask": "255.255.255.0", "gateway": "
10.88.0.1", "ipv6_local_address": "fe80::2a29:86ff:fe65:6fda", "ipv6_auto_address": "", "cookie": 1862109339, "virtual_ip":0}' -k https://10.88.0.82/xhrnetworkset.jsp
{"uptstatus": 1} [redacted] curl -X POST -H 'Content-Type: application/json' -d '{"cookie": 1862109339,"seldPdu": 1,"reset": 1}' -k https://10.88.0.82/xhrresetdevset.jsp
```

Note *- the response {"upstatus":1} – This response confirms the command executed gracefully.*

Any network related data changes, PDU needs to be rebooted. Reset PDU curl command can be used to reboot the PDU CURL

Curl Command formatted:

```
curl -X POST \
 -H 'Content-Type: application/json' \
 -d '{
        "ipmode": 3,
        "ipautoconfiguration": 0,
        "ipaddress": "10.88.0.82",
        "netmask": "255.255.255.0",  "gateway": "10.88.0.1",
        "ipv6_local_address":
        "fe80::2a29:86ff:fe65:6fda",
        "ipv6_auto_address": "",
        "cookie": 1862109339,
        "virtual_ip":0}' \
 -k https://10.88.0.82/xhrnetworkset.jsp
```



FROM STATIC to DHCP

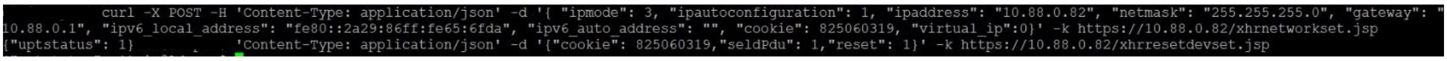
First set the IP Configuration from DHCP to Static and Follow it a by a Reset command

Curl Command:

curl -X POST -H 'Content-Type: application/json' -d '{ "ipmode": 3, "ipautoconfiguration": 1, "ipaddress": "10.88.0.82", "netmask": "255.255.255.0", "gateway": "10.88.0.1", "ipv6_local_address": "fe80::2a29:86ff:fe65:6fda", "ipv6_auto_address": "", "cookie": 1875218967, "virtual_ip":0}' -k https://10.88.0.82/xhrnetworkset.jsp

curl -X POST -H 'Content-Type: application/json' -d '{"cookie": 1875218967,"seldPdu": 1,"reset": 1}' -k https://10.88.0.82/xhrresetdevset.jsp

Screen capture from LINUX box.



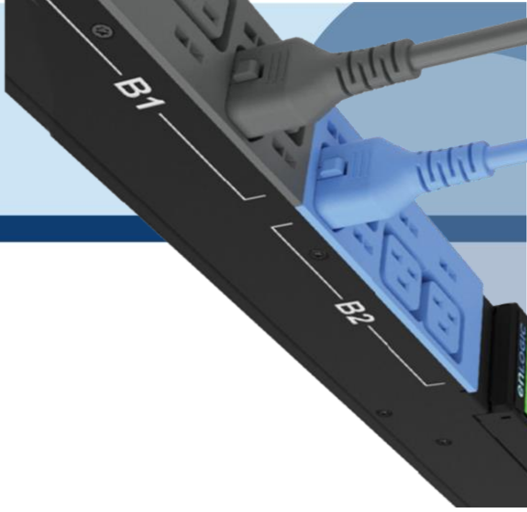
```
          curl -X POST -H 'Content-Type: application/json' -d '{ "ipmode": 3, "ipautoconfiguration": 1, "ipaddress": "10.88.0.82", "netmask": "255.255.255.0", "gateway": "
10.88.0.1", "ipv6_local_address": "fe80::2a29:86ff:fe65:6fda", "ipv6_auto_address": "", "cookie": 825060319, "virtual_ip":0}' -k https://10.88.0.82/xhrnetworkset.jsp
{"uptstatus": 1}            'Content-Type: application/json' -d '{"cookie": 825060319,"seldPdu": 1,"reset": 1}' -k https://10.88.0.82/xhrresetdevset.jsp
```

***Note** - the response {"upstatus":1} – This response confirms the command executed gracefully.*

Any network related data changes, PDU needs to be rebooted. Reset PDU curl command can be used to reboot the PDU CURL

Curl Command formatted:

```
curl -X POST \
 -H 'Content-Type: application/json' \
 -d '{
        "ipmode": 3,
        "ipautoconfiguration": 1,
        "ipaddress": "10.88.0.82",
        "netmask": "255.255.255.0",  "gateway": "10.88.0.1",
        "ipv6_local_address":
        "fe80::2a29:86ff:fe65:6fda",
        "ipv6_auto_address": "",
        "cookie": 40317565,
        "virtual_ip":0}' \
 -k https://10.88.0.82/xhrnetworkset.jsp
```

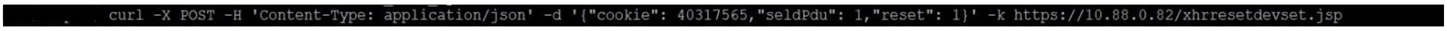


9. RESET PDU:

Curl Command:

```
curl -X POST -H 'Content-Type: application/json' -d '{"cookie": 1862109339,"seldPdu": 1,"reset": 1}' -k
https://10.88.0.82/xhrresetdevset.jsp
```

Screen capture from LINUX box.



```
curl -X POST -H 'Content-Type: application/json' -d '{"cookie": 40317565,"seldPdu": 1,"reset": 1}' -k https://10.88.0.82/xhrresetdevset.jsp
```

***Note** - the response {"upstatus":1} – This response confirms the command executed gracefully.*

To customize and select PDU in Daisy Chain, seldPdu in above could be modified as below seldPdu

= 255 [For All]

= 1 [Master PDU]

= 2 [First Daisy Chain] and so on

Curl Command formatted:

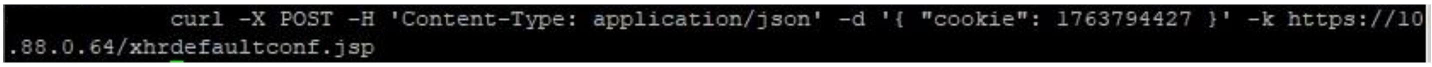
```
curl -X POST \
 -H 'Content-Type: application/json' \
 -d '{
        "cookie": 40317565,
        "seldPdu": 1,
        "reset": 1}' \
-k https://10.88.0.82/xhrresetdevset.jsp
```

RESET PDU TO DEFAULTS

Curl Command:

```
curl -X POST -H 'Content-Type: application/json' -d '{ "cookie": 1763794427 }' -k https://10.88.0.64/xhrdefaultconf.jsp
```

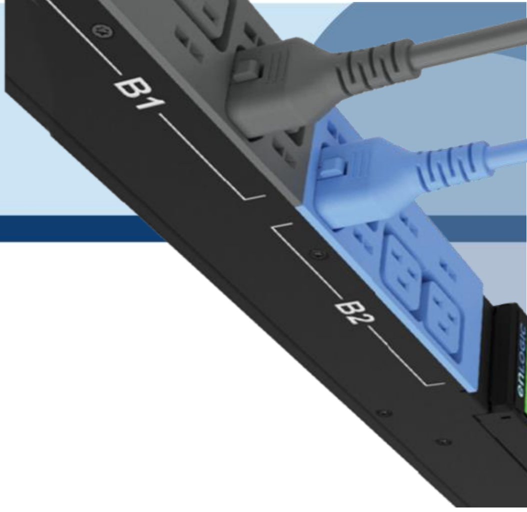
Screen capture from LINUX box.



```
      curl -X POST -H 'Content-Type: application/json' -d '{ "cookie": 1763794427 }' -k https://10
.88.0.64/xhrdefaultconf.jsp
```

Curl Command formatted:

```
curl -X POST \
 -H 'Content-Type: application/json' \
 -d '{
       "cookie": 1763794427 }' \
-k https://10.88.0.64/xhrdefaultconf.jsp
```



10. CONFIGURING NTP SERVER:

Curl Command:

For FIRMWARE <3.1.3

```
curl -X POST -H "Content-Type: application/json" -d
'{"timezone":2803,"date":"111111","time":"014754","chkautotimeadjust":0,"radiouserorntp":2,"ipfirsttimeserv":"139.5
9.15.185","ipesecondtimeserv":"144.24.146.96","offset":0,"cookie":385047644}' -k
https://10.10.105.59/xhrdatetimepost.jsp
```

For FIRMWARE >=3.1.3

```
curl -X POST -H "Content-Type: application/json" -d
'{"timezone":2803,"date":"111111","time":"014754","chkautotimeadjust":0,"radiouserorntp":2,"ipfirsttimeserv":"3.3.3.
3","ipesecondtimeserv":"0.0.0.0","offset":0,"cookie":364319529,"reset": 1,"seldPdu": 1}' -k
https://10.88.0.95/xhrdatetimepost.jsp
```

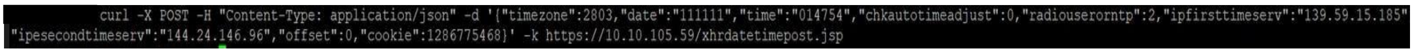
Note:

- Data Body of the command is updated with 2 new parameters which is "reset" and "seldPdu".
- Also PDU will reboot automatically when this curl command is executed
- Curl command will also accept NTP Server IP which is Not-Active

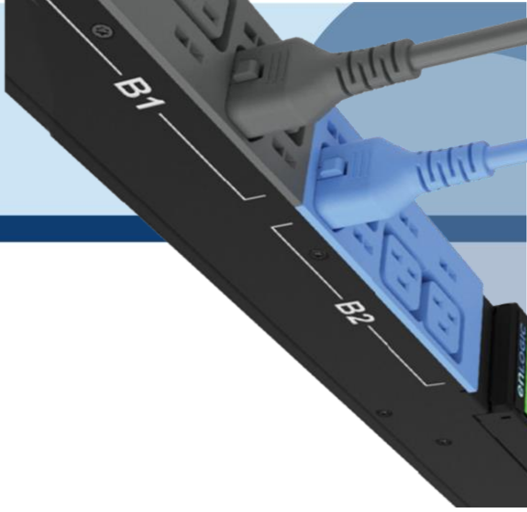
Offset indicates Daylight Saving Time and the Range is as follows:

- 0
- 30 – indicates 30 mins
- 60 – indicates 60 mins

Screen capture from LINUX box.



```
        curl -X POST -H "Content-Type: application/json" -d '{"timezone":2803,"date":"111111","time":"014754","chkautotimeadjust":0,"radiouserorntp":2,"ipfirsttimeserv":"139.59.15.185"
"ipesecondtimeserv":"144.24.146.96","offset":0,"cookie":1286775468}' -k https://10.10.105.59/xhrdatetimepost.jsp
```



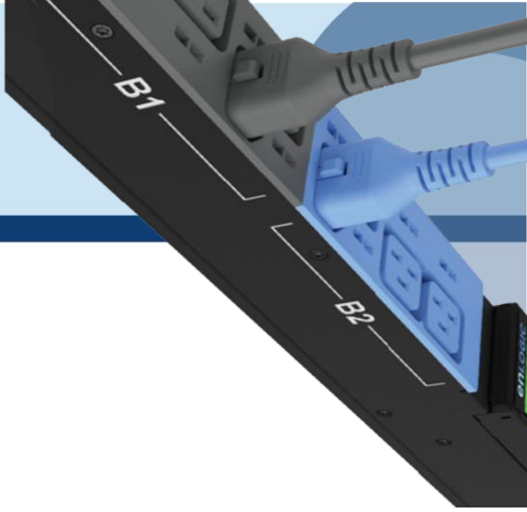
Curl Command formatted:

```
curl -X POST \
-H ‘Content-Type: application/json’ \
-d '{
        "timezone":2803,
        "date":"111111",
        "time":"014754",
        "chkautotimeadjust":0,
        "radiouserorntp":2,
        "ipfirsttimeserv":"139.59.15.185",
        "ipesecondtimeserv":"144.24.146.96",
        "offset":0,
        "cookie":385047644,
        "reset":1,
        "seldPdu":1}' \
-k https://10.10.105.59/xhrdatetimepost.jsp
```

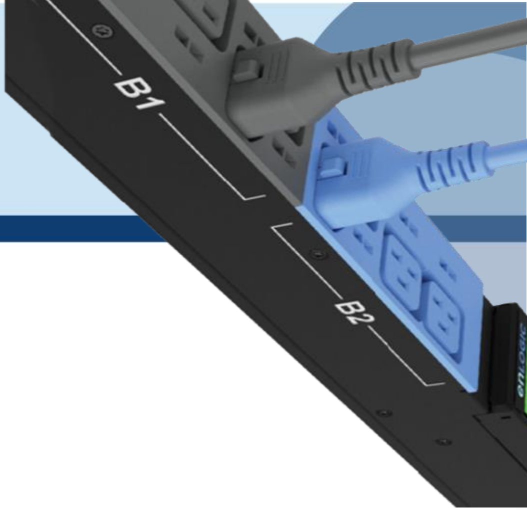
Note: *Make sure the NTP Server are pinging and responds to Requests sent by Client*

Table for Time zone:

Parameters	ENUM
601	(UTC-12:00) International Date Line West
3902	(UTC+13:00) Samoa
801	(UTC-10:00) Hawaii
901	(UTC-09:00) Alaska
1001	(UTC-08:00) Baja California
1002	(UTC-08:00) Pacific Time (US & Canada)
1101	(UTC-07:00) Arizona
1102	(UTC-07:00) Chihuahua, La Paz, Mazatlan
1103	(UTC-07:00) Mountain Time (US & Canada)
1201	(UTC-06:00) Central America
1202	(UTC-06:00) Central Time (US & Canada)
1203	(UTC-06:00) Guadalajara, Mexico City, Monterrey
1204	(UTC-06:00) Saskatchewan
1301	(UTC-05:00) Bogota, Lima, Quito, Rio Branco
1302	(UTC-05:00) Eastern Time (US & Canada)
1303	(UTC-05:00) Indiana (East)
1401	(UTC-04:30) Caracas
1501	(UTC-04:00) Asuncion
1502	(UTC-04:00) Atlantic Time (Canada)
1503	(UTC-04:00) Cuiaba
1504	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
1505	(UTC-04:00) Santiago



Parameters	ENUM
1601	(UTC-03:30) Newfoundland
1701	(UTC-03:00) Brasilia
1702	(UTC-03:00) Buenos Aires
1703	(UTC-03:00) Cayenne, Fortaleza
1704	(UTC-03:00) Greenland
1705	(UTC-03:00) Montevideo
1802	(UTC-02:00) Mid-Atlantic
1901	(UTC-01:00) Azores
1902	(UTC-01:00) Cape Verde Is.
2001	(UTC) Casablanca
2002	(UTC) Coordinated Universal Time
2003	(UTC) Dublin, Edinburgh, Lisbon, London
2004	(UTC) Monrovia, Reykjavik
2101	(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna,
2102	(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague,
2103	(UTC+01:00) Brussels, Copenhagen, Madrid, Paris
2104	(UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb
2105	(UTC+01:00) West Central Africa
2106	(UTC+01:00) Windhoek
2201	(UTC+02:00) Amman
2202	(UTC+02:00) Athens, Bucharest, Istanbul
2203	(UTC+02:00) Beirut
2204	(UTC+02:00) Cairo
2205	(UTC+02:00) E. Europe
2206	(UTC+02:00) Harare, Pretoria
2207	(UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius,
2209	(UTC+02:00) Jerusalem
2301	(UTC+03:00) Baghdad
2303	(UTC+03:00) Kuwait, Riyadh
2304	(UTC+03:00) Nairobi
2503	(UTC+04:00) Moscow, St. Petersburg, Volgograd
2505	(UTC+04:00) Tbilisi
2401	(UTC+03:30) Tehran
2501	(UTC+04:00) Abu Dhabi, Muscat
2502	(UTC+04:00) Baku
2504	(UTC+04:00) Port Louis
2506	(UTC+04:00) Yerevan
2601	(UTC+04:30) Kabul
2701	(UTC+05:00) Islamabad, Karachi
2702	(UTC+05:00) Tashkent
3003	(UTC+06:00) Ekaterinburg
2803	(UTC+05:30) Chennai, Kolkata, Mumbai, Delhi
2804	(UTC+05:30) Sri Jayawardenepura
2901	(UTC+05:45) Kathmandu
3001	(UTC+06:00) Astana
3201	(UTC+07:00) Novosibirsk



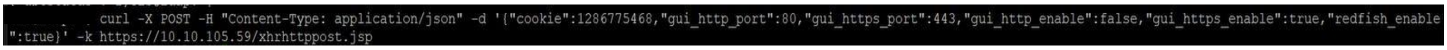
Parameters	ENUM
3201	(UTC+07:00) Bangkok, Hanoi, Jakarta
3302	(UTC+08:00) Krasnoyarsk
3301	(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
3303	(UTC+08:00) Kuala Lumpur, Singapore
3304	(UTC+08:00) Perth
3305	(UTC+08:00) Taipei
3307	(UTC+08:00) Irkutsk
3401	(UTC+09:00) Osaka, Sapporo, Tokyo
3402	(UTC+09:00) Seoul
3605	(UTC+10:00) Yakutsk
3501	(UTC+09:30) Adelaide
3502	(UTC+09:30) Darwin
3601	(UTC+10:00) Brisbane
3602	(UTC+10:00) Canberra, Melbourne, Sydney
3603	(UTC+10:00) Guam, Port Moresby
3604	(UTC+10:00) Hobart
3702	(UTC+11:00) Vladivostok
3701	(UTC+11:00) Solomon Is., New Caledonia
3801	(UTC+12:00) Auckland, Wellington
3803	(UTC+12:00) Fiji
3804	(UTC+12:00) Petropavlovsk-Kamchatsky - Old
3901	(UTC+13:00) Nuku'alofa

11. SETTING REDFISH ON/OFF:

Curl Command:

curl -X POST -H "Content-Type: application/json" -d '{"cookie":911630089,"gui_http_port":80,"gui_https_port":443,"gui_http_enable":false,"gui_https_enable":true,"redfish_enable":true}' -k https://10.10.105.59/xhrhttppost.jsp

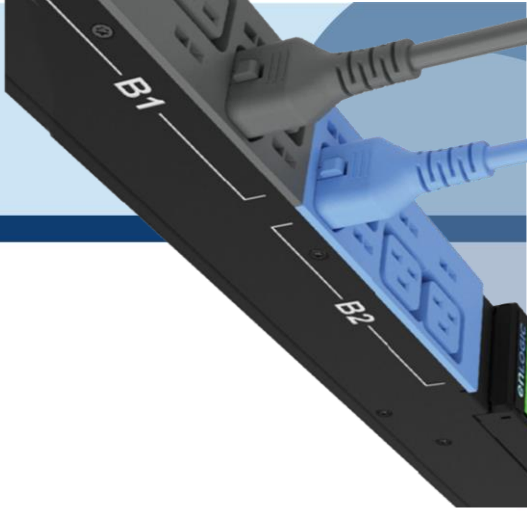
Screen capture from LINUX box.



