



CONNECT AND PROTECT

Enlogic – Advantage & Secure

Power Distribution Units

User Manual Version 1.5 | 20th December 2024



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
V1.3	20.05.2024	OMB Syslog Secondary Radius Server LDAPS Configuration Secure Copy Protocol [SCP] TELNET HTTP/HTTPS redirection Web UI Improvements – Power Share, Power Parameters, Outlet & CB Management Redfish New URLs Curl Commands - Sys, User, Dev, Net, Pwr commands updated
V1.4	20.05.2024	TLS1.3 Password Hashing Outlet Grouping Radius Server Configuration 1U/2U Horizontal iPDUs & NMCs Redfish New URLs RESTAPI Curl Commands Outlet Grouping - Curl Commands - Dev commands Sensors Air flow Sensor LED Beacon Handle Update Procedures
V1.5	20.12.2024	Single User Multi Session (SUMS) Residual Current Monitoring (RCM) Overload Prevention (OLP) 8021.X Authentication Redfish Newly implemented URLs Curl Commands - Sys, User, Dev, Net, Pwr commands updated Zero Touch Provisioning (ZTP) Open SSH 9.9 Access Control List Web UI Improvements

TABLE OF CONTENTS

GENERAL SAFETY INSTRUCTIONS.....	8
INSTALLATION AND OPERATION SAFETY INSTRUCTIONS.....	8
SAFETY INSTRUCTIONS – DISCLAIMER.....	8
SAFETY SYMBOLS	9
SAFETY INFORMATION FOR OPERATORS.....	9
PRODUCT LABELS AND STANDARDS	10
REFERENCES AND ARCHITECTURE SPECIFICATIONS.....	10
GENERAL INSTALLATION.....	11
UL 2900 CERTIFIED BY UL CAP.....	12
PRODUCT & DOCUMENTS	12
REGIONS SUPPORTED	13
INPUT & OUTPUT CURRENT RATINGS.....	14
PRODUCT DESCRIPTION.....	17
IPDU & ITS COMPONENTS	18
PRODUCT COMPONENTS NMC.....	19
DISPLAYS.....	20
INTERFACES	20
RESET BUTTON.....	21
ADVANCED NETWORK MANAGEMENT CONTROLLER (NMC) NETWORK SECURITY.....	22
ENCRYPTION	22
REMOTE AUTHENTICATION.....	22
LOGIN & PASSWORD POLICY.....	23
CERTIFICATES.....	23
FIRMWARE AND CONF FILE ENCRYPTION	24
CHAIN OF TRUST FIRMWARE SIGNATURE.....	24
SECURE BOOT.....	24
CONF FILE.....	24
OTHER VULNERABILITIES.....	25
NETWORK SECURITY HARDENING GUIDE	25
DISABLE SNMPV1 AND ENABLE SNMPV3	26
CONFIGURE SNMPV3 TO USE AES/SHA.....	26
CHANGE THE ADMIN USER ACCOUNT PASSWORD	26
ENABLE STRONG PASSWORDS.....	26
HASHING PASSWORDS FOR INCREASED CYBERSECURITY	26
DEFAULT PORTS	27
SEVEN SEGMENT LED DISPLAY	28
OLED DISPLAY AND NETWORK MANAGEMENT CONTROLLER (NMC).....	29
MAIN MENU SELECTIONS.....	30
SETUP MENU.....	30
NETWORK SUBMENU.....	31
DEVICE SUBMENU.....	31
SCREEN SUBMENU.....	32
LANGUAGE SUBMENU	32
USB SUBMENU	33
UNITS SUBMENU	33
ALARMS MENU	34
POWER MENU	34
DEVICE SUBMENU.....	34
PHASE SUBMENU.....	34