```
curl -X POST -H "Content-Type: application/json" -d '{"cookie":1286775468,"gui_http_port":80,"gui_https_port":443,"gui_http_enable":false,"gui_https_enable":true,"redfish_enable
":true}' -k https://10.10.105.59/xhrhttppost.jsp
```

Curl Command formatted:

```
curl -X POST -H \
"Content-Type: application/json"
-d '{
        "cookie":911630089,
        "gui_http_port":80,
        "gui_https_port":443,
        "gui_http_enable":false,
        "gui_https_enable":true,
        "redfish_enable":true}' \
-k https://10.10.105.59/xhrhttppost.jsp
```



12. **OUTLET NAME CHANGE:**

RESTAPI THROUGH POSTMAN

URI - https://10.88.0.57/xhroutset.jsp

Method – POST

Body should contain following as payload, note the cookie, cookie needs to be obtained before using this post.

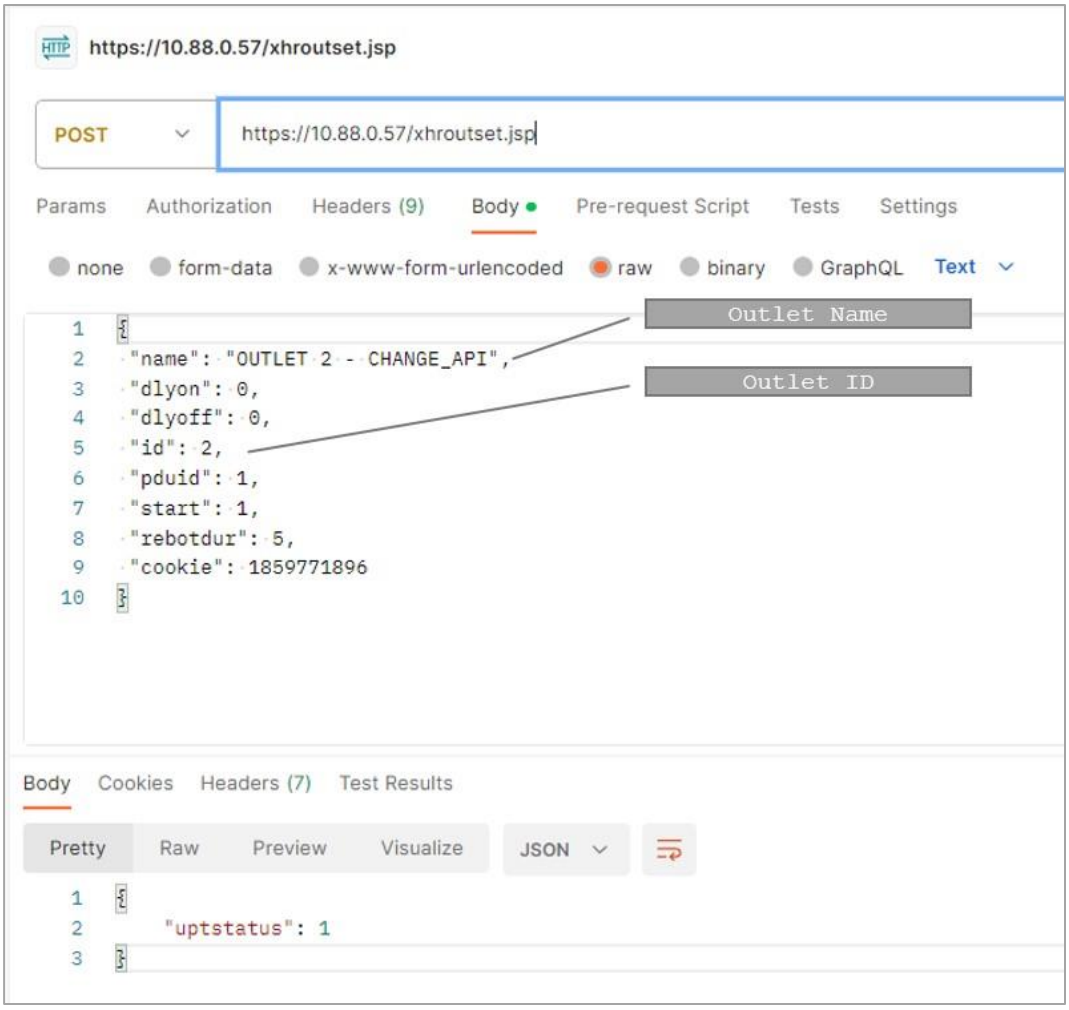
Command formatted:

```
{
 "name": "OUTLET 1 - CHANGE",
 "dlyon": 0,
 "dlyoff": 0,
 "id": 1,
 "pduid": 1,
 "start": 1,
 "rebotdur": 5,
 "cookie": 1908554593 }
```

Note:

- name represents Outlet Name
- dlyon represents On Delay ranging from 0-7200 seconds
- dlyoff represents Off Delay ranging from 0-7200 seconds
- id represents outlet ID. For example to change outlet 2, use id as 2.
- pduid represents daisy chain pdu id.
- start represents ‵State On Startup”. 1 indicates ON, 0 indicates OFF • cookie represents cookie ID

Screen capture from Postman Tool:



https://10.88.0.57/xhroutset.jsp

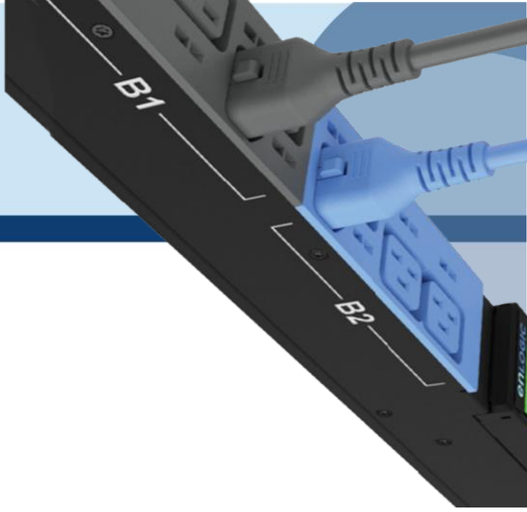
POST https://10.88.0.57/xhroutset.jsp

```
{
 "name": "OUTLET 2 - CHANGE_API",
 "dlyon": 0,
 "dlyoff": 0,
 "id": 2,
 "pduid": 1,
 "start": 1,
 "rebotdur": 5,
 "cookie": 1859771896
}
```

```
{
    "uptstatus": 1
}
```

Curl Command:

```
curl -X POST -H "Content-Type: application/json" -d '{“name": "OUTLET 1 - CHANGE","dlyon": 0,"dlyoff": 0,"id":
1,"pduid": 1,"start": 1,"rebotdur": 5,"cookie": 1908554593}' -k https://10.88.0.57/xhroutset.jsp
```



Curl Command formatted:

```
curl -X POST -H \
"Content-Type: application/json"
-d '
{
        "name": "OUTLET 1 - CHANGE",
        "dlyon": 0,
        "dlyoff": 0,
        "id": 1,
        "pduid": 1,
        "start": 1,
        "rebotdur": 5,
        "cookie": 1908554593
}' \
-k https://10.88.0.57/xhroutset.jsp
```

13. OUTLET CONTROL ENABLE & DISABLE:

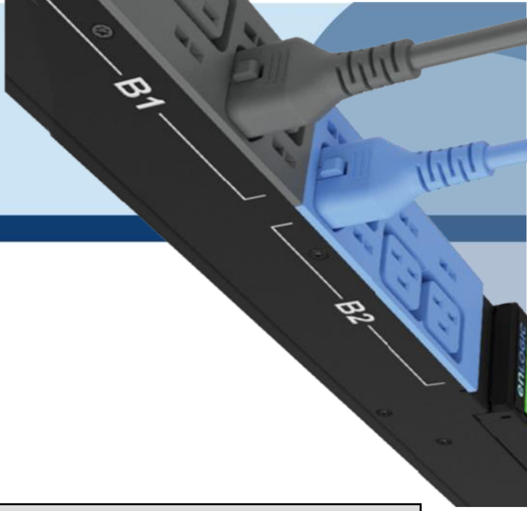
Curl Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"cookie": 1519923071,"enable": 1}' -k
https://10.88.0.57/outlet_control_enable_set
```

Command formatted:

```
curl -X POST -H \
"Content-Type: application/json" \
-d '
{
        "cookie": 1519923071,
        "enable": 1
}'\
-k https://10.88.0.57/outlet_control_enable_set
```

Parameters	Type	Range
cookie	int	Retrieved from Session Token
enable	int/Flag	0 Or 1



14. OUTLET CONTROL ON & OFF:

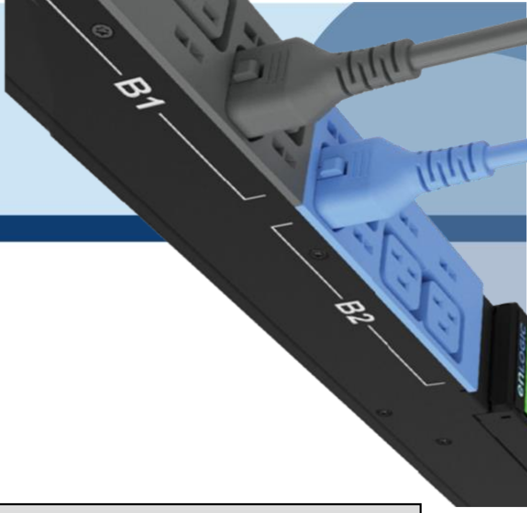
Curl Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"cookie": 1519923071,"outlet1": 2,"outlet2": 0,"pduid": 1,"powstat": 0}' -k https://10.88.0.57/xhroutpowstatset.jsp
```

Command formatted:

```
curl -X POST -H \
"Content-Type: application/json" \ -d '
{
     "cookie": 1519923071,
     "outlet1": 2,
     "outlet2": 0,
     "pduid": 1,
     "powstat": 0
}' \
-k https://10.88.0.57/xhroutpowstatset.jsp
```

Parameters	Type	Range
cookie	int	Retrieved from Session Token
outlet1	int	Outlets 1-24: 2^outlet_no
outlet2	int	Outlets 25-48: 2^(outlet_no - 25)
pduid	int	PDU1-64
powstat	int	0-Off, 1-On, 2-Off Delay, 3-On Delays, 4-Reboot Immediately, 5- Reboot Delayed



15. OUTLET CONTROL WITH DELAYS:

Curl Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"name": "OUTLET 2","dlyon": 5,"dlyoff": 5,"id": 2,"pduid":
1,"start": 1,"rebotdur": 5,"cookie": 1519923071}' -k http://localhost:8080/api/xhroutset.jsp
```

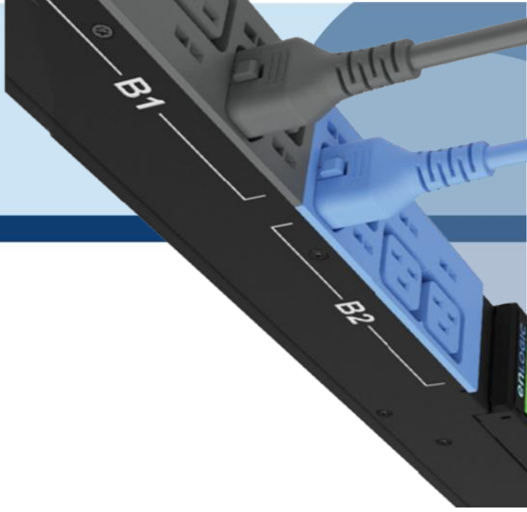
Command formatted:

```
curl -X POST -H \
"Content-Type: application/json" \
-d '\
{
        "name": "OUTLET 2",
        "dlyon": 5,
        "dlyoff": 5,
        "id": 2,
        "pduid": 1,
        "start": 1,
        "rebotdur": 5,
        "cookie": 1519923071
}' \
-k http://localhost:8080/api/xhroutset.jsp
```

Note:

- name represents Outlet Name
- dlyon represents On Delay ranging from 0-7200 seconds
- dlyoff represents Off Delay ranging from 0-7200 seconds
- id represents outlet ID. For example to change outlet 2, use id as 2.
- pduid represents daisy chain pdu id.
- start represents ‘State On Startup”. 1 indicates ON, 0 indicates OFF • cookie represents cookie ID

Parameters	Type	Range
cookie	int	Retrieved from Session Token
name	String	32
dlyon	int	0 to 7200 sec
dlyoff	int	0 to 7200 sec
id	int	Outlet Number (1-48/64)
pduid	int	PDU1-64
rebotdur	int	5 to 60 sec
start	Int/Enum	0- Off, 1 - On, 2- Last Known

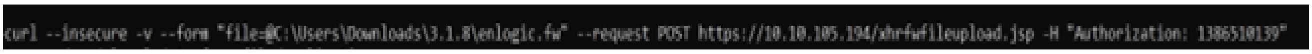


16. FIRMWARE UPLOAD USING API:

Curl Command:

```
curl --insecure -v --form "file=@C:\Users\Downloads\3.1.8\enlogic.fw" --request POST
https://10.10.105.194/xhrfwfileupload.jsp  -H "Authorization: 1386510139"
```

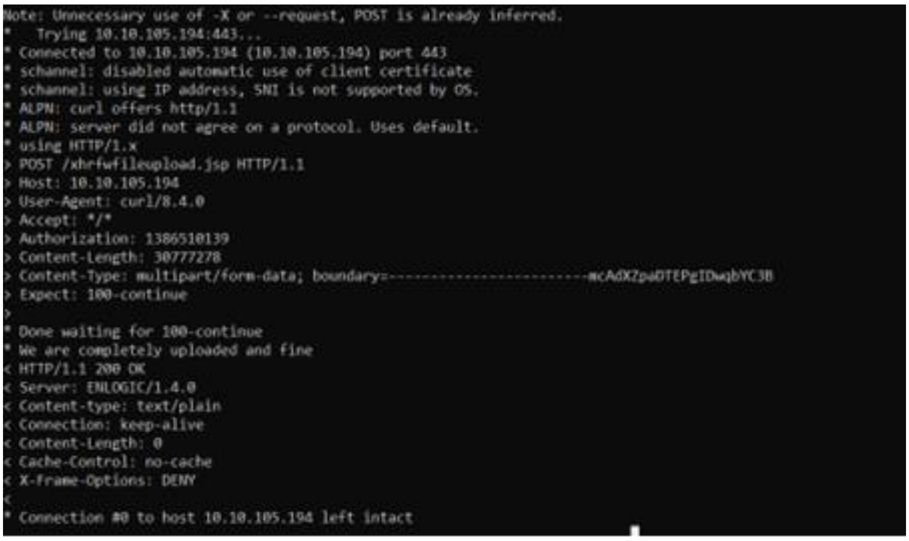
Screen capture from LINUX box.



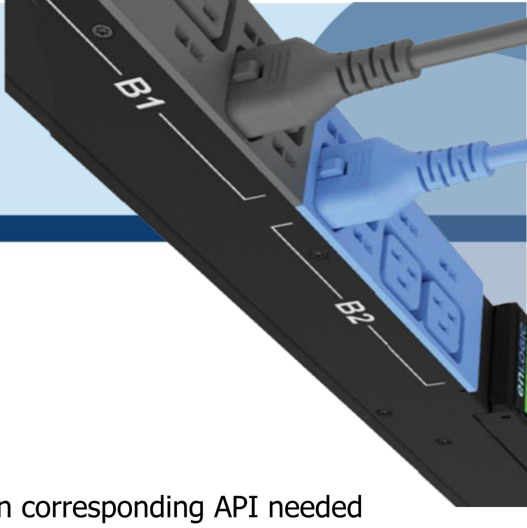
```
curl --insecure -v --form "file=@C:\Users\Downloads\3.1.8\enlogic.fw" --request POST https://10.10.105.194/xhrfwfileupload.jsp -H "Authorization: 1386510139"
```

Note- *the response HTTP/1.1 200 OK – This response confirms the command executed gracefully. This command works only in the Windows Command prompt.*

Response:



```
Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 10.10.105.194:443...
* Connected to 10.10.105.194 (10.10.105.194) port 443
* schannel: disabled automatic use of client certificate
* schannel: using IP address, SNI is not supported by OS.
* ALPN: curl offers http/1.1
* ALPN: server did not agree on a protocol. Uses default.
* using HTTP/1.x
> POST /xhrfwfileupload.jsp HTTP/1.1
> Host: 10.10.105.194
> User-Agent: curl/8.4.0
> Accept: */*
> Authorization: 1386510139
> Content-Length: 30777278
> Content-Type: multipart/form-data; boundary=------------------------mcAdXZpaDTEPgIDwqbYC3B
> Expect: 100-continue
>
* Done waiting for 100-continue
* We are completely uploaded and fine
< HTTP/1.1 200 OK
< Server: ENLOGIC/1.4.0
< Content-type: text/plain
< Connection: keep-alive
< Content-Length: 0
< Cache-Control: no-cache
< X-Frame-Options: DENY
<
* Connection #0 to host 10.10.105.194 left intact
```



RESTAPI – FIRMWARE UPLOAD FLOW

Summary:

Here is the basic workflow of the Firmware upload process and then corresponding API needed to perform a FW upload via API.

API's Used:

API Name: xhrlogin.jsp

The **xhrlogin.jsp** API is used to log in to a system and obtain a cookie for subsequent requests.

Authentication

No authentication is required to access this API.

Endpoint

POST /xhrlogin.jsp

This endpoint logs the user into the system and returns a cookie to be used in subsequent requests.

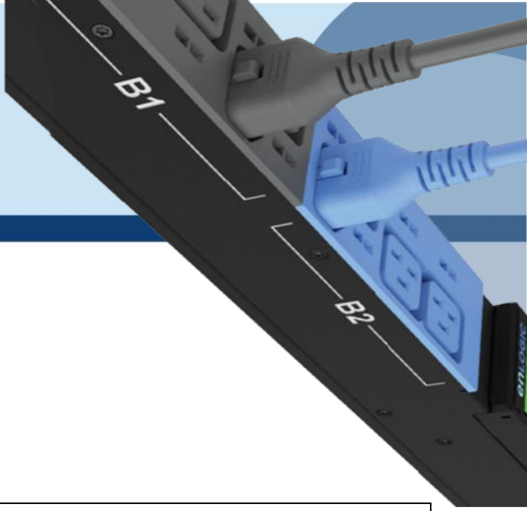
Request Body

The request body must be a JSON object with the following properties:

Property	Type	Required	Description
username	string	Yes	The username of the user to log in
password	string	Yes	The password of the user to log in
cookie	integer	Yes	The initial cookie value for the session

Example Request:

```
{
  "username": "admin",
  "password": "123456789",
  "cookie": 0
}
```



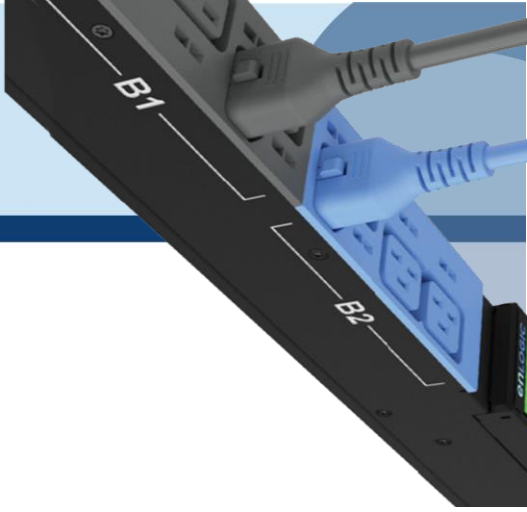
Response Body

The response body is a JSON object with the following properties:

Property	Type	Description
change_password	Boolean	Whether the user is required to change their password
Property	**Type**	**Description**
is_ldap	Boolean	Whether the user is an LDAP user
role	string	The user's role in the system
cookie	integer	The cookie value to be used in subsequent requests
temperature	integer	The temperature of the system (this property is not used and can be ignored)
pdumode	integer	The PDU (Power Distribution Unit) mode of the system (this property is not used and can be ignored)
privilege	integer	The user's privilege level (this property is not used and can be ignored)

Example Response:

```
{
  "change_password": false,
  "is_ldap": false,
  "role": "admin",
  "cookie": 1708930464,
  "temperature": 0,
  "pdumode": 0,
  "privilege": 1701890430
}
```



Response Codes

The xhrlogin.jsp API may return the following HTTP status codes:

Status Code	Description
200	The request was successful
400	The request was invalid or incomplete
401	Invalid Username or Password
427	User is Blocked
500	An error occurred on the server

We need to login to the PDU to get the Token and make use of the token-based authentication.

API Name: xhrfwfilepost.jsp

API Description: This API is used to upload firmware files to the server.

Authentication

Authentication is required to use this API. Users must provide a valid Authorization header in the request.

Endpoint

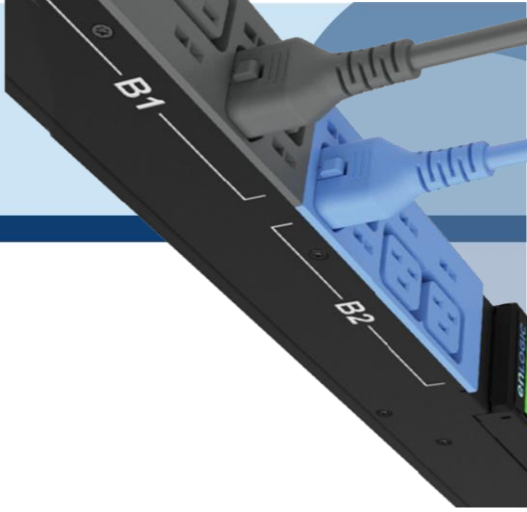
Endpoint: /xhrfwfilepost.jsp

HTTP Method: POST

Description: This endpoint is used to upload firmware files to the server.

Request Headers

Name	Type	Required	Description
Authorization	String	yes	The authorization header containing the authentication token.



Request Body

The request body must contain the firmware file to be uploaded.

Request Example

POST /xhrfwfilepost.jsp HTTP/1.1

Authorization: 1708930464 (cookie value from LOGIN API)

Content-Type: application/octet-stream

<firmware file content>

Response Format

The API returns an HTTP response with the following possible status codes:

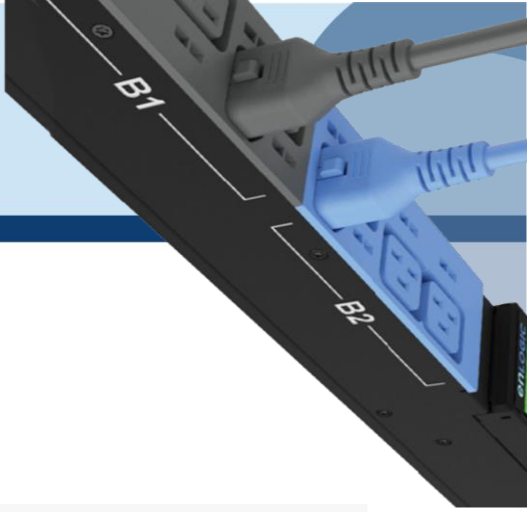
Status Code	**Description**
200	The firmware file was successfully uploaded.
401	The request was not authorized.
427	The File is not uploaded successfully

Response Example

HTTP/1.1 200 OK

HTTP/1.1 401 Unauthorized

This API is responsible for copying over the files to the PDU. The file copy/transfer takes around 2-3 mins. The file is copied to the master PDU and then transferred to the subsequent node PDU in a daisy-chained system.



API Name: xhrsysupddcsend.jsp

API Description: This API is used to send system updates to the device and check the status of the update.

Authentication

Authentication is required to use this API. Users must provide a valid cookie in the request.

Endpoint

Endpoint: /xhrsysupddcsend.jsp

HTTP Method: POST

Description: This endpoint is used to send system updates to the device and check the status of the update. Request Body

Name	Type	Required	Description
cookie	int	yes	The cookie value for the user's session.

Request Example

{"cookie": 1708930464}

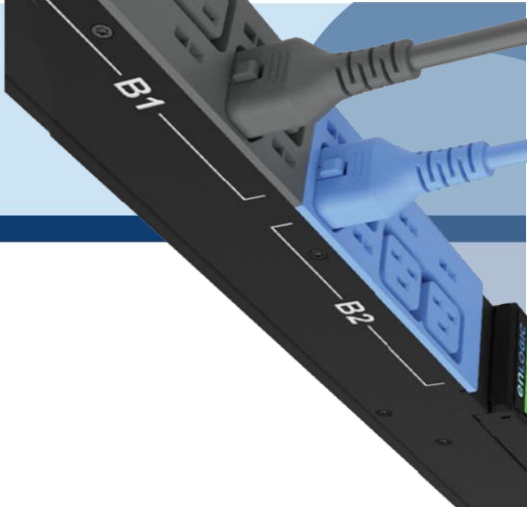
Response

The API returns a JSON object with the following fields:

Field	Type	Description
count	int	The total number of updates being sent.
completed	int	The number of updates that have been completed.
uptstatus	int	The status of the update. Values: 1 (in progress), 0 (failed).
uristatus	int	The status of the URI. Values: 1 (in progress), 2 (completed successfully), 0(failed).

Response Example

```
{
   "count":3,
   "completed":3,
   "uptstatus":1,
   "uristatus":2
}
```



Response Codes

The API may return the following HTTP status codes:

Status Code	Description
200	The request was successful

To check the file is copied over to the entire Daisy-chained system we request this to be running every 30 sec. When uristatus is 2(complete) and the count and completed parameter are matching then we can request the PDU's to be rebooted.

API Name: xhrresetdevset.jsp

API Description: This API is used to reset a device's settings.

Authentication

Authentication is required to use this API. Users must be authenticated using the appropriate credentials before making the request.

Endpoint

Endpoint: /xhrresetdevset.jsp

HTTP Method: POST

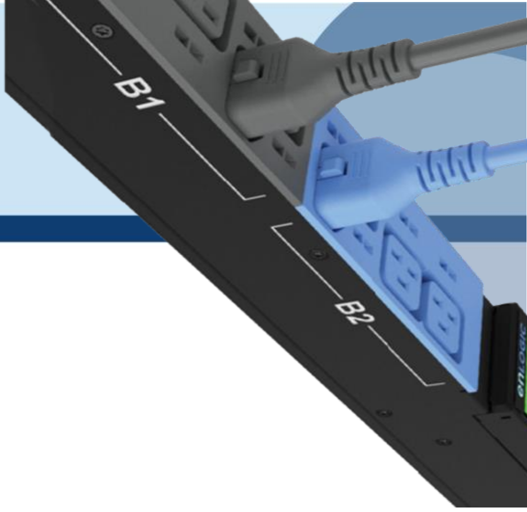
Description: This endpoint is used to reset a device's settings.

Request Headers

This API does not require any request headers.

Request Parameters

Name	Type	Required	Description
cookie	number	yes	The cookie value.
seldPdu	number	yes	The selected PDU value.
reset	number	yes	The reset value.



Request example

POST /xhrresetdevset.jsp HTTP/1.1

Content-Type: application/json

{"cookie":1708930464,"seldPdu":255,"reset":1}

Response Format

The API returns an HTTP response with a JSON object containing the following properties:

Name	Type	Required	Description
uptstatus	number	yes	The status of the update operation.

Response example

HTTP/1.1 200 OK

Content-Type: application/json

{"uptstatus": 1}

Parameter seldPdu is set to 255 to reboot all the PD in the Daisy chain.

API Name: xhrgetuserlist.jsp

API Description: This API is used to get the user list as well as the basic info of the PDU’s.

Authentication

No authentication is required to access this API.

Endpoint

Endpoint: /xhrgetuserlist.jsp

HTTP Method: GET

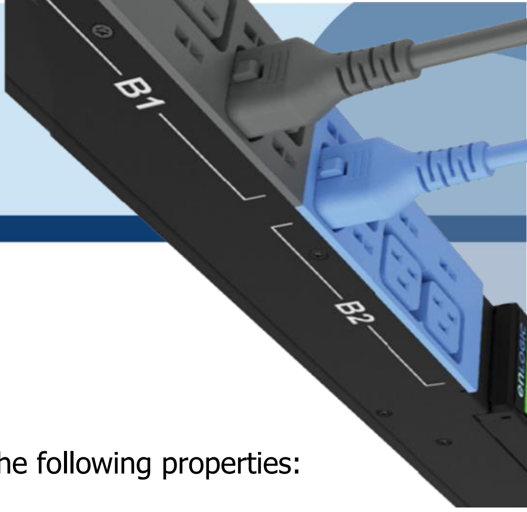
Description: This endpoint is used to get the user list.

Request Headers

This API does not require any request headers.

Request Parameters

This API does not require any request parameters.



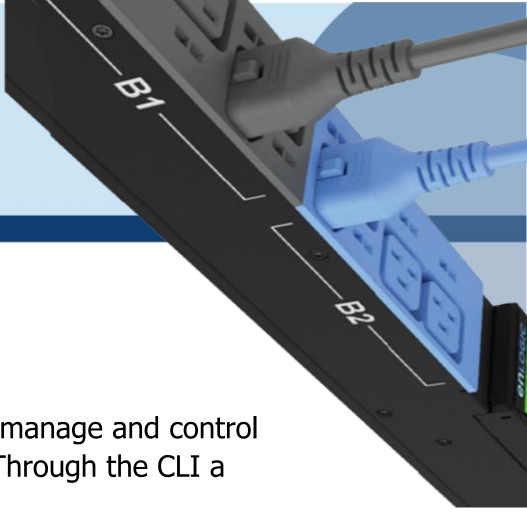
Response Format

The API returns an HTTP response with a JSON object containing the following properties:

Name	Type	Required	Description
fwver	string	yes	The firmware version.
sensor_num	number	yes	The number of sensors.
http	number	yes	HTTP access enabled or not.
https	number	yes	HTTPS access enabled or not.
pdu_type	string	yes	The PDU type.
cbnum	number	yes	The number of circuit breakers.
pdu_num	number	yes	The number of PDUs (Power Distribution Unit).
sku	string	yes	The SKU number.

This API can be used to get the current version of the Firmware and the PDU type (more useful for controlling the outlets based on the type) and basic PDU related info.

The overall time required for the Standalone PDU to perform a Firmware upload is anywhere in between 150-200 seconds. Provided there is no additional traffic coming to the PDU.



The Command Line Interface (CLI)

The Command Line Interface (CLI) is an alternate method used to manage and control the PDU status and parameters, as well as basic admin functions. Through the CLI a user can:

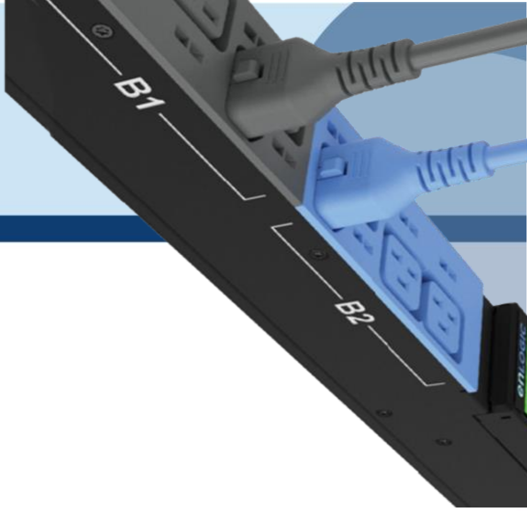
- Reset the PDU
- Display PDU and network properties
- Configure the PDU and network settings
- Switch outlets on/off
- View user information

The CLI can be accessed over a serial connection using a program such as HyperTerminal.

Logging in with HyperTerminal

To login through HyperTerminal, set the COM settings to the following parameters:

- Bits per second: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None



CLI Commands and Prompts

CLI Options

1. To display a list of available options in the CLI, **type '?'** in the command prompt. This will display the 5 main menus and sub menus of command options available: sys, net, usr, dev & pwr.

```
EN2.0>?
```

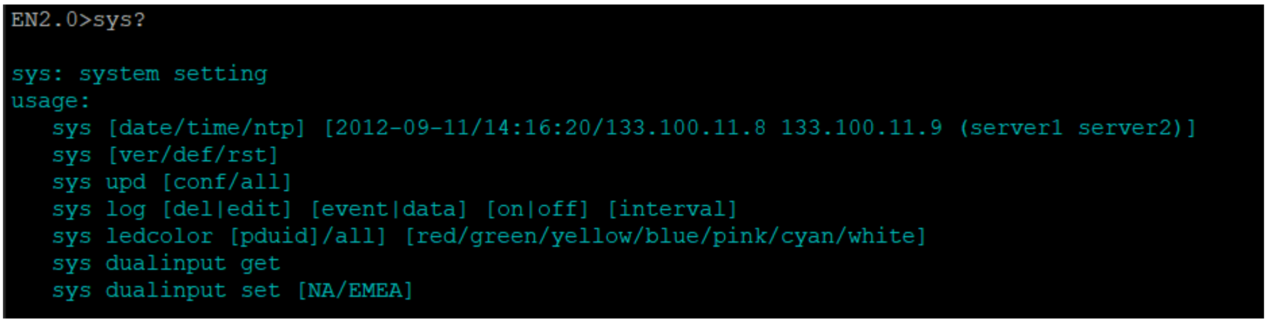
```
sys: system setting
usage:
   sys [date/time/ntp] [2012-09-11/14:16:20/133.100.11.8 133.100.11.9 (server1 server2)]
   sys [ver/def/rst]
   sys upd [conf/all]
   sys log [del|edit] [event|data] [on|off] [interval]
   sys ledcolor [pduid]/all] [red/green/yellow/blue/pink/cyan/white]
   sys dualinput get
   sys dualinput set [NA/EMEA]


user: user setting
usage:
   usr list
   usr login
   usr unlock [username]

net: network configuration command
usage:
   net [ssh/ftps/http/https/redfish] [on/off]
        net snmp [v1v2c/v3] [on/off]
        net snmp port [portnumber]
        net snmp trap [on/off/port] [portnumber]
        net snmp v1v2c <index> <IPaddress> <Read_community> <Write_community>
<Enable/Disable>
        net snmp v3 <index> <username> <securitylevel[AP/ANP/NANP]>
<Auth_password> <Auth_algo[MD5/SHA]> <Priv_key>
<Priv_algo[DES/AES128/AES192/AES256]>
```

```
<Enable/Disable>
   net [mac/tcpip]
   net tcpip [eth0dhcp/eth1dhcp/eth0static/eth1static ip nm gw]
   net tcpip [v6eth0dhcp/v6eth1dhcp/v6eth0static/v6eth1static ip pl gw]
   net ip [v4] [v6] [v4v6]
   net phy [auto/10100mbps/1gbps]
   net dns [-h <hostname> -d <domain> -s1 <server1> -s2 <server2>]
   net dns [disable/enable] [dnsname/servername]]
   net cert [def]


dev: device setting
usage:
   dev daisy [rna/qna] [init] [create]
   dev outlet pduID [status]
   dev outlet pduID [outletindex] [on/off/rebootdelay/ondelay/offdelay]
   dev [sensor/usb] [on/off]
   dev ledstrip [on/off]
   dev powershare [pduID] [func] [on/off]
   dev handle [pduID] [cold/hot] [lock/unlock]
        dev hid [cold/hot] [lock/unlock]


pwr: pdu information
usage:
   pwr [unit/phase/cb/outlet] [idx]
```

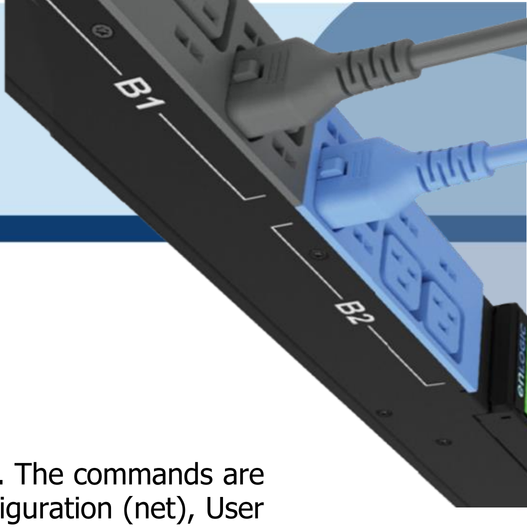
2. To display a list of options available for one of the menus (sys, net, usr, dev or pwr), type the menu command and press enter.

   ***Note**: You can also type the menu command with '?' to show a list of commands*.

For example, below shows the available system options:



```
EN2.0>sys?

sys: system setting
usage:
   sys [date/time/ntp] [2012-09-11/14:16:20/133.100.11.8 133.100.11.9 (server1 server2)]
   sys [ver/def/rst]
   sys upd [conf/all]
   sys log [del|edit] [event|data] [on|off] [interval]
   sys ledcolor [pduid]/all] [red/green/yellow/blue/pink/cyan/white]
   sys dualinput get
   sys dualinput set [NA/EMEA]
```

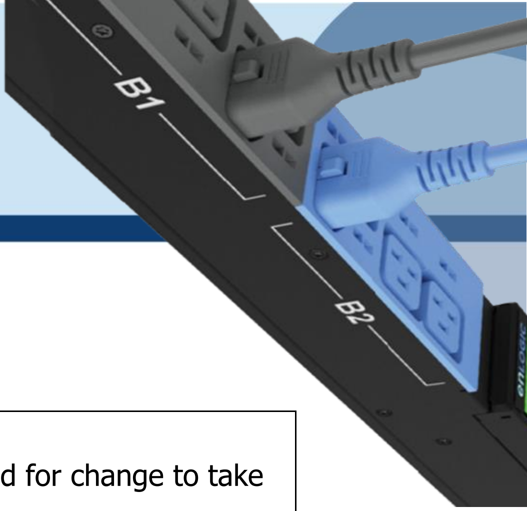


CLI Commands Table

The following is a list of commands available in the CLI to execute. The commands are divided into 5 main categories: System setting (sys), Network configuration (net), User setting (usr), Device setting (dev) and Power (pwr).