BREAKER SUBMENU	36
OUTLET SUBMENU.....	36
SENSORS MENU	37
RCM MENU.....	38
HORIZONTAL iPDU.....	39
MAIN MENU SELECTIONS.....	43
NMC HOT SWAP	57
INSTALLING THE NEW NMC.....	59
OUTLET UNITS	60
SELF-LOCKING COMBO OUTLET	61
NEWLY LAUNCHED OUTLETS & VARIANTS.....	62
SELF-LOCKING CABLE & NON-LOCKING CABLE	63
LOCKING POWER CORDS.....	63
MOUNTING PDU IN SERVER CABINET	65
CONNECTING TO POWER SOURCE.....	65
CONNECTING PDU TO NETWORK.....	66
CONNECTING WITH SERIAL CONNECTION.....	67
CONNECTING SENSORS (OPTIONAL)	69
WEB USER INTERFACE (UI).....	72
INTRODUCTION TO WEB UI.....	72
NAVIGATING THROUGH THE WEB UI.....	74
SINGLE USER MULTIPLE SESSIONS (SUMS).....	75
DASHBOARD	77
CONTROL AND MANAGE.....	81
OUTLET GROUPING.....	83
VIEW LOGS	88
VIEW DATA LOGS.....	89
SETTINGS.....	90
NETWORK SETTINGS.....	90
802.1x Authentication.....	91
WEB/RESTAPI ACCESS CONFIGURATION	95
SSH/FTPS CONFIGURATION.....	96
NETWORK TIME PROTOCOL (NTP)	96
DATE/TIME SETTING	97
DAYLIGHT-SAVING TIME.....	97
SYSLOG CONFIGURATION.....	98
SYSTEM MANAGEMENT.....	100
SNMP MANAGEMENT.....	102
EMAIL SETUP.....	104
EVENT NOTIFICATIONS	106
TRAP RECEIVER.....	107
DEFINING THRESHOLDS.....	109
POWER THRESHOLD	109
INPUT PHASES.....	110
CIRCUIT BREAKER.....	112
CONTROL MANAGEMENT	114
EXTERNAL SENSORS	115
PHASE POWER.....	116
OVERLOAD PREVENTION (OLP)	117
RACK ACCESS CONTROL	121
SMART RACK CONTROL.....	122
RESIDUAL CURRENT MONITORING (RCM).....	126

USER SETTINGS.....	135
LDAP/LDAPS SERVER SETTINGS	140
RADIUS CONFIGURATION.....	142
SESSION MANAGEMENT	145
PASSWORD POLICY.....	146
SNMP	147
WORKING WITH MIB BROWSER	147
REDFISH.....	149
REDFISH CONFIGURATION.....	149
REDFISH AUTHENTICATION AND AUTHORIZATION	150
REDFISH URLS SUPPORTED WITH GET METHOD.....	152
REDFISH URLS SUPPORTED WITH POST METHOD	154
REDFISH URLS SUPPORTED WITH DELETE METHOD	154
NEW REDFISH URLS SUPPORTED WITH POST METHOD.....	155
GETTING STARTED WITH REDFISH.....	156
RESTAPI – CURL COMMANDS.....	126
THE COMMAND LINE INTERFACE (CLI).....	179
CLI COMMANDS AND PROMPTS	179
CLI COMMANDS	180
SYS Commands.....	183
NET COMMANDS.....	186
USR COMMANDS.....	191
DEV COMMANDS.....	195
PWR COMMANDS.....	201
FTPS.....	202
SENSORS.....	203
DETECTING SENSORS.....	209
MONITORING THE EXTERNAL SENSOR.....	213
DAISY CHAIN AND RNA-REDUNDANT NETWORK ACCESS.....	214
RNA (REDUNDANT NETWORK ACCESS) FUNCTIONALITY.....	214
ZERO TOUCH PROVISIONING (ZTP).....	216
POWER SHARE OVER DAISY CHAIN PDUs.....	219
FIRMWARE UPDATE PROCEDURES.....	221
HANDLE UPDATE PROCEDURES	222
QUESTIONS AND ANSWERS (FAQS)	225



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 nVent Enlogic firmware is installed on all nVent 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.
- AC plug on the power supply cord of this product is used as disconnecting device, and it shall be easily accessible when it is installed.
- 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 nVent Enlogic accessories or products recommended by nVent Enlogic along with the nVent Enlogic iPDU.
- Changes and modifications to this equipment can affect the warranty. nVent 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.
- 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 nVent Enlogic accessories or products recommended by nVent Enlogic along with the nVent Enlogic iPDU.
- Changes and modifications to this equipment can affect the warranty. nVent Enlogic is not responsible for damage to this product, resulting from accident, disaster, or misuse.



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 nVent Enlogic iPDU. The warning notices are classified according to severity of the damage occurring and its statistic occurrence.

Symbol	Brief description of the danger
⚠ DANGER	
	The signal word DANGER indicates an immediate danger. Non-observance will result in severe injuries or death.
⚠ WARNING	
	The signal word WARNING indicates danger. Non-observance can lead to severe injury or death.
⚠ CAUTION	
	The signal word CAUTION indicates a danger. Non-observance can lead to injuries.
ATTENTION	
	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 nVent Enlogic iPDU. The nationally applicable health and safety regulations must be adhered as well.