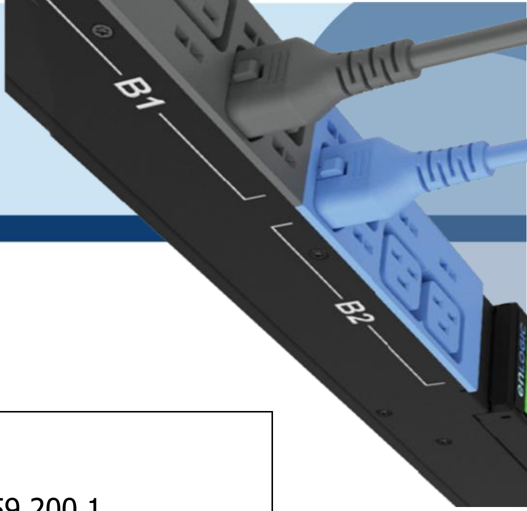
SYS Commands

Sys Commands	Description	Example
sys date [yyyy-mm-dd]	Sets the user input date	EN2.0>sys date 2013-08-12 SUCCESS
sys date	Query on PDU date	EN2.0>sys date SUCCESS Date:2013-08-12 Time:04:58:16
sys time[hh:mm:ss]	Sets the user input time	EN2.0>sys time 09:20:50 SUCCESS
sys time	Query on PDU time	EN2.0>sys time SUCCESS Date:2013-08-12 Time:09:20:53
sys ver	Query on the system versions – firmware, web, boot loader and language version	EN2.0>sys ver SUCCESS Firmware Version: 1.0.6.1 Boot loader Version: 1.1 LANGUAGE Version: 1.01 Web Version: 1.0.5.8
sys def	Set the PDU system to default settings	EN2.0>sys def Reboot required for change to take effort System Reboot now, Are you sure?(Y/N):



SYS Commands

sys rst	Resets the PDU system	EN2.0>sys rst Reboot required for change to take effort System Reboot now, Are you sure?(Y/N):
sys upd [conf/all]	Updates the configuration file	EN2.0>sys upd conf Reboot required for change to take effort System Reboot now, Are you sure?(Y/N):
sys log [del|edit] [event|data] [on|off] [interval]	Edits the data log configuration interval	EN2.0>sys log edit data on 5 SUCCESS EN2.0>sys log edit data off SUCCESS
sys ledcolor [pduid]/all] [dark/red/green/yellow/blue/pink/cyan/white]	Update color of LED	EN2.0>sys ledcolor pduid dark SUCCESS
sys dualinput get	Displays the current region of the PDU	EN2.0>sys dualinput get SUCCESS EMEA rating is active Rating: 346-415V, 32A, 22.0kVA, 50/60Hz
sys dualinput set	Toggle the region of the PDU between NA/EMEA	EN2.0>sys dualinput set NA SUCCESS Input current updated to 24 and voltage updated to 240 Reboot required for change to take effect System Reboot now, Are you sure?(Y/N):Y

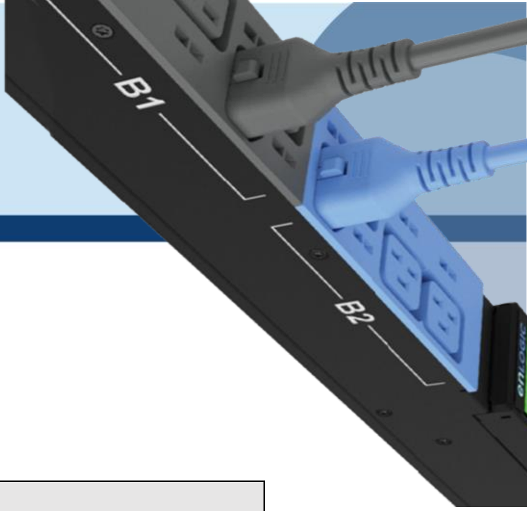


SYS Commands

sys ntp	Displays the primary and secondary IP address of the NTP server & the NTP status	EN2.0>sys ntp SUCCESS Server1 : 162.159.200.1 Server2 : 95.216.144.226 NTP Status : OFF
sys ntp [on/off]	Sets the NTP status to ON/OFF	EN2.0>sys ntp on SUCCESS
sys ntp [primary_ip]	Sets the NTP Primary IP. It is required that the IP address needs to be a valid one.	EN2.0>sys ntp 129.6.15.28 SUCCESS
sys ntp [primary_ip] [secondary_ip]	Sets the NTP It is required that the primary or secondary IP needs to be a valid IP.	EN2.0>sys ntp 129.6.15.28 129.6.15.29 SUCCESS

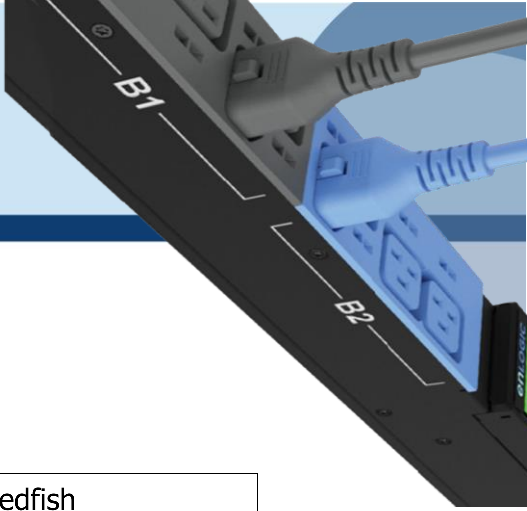
<table>
<tr><td>sys ntp gmtoffset [UTCoffset]</td><td>Sets the UTC code defined for every offset to the PDU for the specific region.
The UTC code can be viewed by entering the NTP help string command.
For setting the NTP offset, NTP needs to be turned ON.</td><td>EN2.0>sys ntp gmtoffset +05:31
SUCCESS
Reboot required for change to take effort
System Reboot now, Are you sure?(Y/N):</td></tr>
<tr><td>sys ntp gmtoffset help</td><td>NTP help string to display the UTC code for every offset of all the region</td><td>EN2.0>sys ntp gmtoffset help
SUCCESS
|Offset | Name | UTC Code

| UTC-12:00 | International Date Line West | -12:00
| UTC-11:00 | Samoa | -11:00</td></tr>
<tr><td>sys ntp gmtoffset</td><td>Displays the current NTP offset of the PDU</td><td>EN2.0>sys ntp gmtoffset
SUCCESS
GMT Name : Chennai, Kolkata, Mumbai, Delhi
GMT Offset : UTC+05:30</td></tr>
</table>

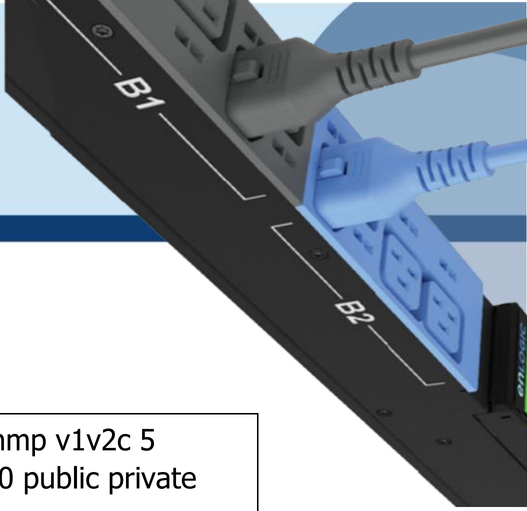


Net Commands

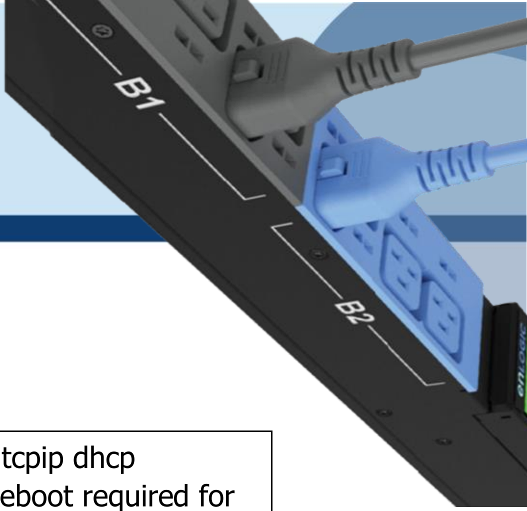
Net Commands	Description	Example
net ssh [on/off]	Sets ssh on/off	EN2.0>net ssh SUCCESS SSH Port: 22 SSH server is running
net ftps [on/off]	Sets ftps on/off	EN2.0>net ftps SUCCESS FTPS Port: 21 Service is running Is Ftp
net http [on/off]	Sets https on/off	EN2.0>net http SUCCESS HTTPS Port: 80 Status: ON EN2.0>net https on Reboot required for change to take effort WEB protocol is changed, reboot to validate System Reboot now, Are you sure?(Y/N):
net https [on/off]	Sets https on/off	EN2.0>net https SUCCESS HTTPS Port: 443 Status: OFF EN2.0>net https on Reboot required for change to take effort WEB protocol is changed, reboot to validate System Reboot now, Are you sure?(Y/N):



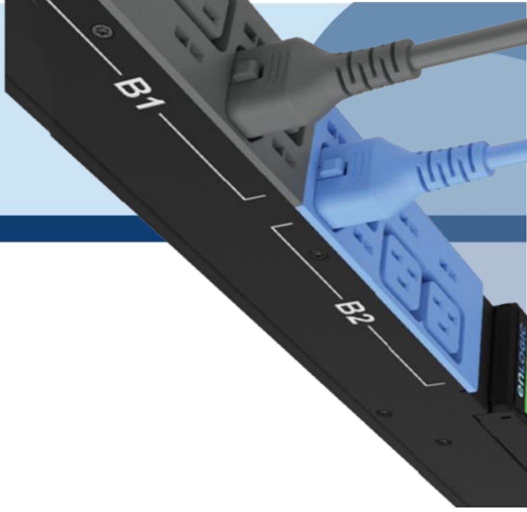
net redfish [on/off]	Sets redfish on/off	EN2.0>net redfish SUCCESS Status: ON EN2.0>net redfish off SUCCESS Status: OFF
net snmp trap [on/off/port] [portnumber]	Changes the snmp trap port number or turns off/on the snmp trap	EN2.0>net snmp trap port 162 Reboot required for change to take effect SNMP trap port is changed, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y



net snmp v1v2c <index> <IPaddress> <Read_community> <Write_community> <Enable/Disable>	Configure the SNMP v1/v2c manager	EN2.0>net snmp v1v2c 5 10.10.105.120 public private enable SUCCESS
net snmp v3 <index> <username> <securitylevel[AP/ANP /NANP]> <Auth_password> <Auth_algo[MD5/SHA]> <Priv_key> <Priv_algo[DES/ AES128/AES192/ AES256]> <Enable/Disable>	Configure the SNMP v3 manager	EN2.0>net snmp v3 3 user1 AP 12345 SHA 12345 AES256 enable SUCCESS
net [mac/tcpip]	Displays the mac address, IPv4	EN2.0>net mac SUCCESS MAC Addr: C8-45-44-66-2B-65 MAC Addr: C8-45-44-66-2B-67 EN2.0>net tcpip SUCCESS eth0 IPv4 Addr: 10.10.105.37 eth0 IPv6 Link Local Addr: fe80:ca45:44ff: fe66:2b65 eth0 IPv6 DHCP Addr: 2001:c0a8: aa01:0:ca45:44ff: fe66:2b65 eth1 IPv4 Addr: 192.168.2.2

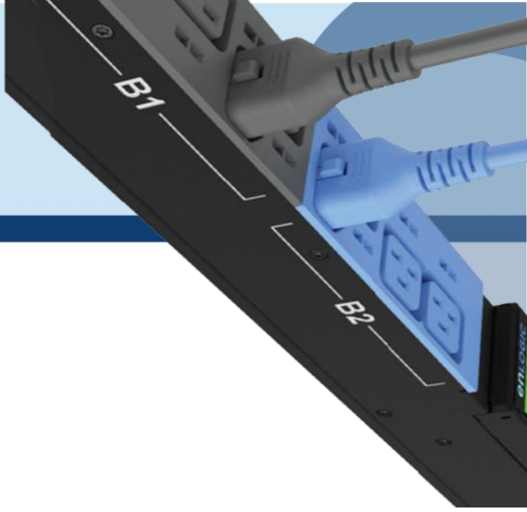


net tcpip [eth0dhcp/eth1dhcp/ eth0static/eth1static ip nm gw]	Changes the IPv4 network to DHCP or Static mode	EN2.0>net tcpip dhcp eth0dhcp Reboot required for change to take effort Network is reconfigured, reboot to validate System Reboot now, Are you sure? (Y/N): Y EN2.0>net tcpip eth1static <10.10.94.20 255.255.255.0 10.10.94.1> Reboot required for change to take effort Network is reconfigured, reboot to validate System Reboot now, Are you sure?(Y/N):Y
net tcpip [v6eth0dhcp/v6eth1dhcp/ v6eth0static/v6eth1static ip pl gw]	Changes the IPv6 network to DHCP or Static mode	EN2.0>net tcpip v6eth0dhcp Reboot required for change to take effect Network is reconfigured, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y

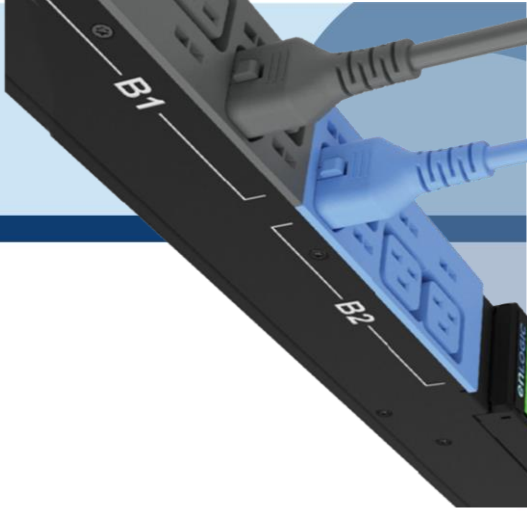


net ip [v4] [v6] [v4v6]	Changes the mode between DUAL, IPv4 or IPv6 Only	EN2.0>net ip SUCCESS IPV4 EN2.0>net ip v6 Reboot required for change to take effort IP protocol is changed, reboot to validate System Reboot now, Are you sure?(Y/N):
net phy [auto/10100mbps/1gbps]	Set the link speed to auto negotiation/10100mbps/1gbps	EN2.0>net phy SUCCESS link speed: auto negotiation EN2.0>net phy 10100mbps Reboot required for change to take effort Phy speed is changed, reboot to validate System Reboot now, Are you sure?(Y/N):

net dns [-h <hostname> -d <domain> -s1 <server1> -s2 <server2>]	Changes the DNS domain name, host name, primary and secondary server	EN2.0>net dns -h admin -d test -s1 10.10.105.20 -s2 10.10.105.21 Reboot required for change to take effect IP protocol is changed, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y
net dns [disable/enable] [dnsname/servername]]	Enables/Disables the DNS server or host by name	EN2.0>net dns enable dnsname Reboot required for change to take effect IP protocol is changed, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y

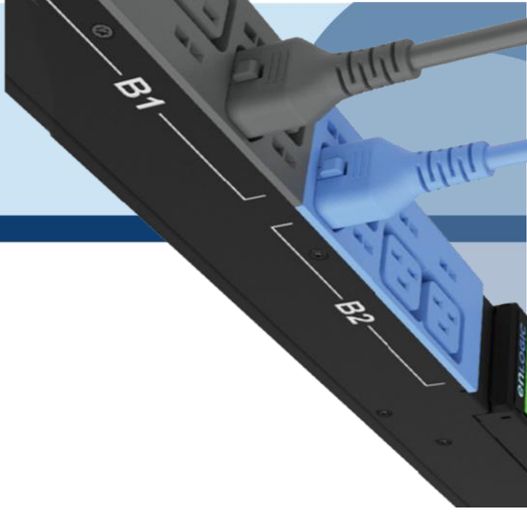


net cert [def]	Updates the certificate file	EN2.0>net cert SUCCESS Custom certificate key file active, in /cert/cert.key Custom certificate cert file active, in /cert/cert.crt EN2.0>net cert def Removing custom certificate key file, in /cert/cert.key Removing custom certificate file, in /cert/cert.crt Reboot required for change to take effect Certificate Setting changed, reboot to validate System Reboot now, Are you sure?(Y/N):



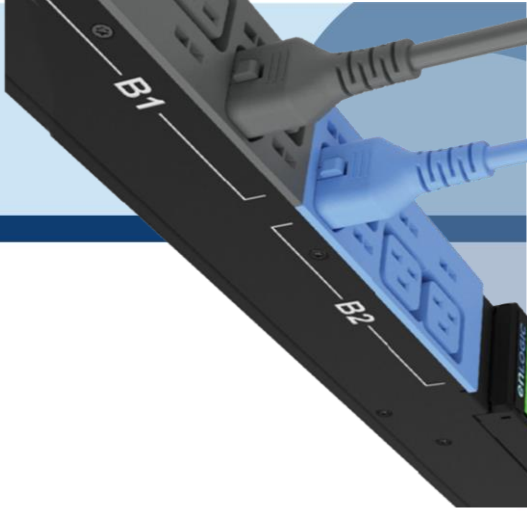
USR Commands

Usr Commands	Description	Example
usr list	Lists out the PDU users	EN2.0>usr list SUCCESS Usr Role Privilege Role id == admin Administrator 1 user 2 manager Administrator 3
usr login	Displays the logged in user details	EN2.0>usr login SUCCESS username: admin ip address: 10.10.94.211 client type: SSH
usr unlock [username]	Unlocks the blocked user	EN2.0>usr unlock en_user SUCCESS

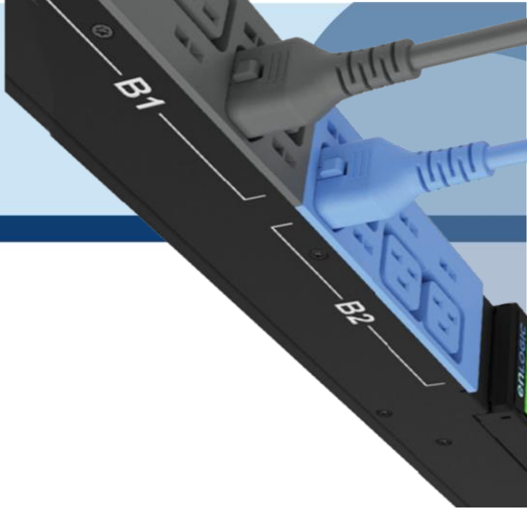


DEV Commands

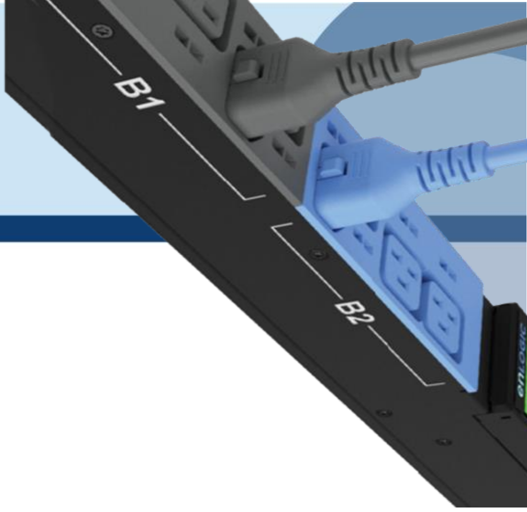
Dev Commands	Description	Example
dev daisy [rna/qna] [init] [create]	Setting the PDU Daisychain to RNA or QNA mode	EN2.0>dev daisy SUCCESS Daisy chain unit number: 1 Daisy chain address list: 0 0 0 Daisy Mode: QNA EN2.0>dev daisy qna create Reboot required for change to take effort System Reboot now, Are you sure?(Y/N):
dev outlet pduID [status]	Displays outlet status.	EN2.0>dev outlet 1 status SUCCESS Relay Outlet Status Outlet# 1: Open Outlet# 2: Open Outlet# 3: Open Outlet# 4: Open Outlet# 5: Open Outlet# 6: Open Outlet# 7: Open Outlet# 8: Open



dev outlet pduID [outletindex] [on/off/rebootdelay/ ondelay/offdelay]	Command to Turn on/off/offdelay/ ondelay/rebootdelay the outlet power	EN2.0>dev outlet 1 1 on SUCCESS EN2.0>dev outlet 1 1 rebootdelay SUCCESS
dev [sensor/usb] [on/off]	Lists out the connected sensors on PDU Turn on/off the USB	EN2.0>dev sensor SUCCESS EN2.0>dev usb on SUCCESS
dev hid [cold/hot] [lock/unlock]	Displays the PDU Rack Access details Locks/Unlocks the HID	EN2.0>dev hid 1 SUCCESS EN2.0>dev hid 1 hot unlock SUCCESS
dev ledstrip [on/off]	Turns on/off the ledstrip	EN2.0>dev ledstrip on SUCCESS

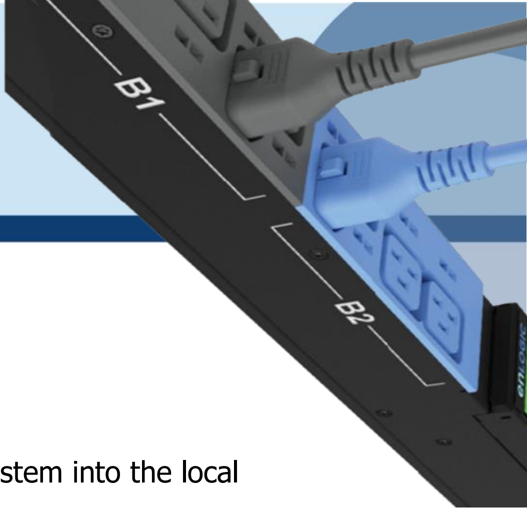


dev powershare	Displays the status of PDU power share	EN2.0>dev power share SUCCESS PDU 1: Downstream: 0 Upstream: 1 Mains: 1 PDU 2: Downstream: 1 Upstream: 1 Mains: 1 PDU 3: Downstream: 1 Upstream: 1 Mains: 1
dev handle [pduID] [cold/hot] [lock/unlock]	Enables handle function	dev handle 1 hot lock



PWR Commands

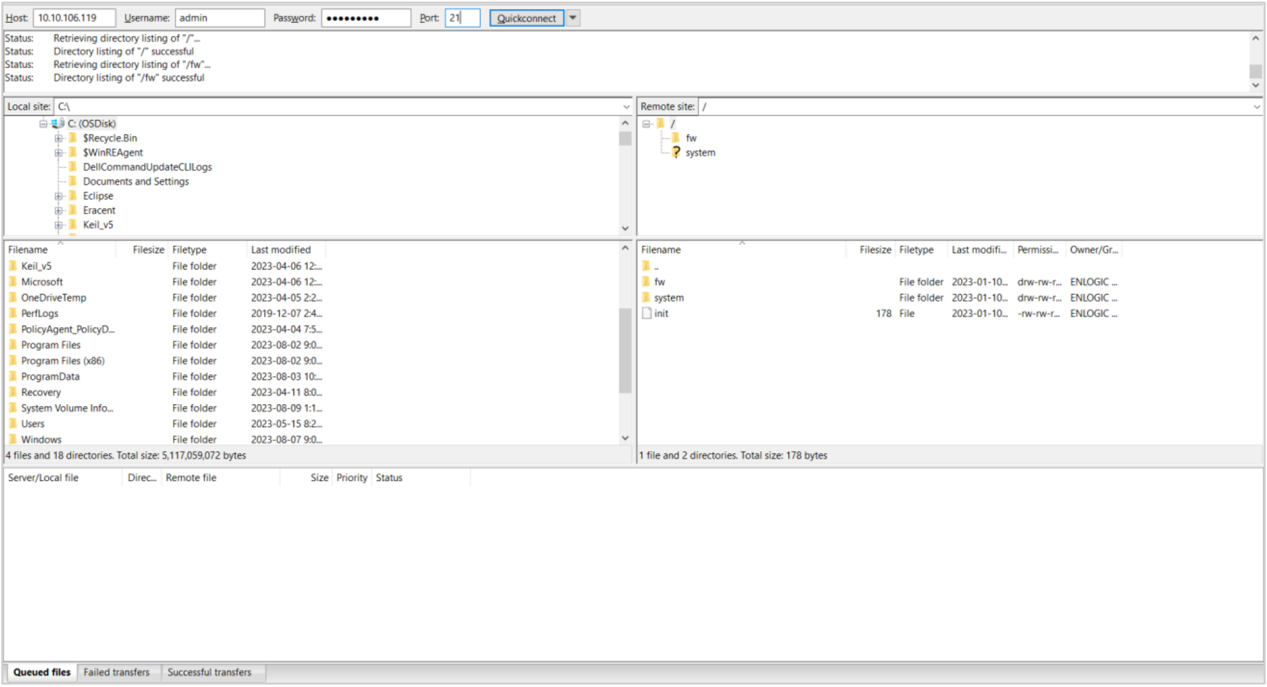
Pwr Commands	Description	Example
pwr [unit/phase/cb/outlet] [idx]	Displays the power readings	EN2.0>pwr unit 1 SUCCESS UNIT power Feature voltage: 0V current: 0.0A active power: 0W apparent power: 0W power factor: 1.00 energy: 0.000kWh EN2.0>pwr outlet 3 SUCCESS OUTLET 3 power Feature voltage: 0V current: 0.0A active power: 0W apparent power: 0W



FTPS

File Transfer Protocol is used to transfer files from the PDU file system into the local drives under a secure network and vice-versa.

1. Enable the FTPS Access through Web UI



Host: 10.10.106.119 Username: admin Password: ●●●●●●●●● Port: 21

```
Status:     Retrieving directory listing of "/"...
Status:     Directory listing of "/" successful
Status:     Retrieving directory listing of "/fw"...
Status:     Directory listing of "/fw" successful
```

Local site: C:\

```
C: (OSDisk)
    $Recycle.Bin
    $WinREAgent
    DellCommandUpdateCLILogs
    Documents and Settings
    Eclipse
    Eracent
    Keil_v5
```

Filename	Filesize	Filetype	Last modified
Keil_v5		File folder	2023-04-06 12:...
Microsoft		File folder	2023-04-06 12:...
OneDriveTemp		File folder	2023-04-05 2:2...
PerfLogs		File folder	2019-12-07 2:4...
PolicyAgent_PolicyD...		File folder	2023-04-04 7:5...
Program Files		File folder	2023-08-02 9:0...
Program Files (x86)		File folder	2023-08-02 9:0...
ProgramData		File folder	2023-08-03 10:...
Recovery		File folder	2023-04-11 8:0...
System Volume Info...		File folder	2023-08-09 1:1...
Users		File folder	2023-05-15 8:2...
Windows		File folder	2023-08-07 9:0...

4 files and 18 directories. Total size: 5,117,059,072 bytes

Remote site: /

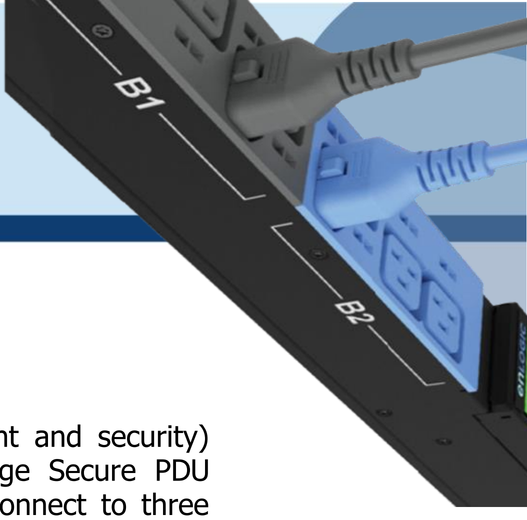
```
/
    fw
    system
```

Filename	Filesize	Filetype	Last modifi...	Permissi...	Owner/Gr...
..					
fw		File folder	2023-01-10...	drw-rw-r...	ENLOGIC ...
system		File folder	2023-01-10...	drw-rw-r...	ENLOGIC ...
init	178	File	2023-01-10...	-rw-rw-r...	ENLOGIC ...

1 file and 2 directories. Total size: 178 bytes

Server/Local file	Direc...	Remote file	Size	Priority	Status

2. Enter the IP address of the PDU at the **Host.**
3. Enter the **Username** and **Password** of a person with the role having administrative privileges.
4. Enter the **Port** number set for the FTPS.
5. Click the **Quickconnect** button to connect the PDU and Local Drive through the FTPS Client.
6. The **Local Site** containing the local drives and **Remote Site** containing the PDU file system comes to view.
7. Using Drag and Drop we can transfer the files between Local and Remote site. We can also use right click and select the upload and download function to perform the file transfer.



Sensors

The Advantage Secure PDU can monitor conditions (environment and security) with Enlogic's sensors. Sensors are connected to the Advantage Secure PDU through the RJ45 connection or Sensor Input Hub, which can connect to three additional sensors. Following are the sensors available:

- Temperature Sensor
- Temperature and Humidity Sensor
- (3) Temperature + (1) Humidity Sensor
- Sensor Input Hub (3 sensor inputs)
- Door Switch Sensor
- Dry Contact Cable
- Spot Fluid Leak Sensor
- Rope Fluid Leak Sensor
- LED Light Strip Sensor
- RJ45-DB9 Cable
- USB to RS232 Cable
- HID RACK Access kit
- ehandle with RFID
- ehandle with RFID + PIN

Sensor Overview

Enlogic sensors allow the users and administrators to monitor, report, and alarm specific conditions in and around a PDU, Inline Meter, and server rack. Conditions such as temperature, humidity, leak, and switches are vital aspects of maintaining an efficient-working data center atmosphere.

Enlogic iPDUs and Inline Meters are designed to collect a maximum of 10 sensor measurements

1. Plug the sensor into the PDU through the RJ45 connection or Sensor Input Hub.

***Note**: It can take 1-3 minutes (depending on model and configuration) for PDU to recognize the sensor.*

2. Log in to the Enlogic Web UI. (The sensors are identified and displayed, after login).

3. Identify each sensor through the serial number in the External Sensors section of the Enlogic Web UI.

4. Make sure that the Advantage Secure PDU begins to automatically manage sensors. If the sensors are not auto managed, refer to the **Viewing and Managing Sensor Information** section.

5. Click **Setup** button to configure the sensor name, description, location, and alarm setup. Refer to the **Viewing and Managing Sensor Information** section for more information.

Temperature and Humidity Sensor Installation Instructions EA9102, EA9103, and EA9105

1. Secure the sensor box to the perforated rack enclosure door by threading a cable tie through the recessed channel in the sensor box and door.

   ***Note**: There are two recessed channels on the back of the sensor box, which is included with a magnet to secure the sensor.*

2. Secure the RJ45 cable along with the desired path to the PDU using the remaining cable ties.
3. For the 3 Temperature and 1 Humidity sensors (model EA9105) only: Secure the two additional temperature probes near the top and the bottom of the perforated rack enclosure door using the cable ties.
4. Use the RJ45 Quick Disconnect Coupler and Ethernet Cable to extend the length of the sensor input cable and/or to serve as an easy disconnect point for rack door removal. Refer to the Advantage Secure User Manual for instructions on, how to create custom cord lengths using the RJ45 Quick Disconnect Coupler.

***Note**: Use either the 1.8m Ethernet cable included with the Enlogic sensor or any other CAT5 or CAT6 Ethernet cable with a standard RJ45 plug.*

5. Plug the sensor cable into the Sensor 1 or Sensor 2 port on the PDU/Inline Energy Meter or the Sensor Hub (model EA9106).

***Note**: It can take 1-3 minutes (depending on model and configuration) for PDU to recognize the sensor.*

6. The Enlogic sensor is installed and ready for use.

Sensor Input Hub Installation Instructions

EA9106

1. Secure the sensor box to the perforated rack enclosure door by threading a cable tie through the recessed channel in the sensor box and door.

   ***Note**: There are two recessed channels on back of the sensor box, which includes the magnet to secure the sensor*.

2. Secure the RJ45 cable along the desired path to the PDU using the remaining cable ties.
3. For the 3 Temperature and 1 Humidity sensors (model EA9105) only: Secure the two additional temperature probes near the top and the bottom of the perforated rack enclosure door using the cable ties.
4. Use the RJ45 Quick Disconnect Coupler and an Ethernet cable to extend the length of the sensor input cable and/or to serve as an easy disconnect point for rack door removal. Refer to the
   Advantage Secure User Manual for instructions on how to create custom cord lengths using the RJ45 Quick Disconnect Coupler.

***Note**: Use either the 1.8m Ethernet cable included with the Enlogic sensor or any other CAT5 or CAT6 Ethernet cable with a standard RJ45 plug*.

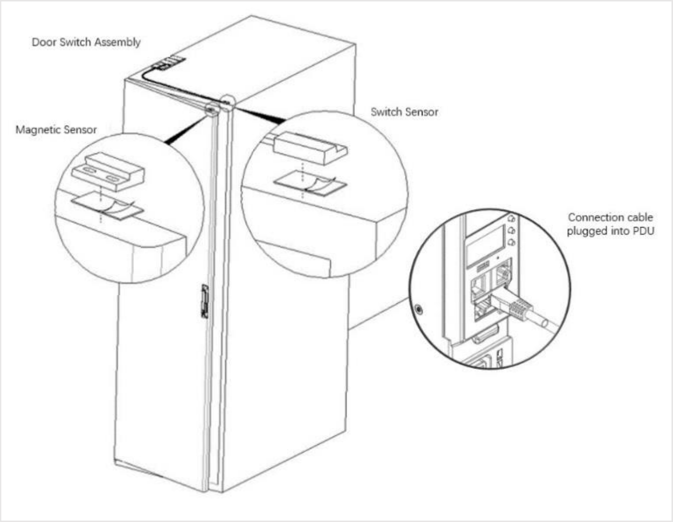
5. Plug the sensor cable into the Sensor 1 or Sensor 2 port on the PDU/Inline Energy Meter or the Sensor Hub (model EA9106).

Door Switch Sensor Installation Instructions

EA9109

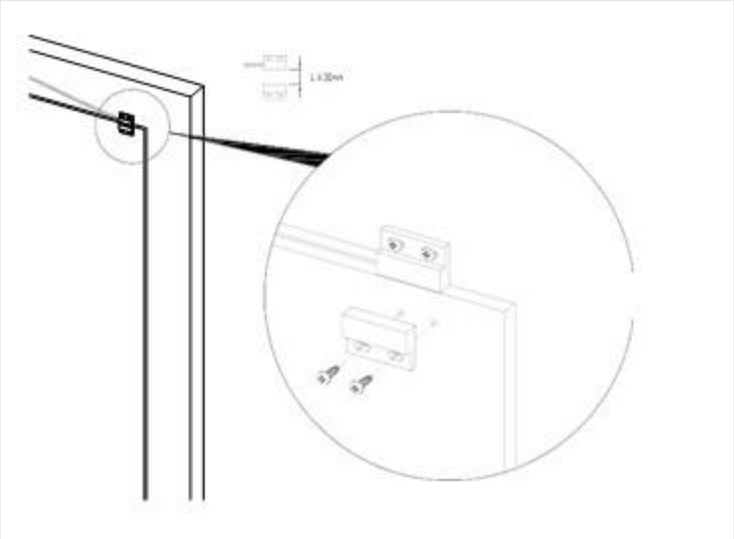
Top Door Mounting Option

1. Attach the door switch assembly to the top of the rack using the Adhesive backed mount and cable ties.
2. Attach the Switch Sensor to the top corner of the rack (on the side that the rack door will close) using double-sided tape. Secure the cable to the top of the rack using cable ties.
3. Attach the Magnetic Sensor to the rack door using double-sided tape.



4. Thread the sensor connection cable through the rack. Secure the cable with cable ties. Plug the cable into a sensor port on the PDU.
5. Log into the Web Interface, or Serial to manage the door sensor alarm and notification settings. The sensor is designed to alarm if the door is opened more than 10 mm.
6. Attach the Door Switch assembly to the top of the rack using the Adhesive backed mount and cable ties.
7. Attach the Switch Sensor to the inside of the rack (on the side that the rack door will close) using 4 screws (FS00041). Secure the cable to the top of the rack using cable ties.
8. Attach the Magnetic Sensor to the rack door using screws.
9. Thread the sensor connection cable through the rack. Secure the cable with cable ties. Plug the cable into a sensor port on the PDU.
10. Log into the Web Interface, or Serial to manage the door sensor alarm and notification settings. The sensor is designed to alarm if the door is opened more than 10 mm.

Door Mounting Option



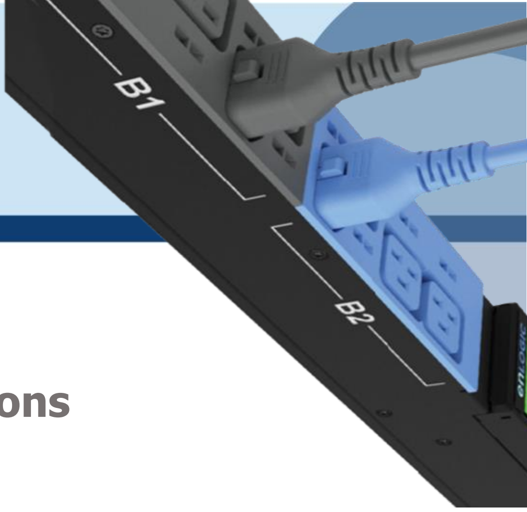
1. Attach the Door Switch assembly to the top of a door jamb using the Adhesive backed mount and cable ties.

2. Attach the Switch Sensor to the door (on the side that the rack do0g5000000000vv0or will close) using the 4 screws (FS00041). Secure the cable to the top of the rack using cable ties.

3. Attach the Magnetic Sensor to the rack door using screws.

4. Thread the sensor connection cable through the rack. Secure the cable with cable ties. Plug the cable into a sensor port on the PDU.

5. Log into the Web Interface, or Serial to manage the Door Sensor alarm and notification settings. The sensor is designed to alarm if the door is opened more than 10mm.



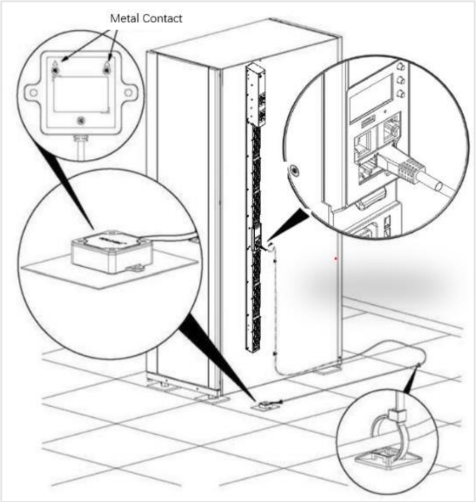
Dry Contact Cable Installation Instructions

EA9110

1. Attach the open wire leads on the dry contact cable to a dry contact sensor. *Refer to instructions for the dry contact sensor for this step.*
2. Connect the RJ-45 jack of the Enlogic Dry Contact Cable to a sensor port on the PDU, Inline Energy Meter, or Sensor Hub (model EA9106).
3. Go to the Enlogic Web UI to setup specific conditions to monitor and alarm for this sensor.

Spot Fluid Leak Sensor Installation Instructions

EA9111

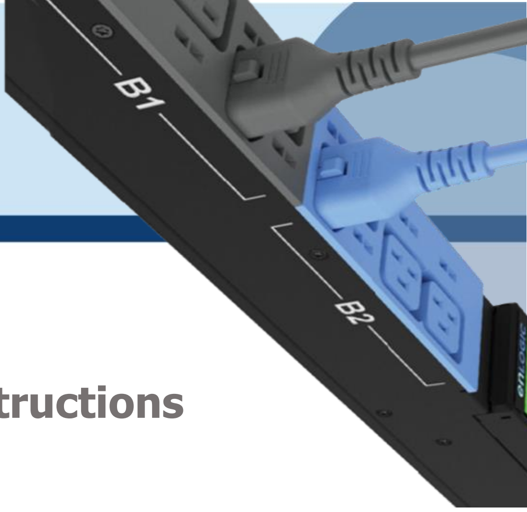


1. Place the fluid sensor on the surface to be monitored. Secure the cable using cable ties and/or adhesive mounts.

   ***Note**: The Spot Fluid Leak Sensor uses electronic circuits to detect the presence of liquid. Certain materials, such as metal surfaces or cement floor, can activate a false leak signal. To avoid this occurrence, place the sensor on the installation pad, (provided). The installation pad is best to install on a clean, dry surface.*

2. Plug the RJ-45 cable into a sensor port on the Enlogic iPDU, Inline Energy Meter, or Sensor Hub (model EA9106)

3. Go to the Enlogic Web UI to setup specific conditions to monitor and alarm for this sensor.



Rope Fluid Leak Sensor Installation Instructions EA9112

1. Connect the RJ-45 jack on the Rope Fluid Leak Sensor assembly to a sensor port on the Enlogic iPDU, Inline Energy Meter, or Sensor Hub (model EA9106).

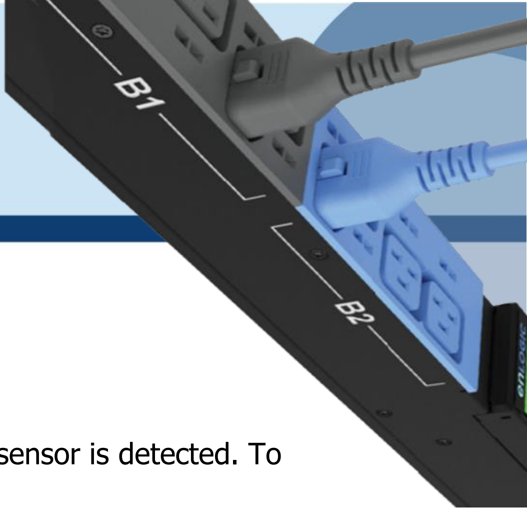
2. Thread the Rope Fluid Leak Sensor cable (EW00253) through the rack and along the desired path of detection.

   ***Note**: Up to 5 Rope Fluid Leak Sensor Cables can be connected to lengthen the detection zone. These can be purchased through Enlogic*.

3. Secure the Rope Fluid Leak Sensor cable to the rack and ground using the cable ties and/or adhesive mounting strips provided.

   Note:

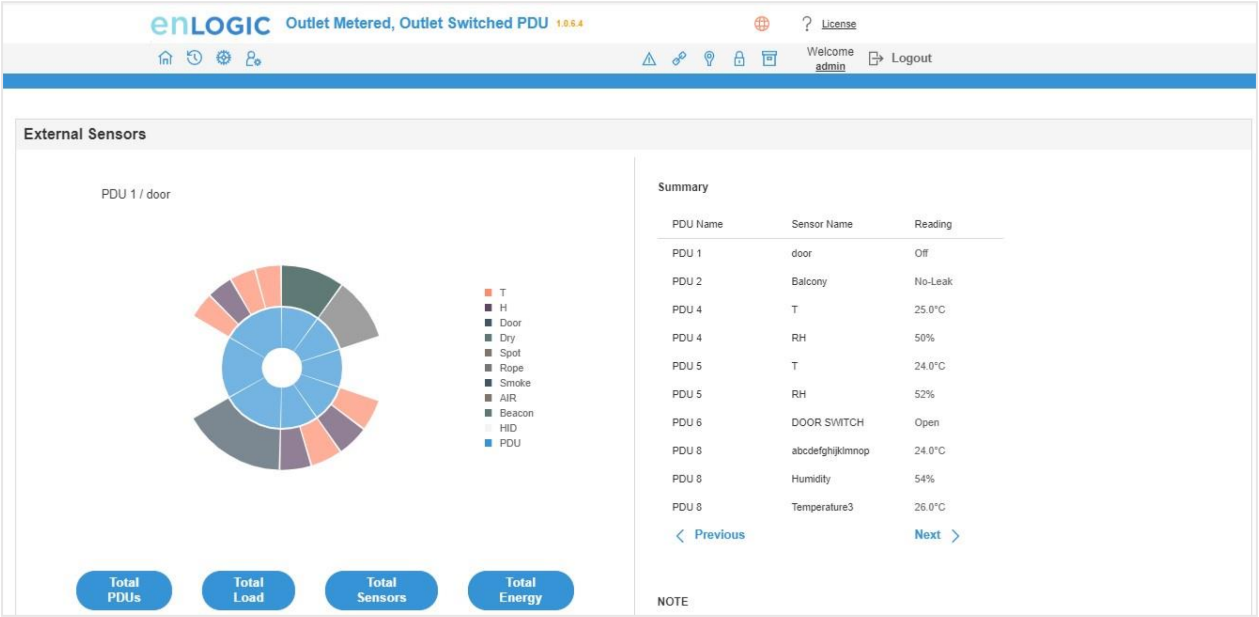
   - *The wire mount (shown here) is for installation on the floor or ground surface. This must be used in the detection area.*
   - *If mounting to a cabinet or wall, use the adhesive-backed mount (provided). The adhesive backed is mounted in the detection area to prevent and notify delay leakage.*



Detecting Sensors

The sensor serial number is listed in the Enlogic Web UI when the sensor is detected. To identify each detected sensor:

1. Go to Overview/Dashboard
2. Select **Total Sensors** to view all connected sensors



External Sensors

PDU 1 / door

Summary

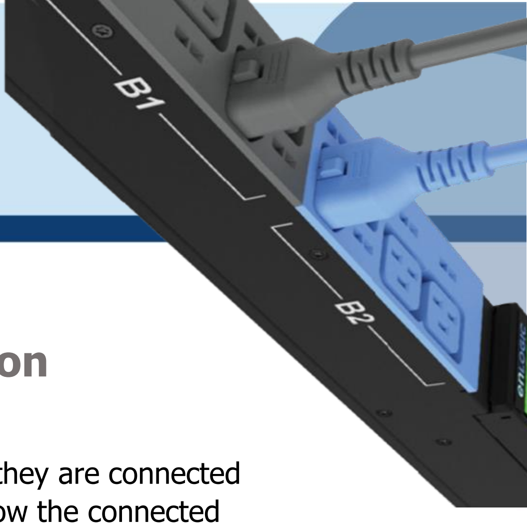
PDU Name	Sensor Name	Reading
PDU 1	door	Off
PDU 2	Balcony	No-Leak
PDU 4	T	25.0°C
PDU 4	RH	50%
PDU 5	T	24.0°C
PDU 5	RH	52%
PDU 6	DOOR SWITCH	Open
PDU 8	abcdefghijklmnop	24.0°C
PDU 8	Humidity	54%
PDU 8	Temperature3	26.0°C

NOTE

Configuring Sensors

To configure the sensor name, location, alarms, notifications, and details, open the Web UI:

1. Go to **Dashboard** to view all connected external sensors.
2. Select **Total Sensors** to view the External Sensors page.
3. Go to Settings -> Threshold -> External Sensors to configure.
4. In the **Edit** dialog box, type new data in the following fields, (for example in the 3 Temperature and 1 Humidity sensor):
    - High Critical
    - High Warning
    - Low Warning
    - Low Critical
5. Click **Save** to complete the sensor setup. Repeat this process for additional sensors.

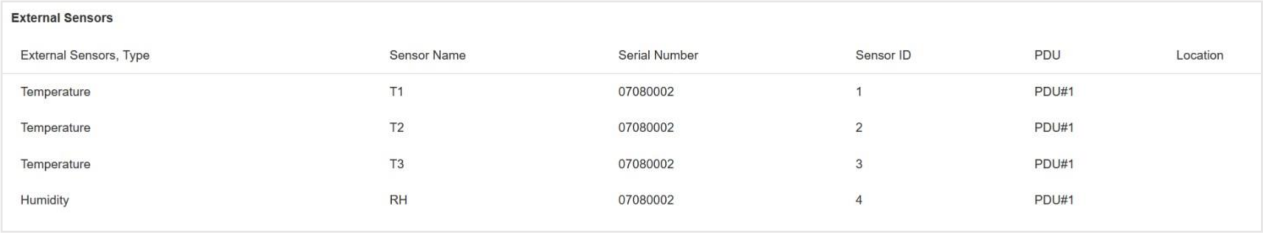


Viewing and Managing Sensor Information

Readings of the sensors are available in the Enlogic Web UI when they are connected properly. The main Dashboard page and External Sensors page show the connected sensors information.

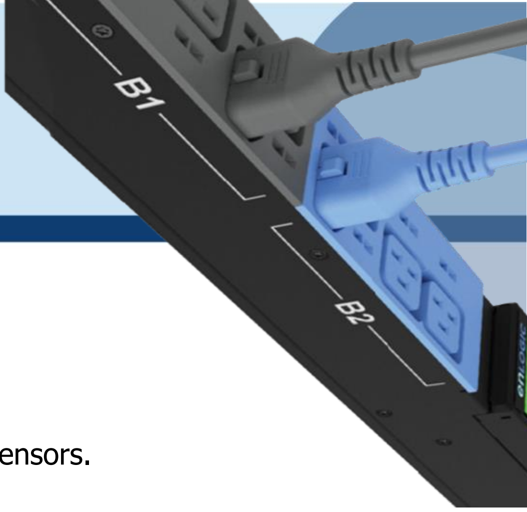
To View Connected Sensors

1. Open the **Dashboard**.
2. View the External Sensors section on the Dashboard page to see:
    - A list of sensors, which can be connected.
    - Information of each managed sensor: Sensor Name, Location, and Measurement.
3. Go to **Overview/Identification (**bottom of the page shows all connected sensors).
4. Below information is displayed for each connected sensor:
    - Type
    - Name
    - Serial number
    - ID
    - PDU Name
    - Location



External Sensors

External Sensors, Type	Sensor Name	Serial Number	Sensor ID	PDU	Location
Temperature	T1	07080002	1	PDU#1	
Temperature	T2	07080002	2	PDU#1	
Temperature	T3	07080002	3	PDU#1	
Humidity	RH	07080002	4	PDU#1	

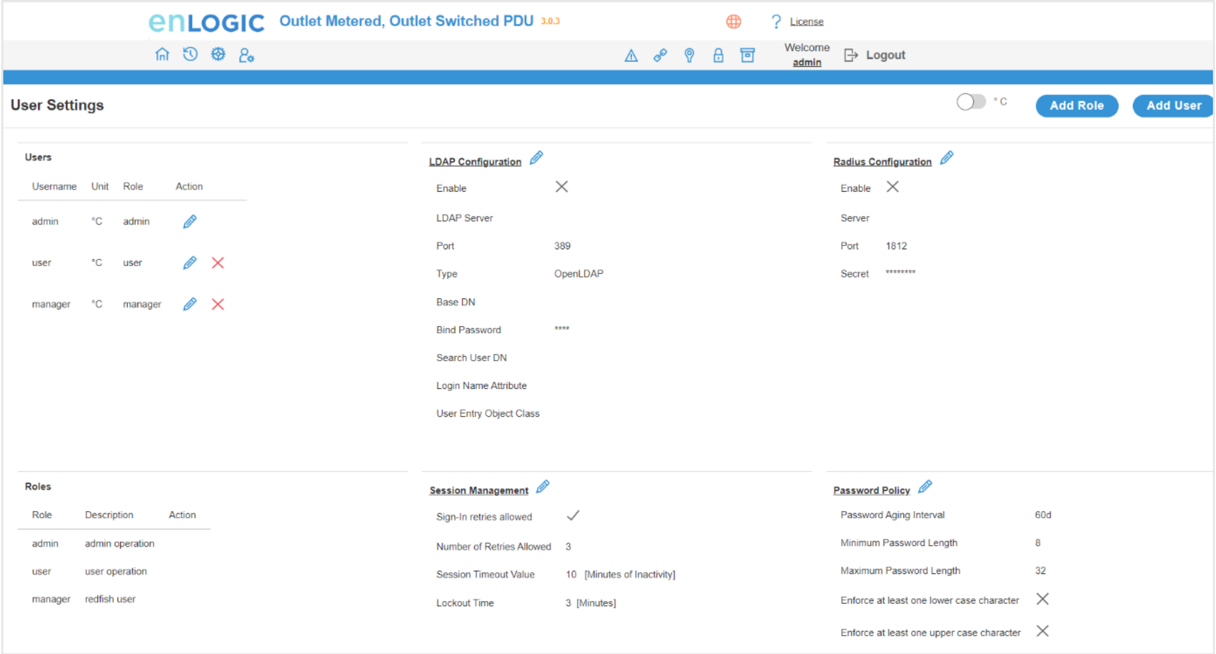


Edit External Sensor Threshold

1. Go to **Settings>>Thresholds** to view all connected external sensors.
2. In the **External Sensor** section, select the sensor to edit.
3. Click **Edit** icon in the **Action** field.
4. Type new data in the following fields, for example in the 3 Temperature & 1 Humidity sensor:
   - High Critical
   - High Warning
   - Low Warning
   - Low Critical
5. Click **Save** to proceed further.

Toggle Temperature Units between Celsius & Fahrenheit

1. Go to User **Settings** page.
2. On the top-right corner, a toggle button is displayed.
3. Click and **Toggle** between **Celsius C ° to Fahrenheit F °** based on the requirements.



User Settings

Users

Username	Unit	Role	Action
admin	°C	admin	✎
user	°C	user	✎ ✕
manager	°C	manager	✎ ✕

LDAP Configuration ✎

Enable	✕
LDAP Server	
Port	389
Type	OpenLDAP
Base DN	
Bind Password	****
Search User DN	
Login Name Attribute	
User Entry Object Class	

Radius Configuration ✎

Enable	✕
Server	
Port	1812
Secret	********

Roles

Role	Description	Action
admin	admin operation	
user	user operation	
manager	redfish user	

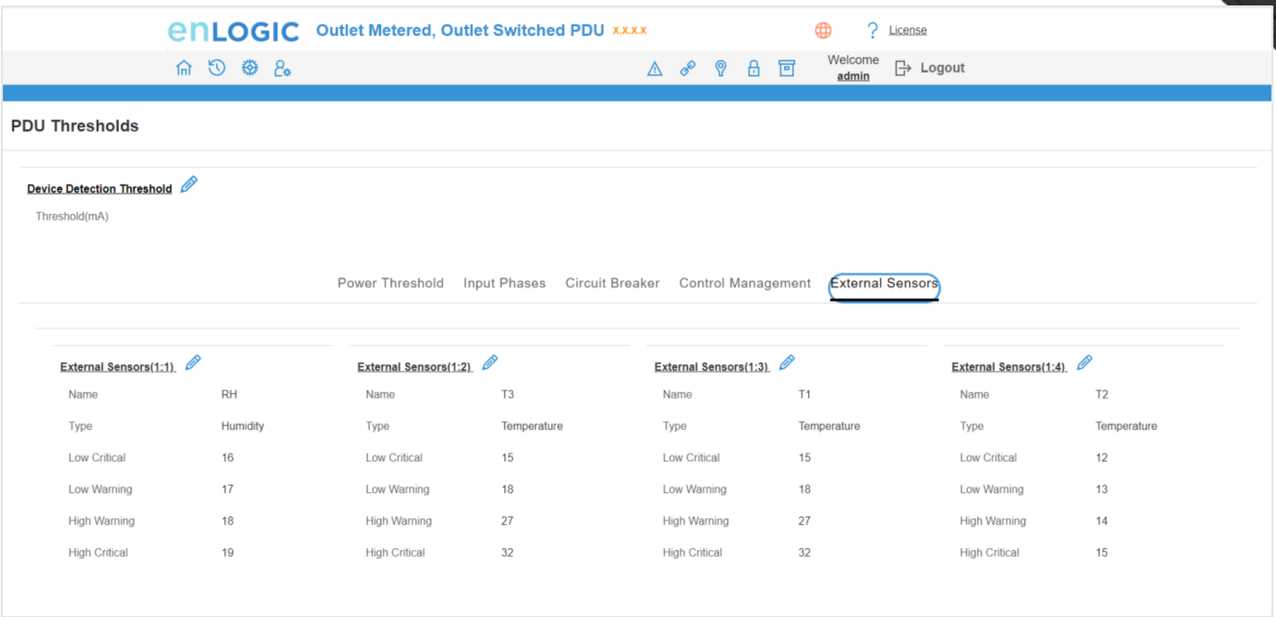
Session Management ✎

Sign-In retries allowed	✓
Number of Retries Allowed	3
Session Timeout Value	10 [Minutes of Inactivity]
Lockout Time	3 [Minutes]

Password Policy ✎

Password Aging Interval	60d
Minimum Password Length	8
Maximum Password Length	32
Enforce at least one lower case character	✕
Enforce at least one upper case character	✕

4. Click and Toggle on **Celsius C °** and view the temperature information stored in Celsius °



PDU Thresholds

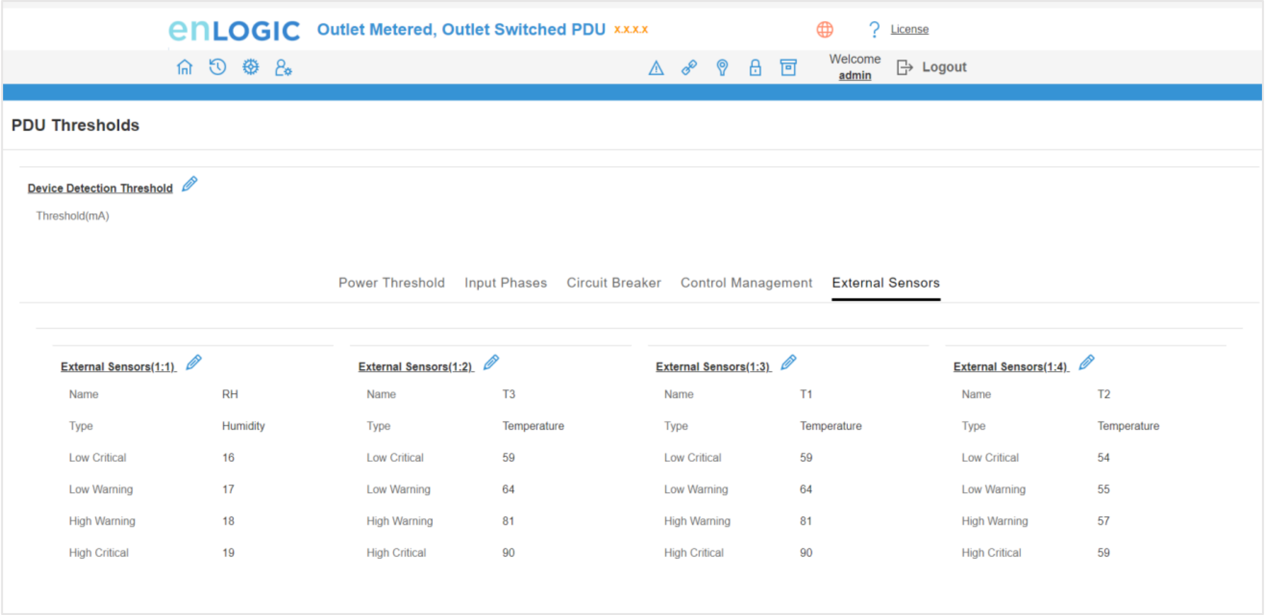
Device Detection Threshold

Threshold(mA)

Power Threshold | Input Phases | Circuit Breaker | Control Management | External Sensors

External Sensors(1:1)		External Sensors(1:2)		External Sensors(1:3)		External Sensors(1:4)	
Name	RH	Name	T3	Name	T1	Name	T2
Type	Humidity	Type	Temperature	Type	Temperature	Type	Temperature
Low Critical	16	Low Critical	15	Low Critical	15	Low Critical	12
Low Warning	17	Low Warning	18	Low Warning	18	Low Warning	13
High Warning	18	High Warning	27	High Warning	27	High Warning	14
High Critical	19	High Critical	32	High Critical	32	High Critical	15

5. Click and Toggle on **Fahrenheit F °** and view the temperature information stored in Fahrenheit °



PDU Thresholds

Device Detection Threshold

Threshold(mA)

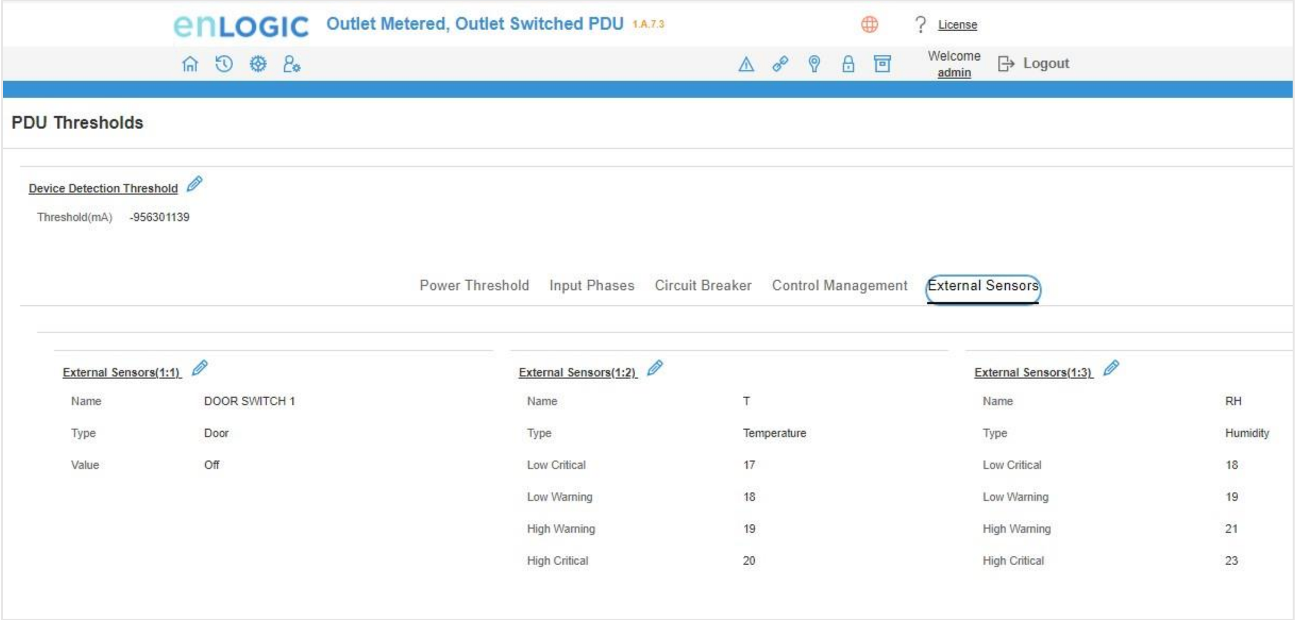
Power Threshold | Input Phases | Circuit Breaker | Control Management | External Sensors

External Sensors(1:1)		External Sensors(1:2)		External Sensors(1:3)		External Sensors(1:4)	
Name	RH	Name	T3	Name	T1	Name	T2
Type	Humidity	Type	Temperature	Type	Temperature	Type	Temperature
Low Critical	16	Low Critical	59	Low Critical	59	Low Critical	54
Low Warning	17	Low Warning	64	Low Warning	64	Low Warning	55
High Warning	18	High Warning	81	High Warning	81	High Warning	57
High Critical	19	High Critical	90	High Critical	90	High Critical	59

Monitoring the External Sensor

You can view the sensor details including name, location, value, etc.

1. From the Dashboard in the Web Interface, go to the **External Sensors** section or **Settings/PDU thresholds** to view all connected external sensors to view details.



PDU Thresholds

Device Detection Threshold

Threshold(mA) -956301139

External Sensors(1:1)

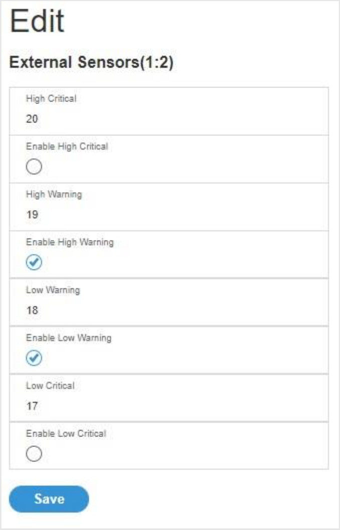
Name	DOOR SWITCH 1
Type	Door
Value	Off

External Sensors(1:2)

Name	T
Type	Temperature
Low Critical	17
Low Warning	18
High Warning	19
High Critical	20

External Sensors(1:3)

Name	RH
Type	Humidity
Low Critical	18
Low Warning	19
High Warning	21
High Critical	23


Edit

External Sensors(1:2)

High Critical
20

Enable High Critical
○

High Warning
19

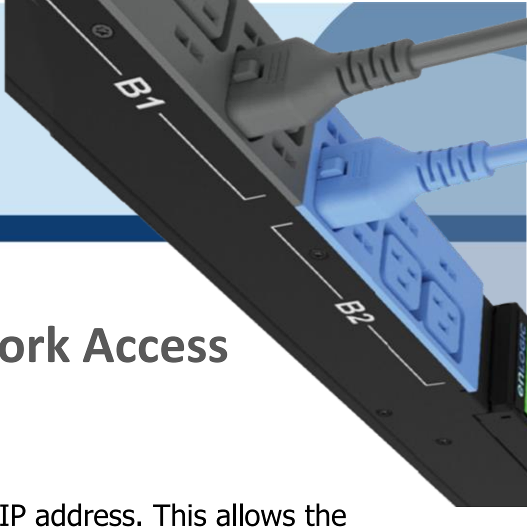
Enable High Warning
✓

Low Warning
18

Enable Low Warning
✓

Low Critical
17

Enable Low Critical
○



Daisy Chain and RNA–Redundant Network Access

Daisy-Chain Functionality

In daisy chain mode, up to **64** PDUs can be connected via one (1) IP address. This allows the user to gather information and data of all daisy chained PDUs from the master PDU.

The daisy chain functionality reduces the network services cost for PDUs. For example, a standard network switch is used in a data center can contain 24 ports. Without using the daisy chain function, each port supplies network services to one (1) PDU. However, if using the daisy chain features of Enlogic, a typical network switch with 24 ports can supply network services for up to **1536** PDUs.

Daisy-Chain Setup

Follow below steps to setup the connection up to **64** PDUs of the same SKU via single IP address:

1. Configure the PDU, which is first in line on the Daisy Chain.

Note: *Refer to the Network* Settings *section for more information.*

2. After the initial PDU is configured, connect the Ethernet cord from the 10/100 port (on the configured PDU) to the 10/100/1000 port (on the second PDU) in the daisy chain line.

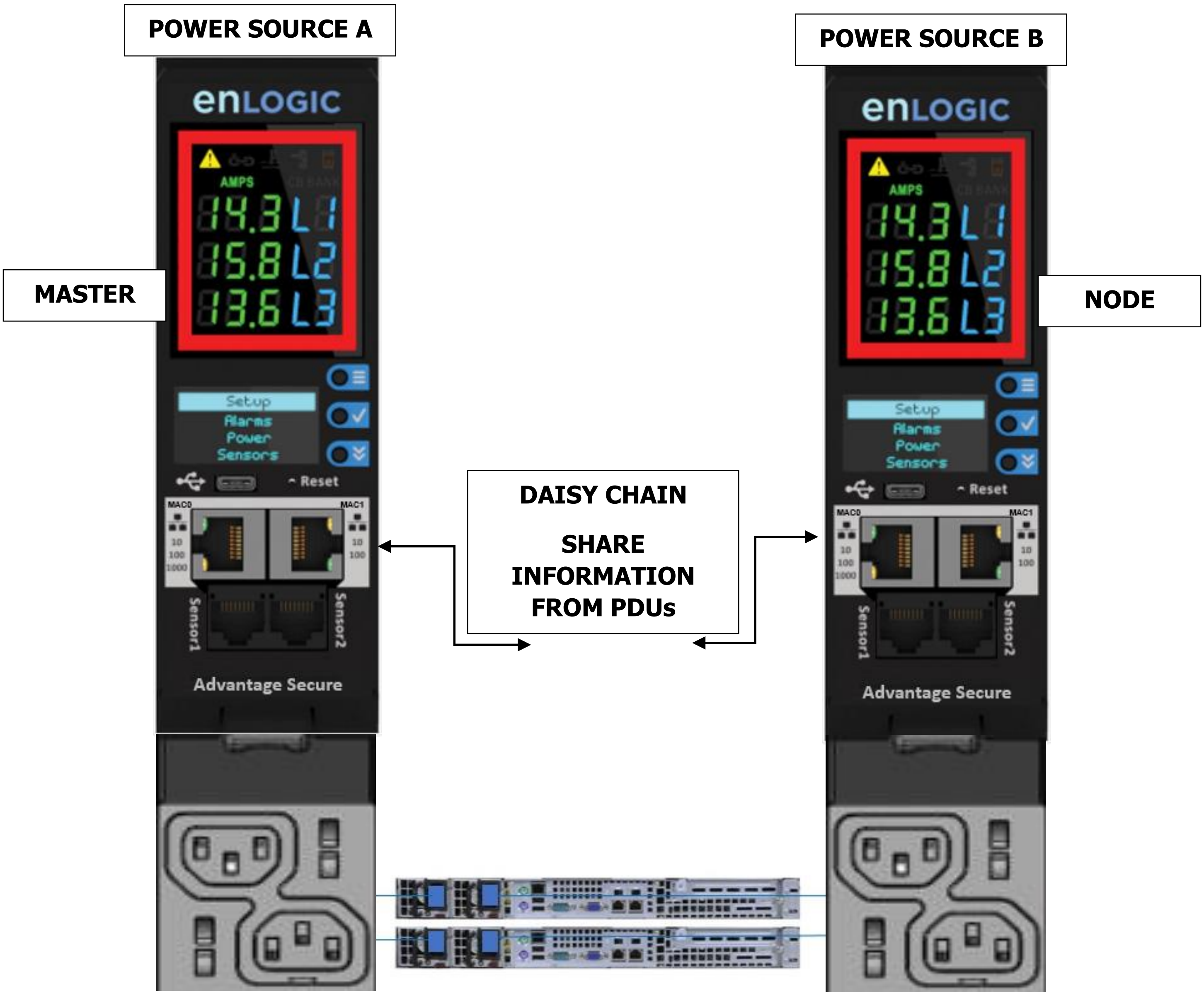
3. Repeat **step 2**, connecting PDUs from the 10/100 port to the 10/100/1000 port for up to **64** PDUs.

Note: *The length of the Ethernet cords connecting the PDUs must be less than 6 m (20 ft.).*

4. By default, the Daisy Chain command is enabled in the PDU configuration file and default mode of the PDU is QNA. Go to the **web interface** (or management software) to manage and control the PDUs in the Daisy Chain.

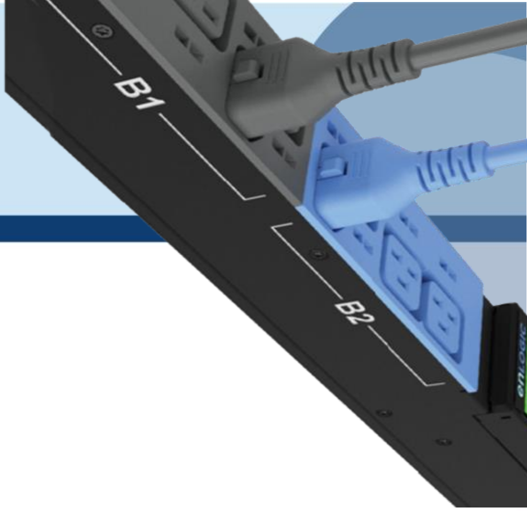
RNA (Redundant Network Access) Functionality

Enlogic RNA allows secure access of PDU data and statistics on two separate private networks. RNA is used with a redundant power delivery design including two rack PDUs for each IT rack. PDUs are used in RNA applications that must be of the same SKU.



How it Works

- Using Enlogic RNA, the landlord and tenant maintain two separate private networks that do not overlap.
- Enlogic RNA works using a redundant power delivery design (i.e., two rack PDUs for each IT rack).
- Each PDU is separately connected to the Tenant or Landlord’s private communications network.
- The two PDUs are connected with the data communications bus to allow PDUs to share user-defined information.
- Each PDU acts like a master PDU to report PDU data to both networks.



RNA Setup

To setup RNA mode on Daisy chain setup the user must,

1. Configure the PDU for RNA Mode (using CLI).
2. Connect the LAN Network cords and Ethernet cords between PDUs.

To Connect PDUs for RNA Setup

After the PDUs are configured for RNA

1. Connect the LAN network cable from network switch to the PDU1 Port1.
2. Connect another LAN NETWORK cable to Port 2 of last PDU in the daisy chain setup.
3. Connect the Ethernet cable from the Landlord PDU port 2 to Tenant PDU port 1 (to establish daisy chain connection).
4. Next step is to configure RNA mode to establish RNA connection.

To Configure RNA Mode in the CLI

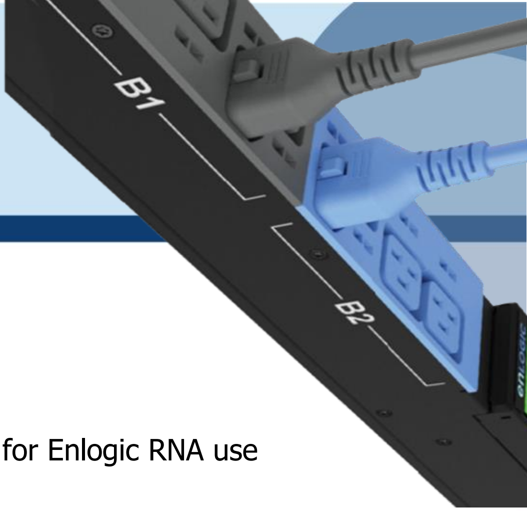
1. Login to the CLI and type the command 'dev daisy rna' on the last PDU of daisy chain setup.
2. The following message will appear:

   SUCCESS

   System Reboot now, Are you sure? (Y/ N)

3. Type Y to confirm reboot.
4. After reboot, the PDU will be setup to RNA Mode.

***Note**: RNA mode enabled PDU's should not be placed in between the daisy chain system*.



Daisy Chain and RNA Commands in CLI

The following is a list of executable commands available in the CLI for Enlogic RNA use only.

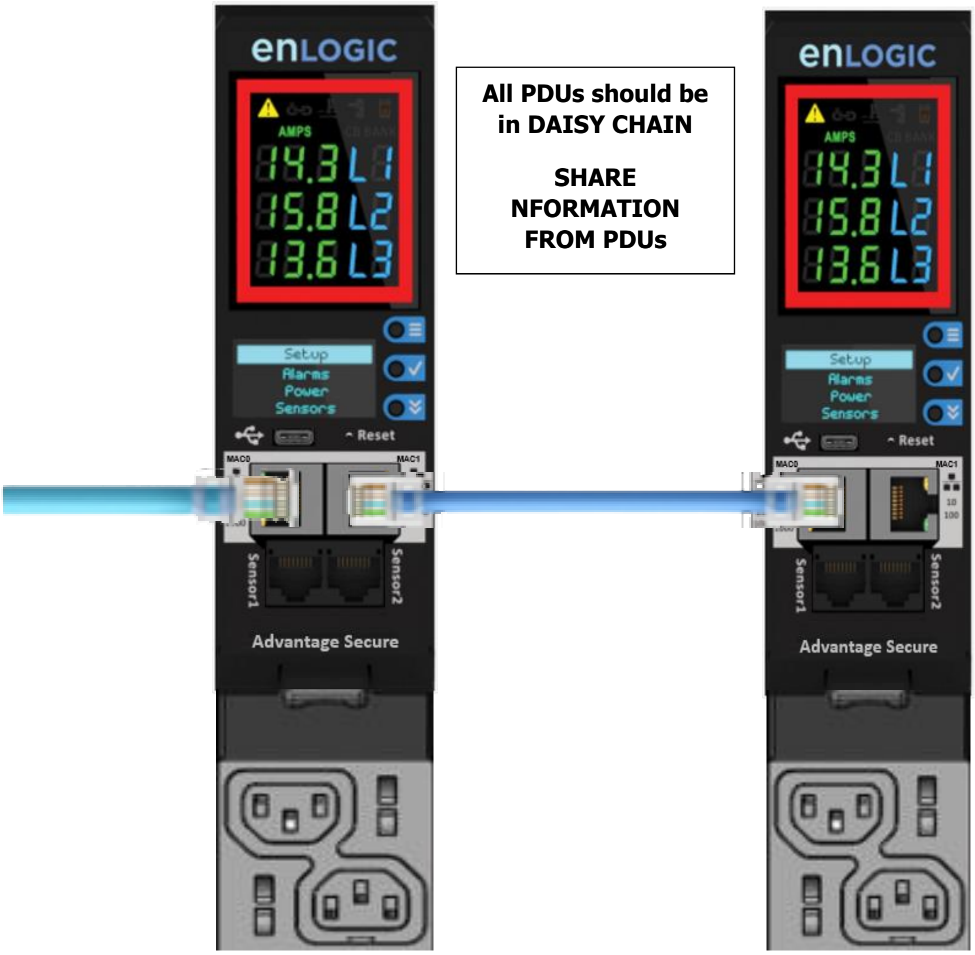
Command	Description	Example
dev daisy rna	Changes mode from daisy chain to RNA	EN2.0> dev daisy rna System Reboot now, Are you sure?(Y/ N):
dev daisy qna	Changes mode from RNA to daisy chain	EN2.0> dev daisy qna System Reboot now, Are you sure?(Y/ N):

Power Share over Daisy Chain PDUs

Enlogic PDUs now come with a built-in failover power capability called **"Power Share".** This function makes sure that the consequences of any unforeseen outages or data center outages are minimized. By giving the NMC redundant power, the Power Share feature reduces the possibility of a power outage on one of the power feeds before it occurs and keeps an eye on the downstream daisy chained PDUs.

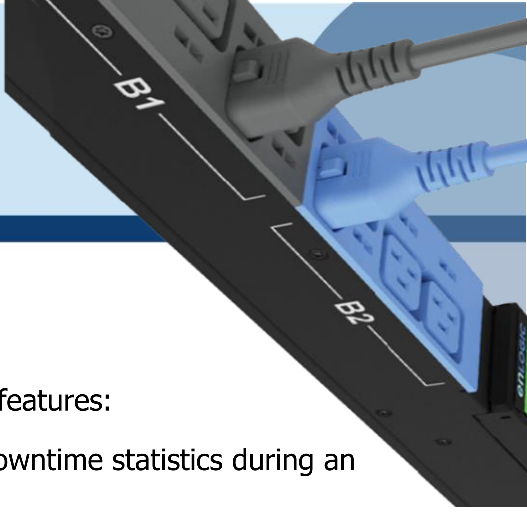
In this case, the PDUs share power via the same Ethernet connection that is used in a daisy chain, allowing the PDU to continue receiving DC power from the linked PDU even in the event that it loses AC power.

In addition to the increased resilience and stability, this functionality allows the **"lost power"** PDU to continue maintaining network communications, sensor functions, and security operations.



All PDUs should be in DAISY CHAIN

SHARE NFORMATION FROM PDUs



Upcoming features

Enlogic firmware will support the following upcoming Power Share features:

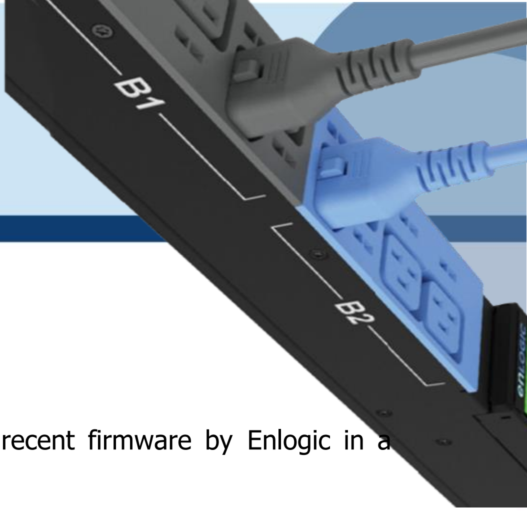
1. Enlogic Power Share feature helps customers understand downtime statistics during an outage and enhancing overall responsiveness.
2. Power Share also lowers the Mean Time to Repair (MTTR) by sending out timely notifications/alarms.
3. Users can set alerts and alarms, giving them crucial seconds to make decisions that will lessen accidental power interruptions.
4. SNMP, WEB UI, CLI and SSH are the four interfaces that can be used to monitor and control Power Share features. When the PDU is in Power Share mode this information is displayed in any/all of the above interfaces.
5. In the WEB UI, the Event logs also display that the PDU has lost its Main power and is in Power Share mode.
6. The downed controller receives redundant power via Power Share. As a consequence, visibility and network connectivity are maintained. The user can reach their destination more quickly and effectively since they are immediately notified of the fallen controller.
7. Power Share maintains connectivity to all downstream and upstream devices and keeps an eye on all sensor and power meter reading data. The fallen PDU's power reading would be the only thing unavailable.

Limitations

Enlogic PDUs now come with a built-in failover power capability called **"Power Share".** There are a few restrictions:

1. Only PDUs that are daisy chained—that is, linked to AC power—are eligible for the Power Share function. To power share PDUs, a Cat6 patch cable is used.
2. The PDU cannot share power with the PDUs next to it if it is currently consuming DC power.
3. In the case of an AC power source failure, each PDU has the capacity to supply DC power to power the sensors and network management electronics in the PDU [previous and next in sequence]. EG: In a 64 PDU daisy chain setup if the 50th PDU loses AC power, the 49th or 51st PDU will power share.
4. The Power Share feature never extends power beyond the adjacent PDUs.
5. Power Share allows power to be shared just with additional two NMC; power to the outlets is not shared and the outlet LED lights are turned off. This keeps both NMCs operating at maximum capacity. The alerts notify the user when a PDU loses power, this allows for a quick remediation by identifying where and when an outage occurs.
6. The Power Share feature of NMC helps mitigate the risks of a power loss on either power feed before they happen, maintains your visibility into daisy chained PDUs.

   Please refer the **Questions and Answers (FAQs)** page below for some terminologies used in this section.



Firmware Update Procedures

Enlogic iPDUs and Inline Meters can be updated to support the most recent firmware by Enlogic in a variety of ways.

USB Method

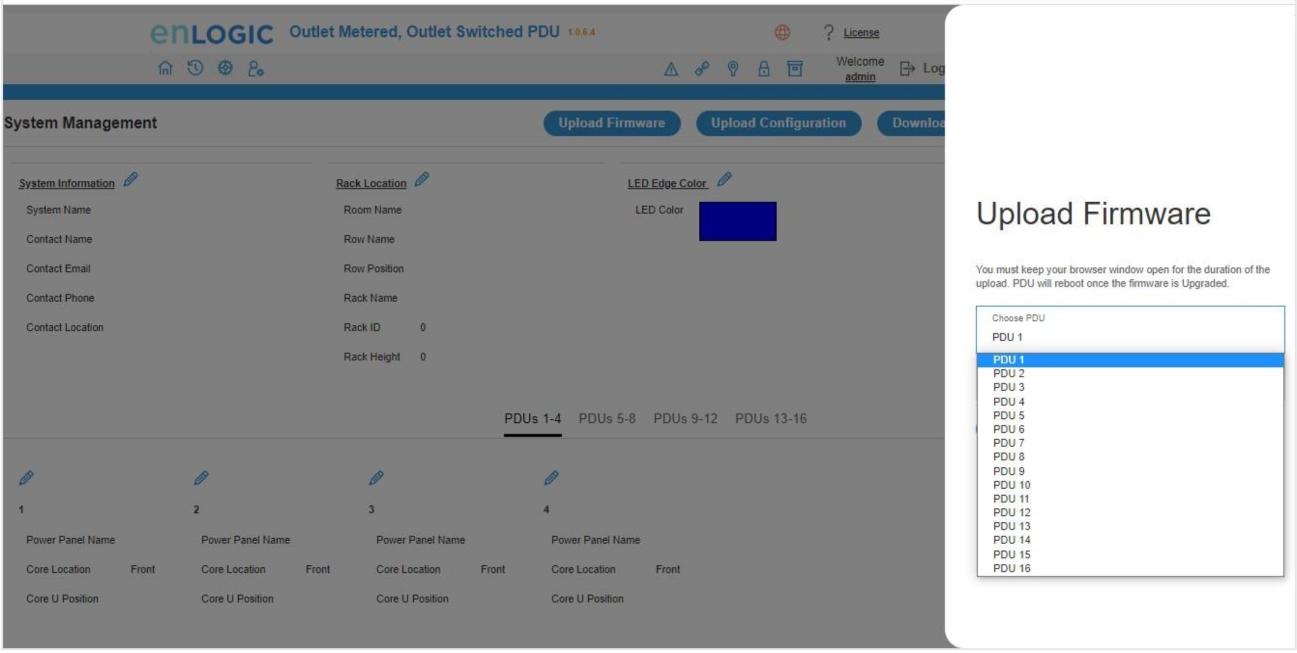
1. Go to www.enlogic.com and download the most recent Firmware version, ‘enlogic.fw’.
2. Select Firmware Upload and click Yes to confirm.

***Note**: The OLED will show the Firmware update progress. It also shows the process of updating. When the update is complete, the PDU will automatically reboot*.

3. Go to **Setup** and select **Device** and **Firmware** to confirm that the Firmware uploaded successfully.

Web Interface Method

1. Go to www.enlogic.com and download the most recent Firmware version, enlogic.fw . Save this file into a folder location.
2. Go to System management page and select the Upload Firmware option.
3. Select the PDU you want to upload firmware and upload the enlogic.fw file.



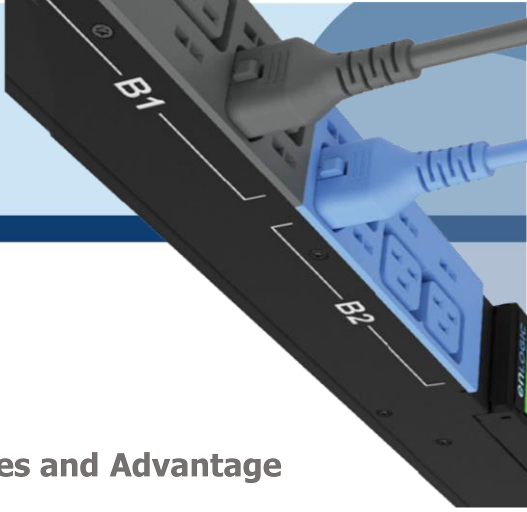
You must keep your browser window open for the duration of the upload. PDU will reboot once the firmware is Upgraded.

***Note**: PDU will reboot, and Firmware upgrade will complete.*

4. To access the PDU using an FTPS program, FTPS must be enabled through the PDU Web Interface or through CLI or through SSH.

5. In the Web Interface, go to Network Settings -> FTPS.
6. Select the check box to **enable FTPS Access**.
7. Login to an FTP program with a role with administration privileges.
8. Transfer the firmware file enlogic.fw to /fw folder.
9. Connect to the PDU via SSH using a program such as TeraTerm or PUTTY.
10. Login using a role with administration privileges.
11. Execute the CLI command "sys upd all" to perform the FW upload operation.

After reboot message indication in console, push the “Y” from the prompt (Y/N) displays for the PDU reboot ***Note:*** *For Master PDU / Standalone configuration, at the (Y/N) prompt will be appeared for PDU reboot, type Y. When the upload is finished, the system will reboot automatically.*



Questions and Answers (FAQs)

Q1. What are the differences between Advantage Series and Advantage Secure PDUs (or NMCs)?”

Answer: Advantage Secure is a newer offer that adds a cybersecurity feature called Secure Boot. This adds hardware support to provide a “root of trust” that increases protection against attempts to load non-authenticated firmware to the PDU. It also adds additional flash memory for future use.

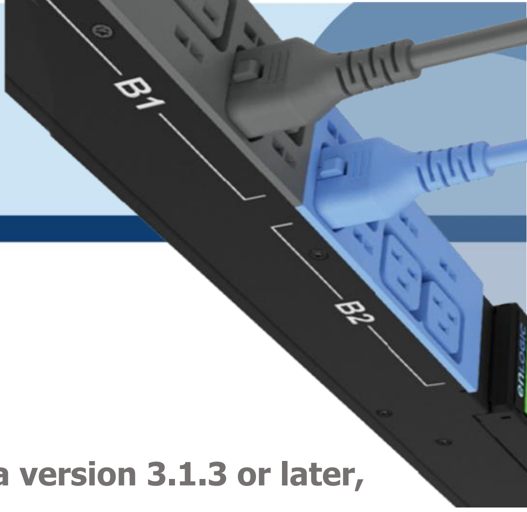
Q2. Are there any changes to the firmware file's format from earlier iterations for the Enlogic Firmware?

Answer: Unlike previous compressed or zipped files [.tar/.zip], the firmware file for all new versions will be provided in the **enlogic.fw** format.

Q3. How can we upgrade current or new NMCs to the latest firmware version 3.1.9?

Answer: Follow the steps mentioned before for the current in use or new NMCs:

- The firmware upgrades should be performed in the following order for **Advantage Series NMCs**:
  - Firmware version 2.0.6.7 .
  - Upgrade Bridge firmware 3.0.0.2 using the update folder in the USB, or enlogic.tar using the WEBUI & FTPS.
  - From, 3.0.0.2 [bridge firmware] to flash new firmware [3.1.3] use **enlogic.fw** using USB, WEBUI & FTPS.
- The firmware upgrades should be performed in the following order for **Advantage Secure NMCs:**
  - Firmware version 3.0.4 .
  - From, 3.0.4 to flash new firmware [3.1.3] use **enlogic.fw** using USB, WEBUI & FTPS.



Q4. When updating from a lower firmware version to a version 3.1.3 or later, are there any specific actions recommended?

Answer: It is recommended for users to execute the command “**dbg energyclr**”, to erase all previously saved energy accumulation values from the PDU. Customer service can assist by providing a script that can accommodate a list of PDU addresses.

Q5. When updating from a lower firmware version to a version 3.1.3 or later, can the firmware then be downgraded to a previous version?

Answer: Due to underlying file system improvements made in version 3.1.3, downgrades to a previous firmware version are not supported.

Q6. Can older iPDUs support the new Advantage Secure NMCs and Hot Swapping?

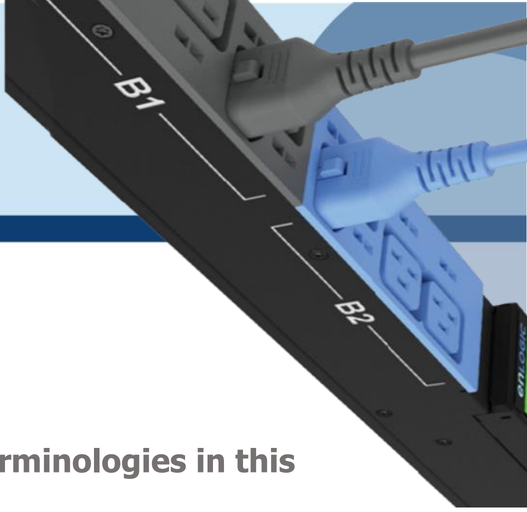
Answer: Older iPDU’s NMCs cannot be hot swapped with the new Advantage Secure NMCs.

Q7. After updating firmware to a new version, can I use a configuration file created from the previous firmware version?

Answer: After flashing the new Firmware, previously stored configuration files cannot be used.

Q8. Will the MIB files in the new Firmware support IPv6 addresses?

Answer: The new Firmware will support a new MIB file that contains IPv6 addresses.



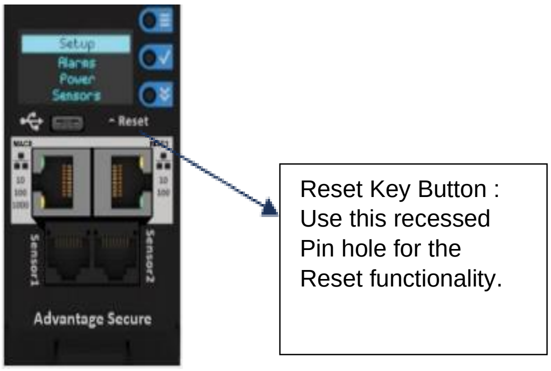
Q9. Could we understand some of the Power Share Terminologies in this document?

Acronym	Abbreviation
Power Share function	Parameter used to enable and/or disable Power Share mode
AC	Alternating Current/Standard electricity provided to devices
DC	Direct Current/One-directional flow of electric charge
Main Power	AC Power incoming from main supply to a PDU
Backup Power	Power supplied by an adjacent controller during Mains power loss
Upstream	Power sharing capability of a PDU to its preceding PDU
Downstream	Power sharing capability of a master PDU to the next/succeeding PDU
Cat6 patch cable	Cat6 Ethernet cable is a network cable used for connecting devices or PDUs
MTTR (mean time to repair)	MTTR (mean time to repair) is the average time it takes to repair a system (usually technical or mechanical). It includes both the repair time and any testing time.

Q10. What should a user do if they see an iPDU transitioning into an unknown state?

Answer: If this happens, the user can perform a soft RESET on the iPDU.

NMC Reboot [RST]	Use a pin, press, and hold the recessed RESET key button for about 8 seconds, which will initiate the reset option without changing any configuration values. The OLED display will show the RST during this operation.



Reset Key Button : Use this recessed Pin hole for the Reset functionality.