⚠ WARNING	
	<p>Risk of injury due to insufficient personal protective equipment</p> <p>If you use wrong / no protective equipment at all, serious injuries are possible.</p> <ul style="list-style-type: none"> • 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.
	<p>Please refer to specific Drawing Assembly or the Circuit diagram for the total current of the combination of different outlets per model.</p>

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 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.

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

A screenshot of a web browser showing the 'REGISTER THE PRODUCT' page. The page has a dark header with navigation links: 'PRODUCTS', 'RESOURCES & SUPPORT', and 'FIND THE PARTNER'. Below the header, the text 'REGISTER THE PRODUCT' is centered, with a breadcrumb trail 'Home > Product Registration'. The main content area contains a form titled 'PRODUCT REGISTRATION' with the following fields: 'First Name', 'Last Name', 'Email', and 'UID and Serial Numbers'. A 'SUBMIT' button is located at the bottom right of the form. A small instruction above the form reads: 'To register your Enlogic product under the standard 3-year warranty, submit the following information below.'

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- 30P	30A THREE PHASE

INPUT & OUTPUT CURRENT RATINGS

The PDU should be connected to Input current $\leq 27.7A$ for Delta series and “Wye in + Delta out” series, attached is all models, only the models indicated below cannot be configured to reach the maximum output current of 10A or 16A.

1. For EP#0*16-XXXX-C, EP#0*16-XXXX-L, EP#1*16-XXXX-C, EP#1*16-XXXX-L, EP#2*16-XXXX-C, EP#2*16-XXXX-L, EP#5*16-XXXX-C, EP#5*16-XXXX-L, EP#6*16-XXXX-C, EP#6*16-XXXX-L

INPUT:

200-240VAC, DELTA, 3-PHASE, 50/60Hz, 16A

OUTPUT:

C13/C15 Combo/Locking; 100-240VAC, 9.2A max per outlet

C13/C15/C19 Combo/Locking; 100-240VAC, 9.2A max per outlet

INPUT:

120/208VAC, WYE, 3W+PE 3-PHASE, 50/60Hz, 16A

OUTPUT:

C13/C15 Combo/Locking; 208VAC, 9.2A max per outlet

C13/C15/C19 Combo/Locking; 208VAC, 9.2A max per outlet

2. For EP#0*24-XXXX-C, EP#0*24-XXXX-L, EP#1*24-XXXX-C, EP#1*24-XXXX-L, EP#2*24-XXXX-C, EP#2*24-XXXX-L, EP#5*24-XXXX-C, EP#5*24-XXXX-L, EP#6*24-XXXX-C, EP#6*24-XXXX-L

INPUT:

200-240VAC, DELTA, 3-PHASE, 50/60Hz, 24A

OUTPUT:

C13/C15/C19 Combo/Locking; 100-240VAC, 10A max per outlet

C13/C15/C19 Combo/Locking; 100-240VAC, 13.8A max per outlet

INPUT:

120/208VAC, WYE, 3W+PE, 3-PHASE, 50/60Hz, 24A

OUTPUT:

C13/C15 Combo/Locking; 208VAC, 10A max per outlet

C13/C15/C19 Combo/Locking; 208VAC, 13.8A max per outlet

3. For EP#0&*16-XXXX, EP#1&*16-XXXX, EP#2&*16-XXXX, EP#5&*16-XXXX, EP#6&*16-XXXX

INPUT:

200-240VAC, DELTA, 3-PHASE, 50/60Hz, 16A

OUTPUT:

C13; 100-240VAC, 50/60Hz, 9.2A max per outlet

C19; 100-240VAC, 50/60Hz, 9.2A max per outlet

INPUT:

120/208VAC, WYE, 3W+PE 3-PHASE, 50/60Hz, 16A

OUTPUT:

C13; 208VAC, 50/60Hz, 9.2A max per outlet

C19; 208VAC, 50/60Hz, 9.2A max per outlet

4. For EP#0&*24-XXXX, EP#1&*24-XXXX, EP#2&*24-XXXX, EP#5&*24-XXXX, EP#6&*24-XXXX

INPUT:

200-240VAC, DELTA, 3-PHASE, 50/60Hz, 24A

OUTPUT:

C13; 100-240VAC, 50/60Hz, 10A max per outlet

C19; 100-240VAC, 50/60Hz, 13.8A max per outlet

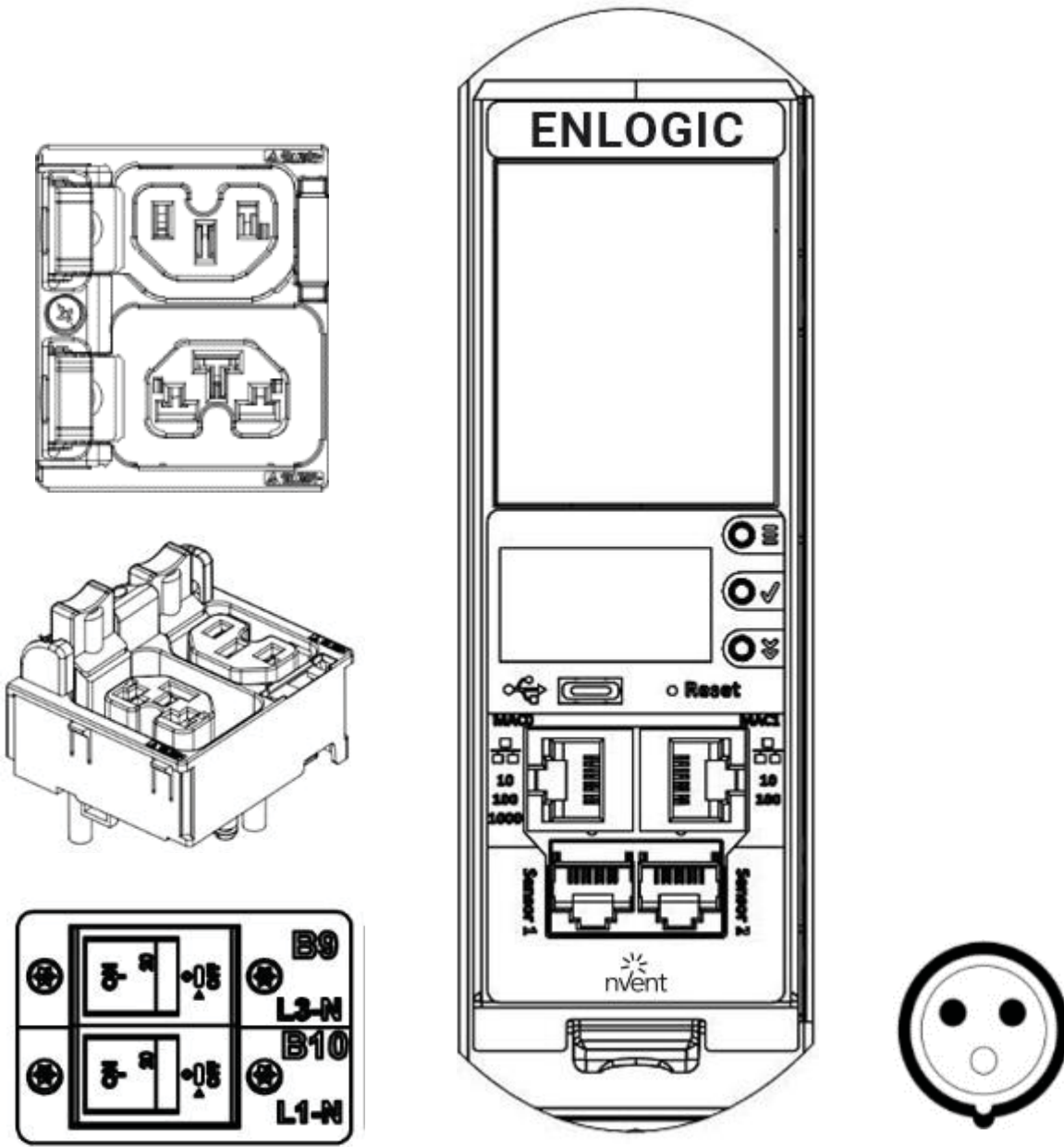
INPUT:

120/208VAC, WYE, 3W+PE 3-PHASE, 50/60Hz, 24A

OUTPUT:

C13; 208VAC, 50/60Hz, 10A max per outlet

C19; 208VAC, 50/60Hz, 13.8A max per outlet



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	✓		✓

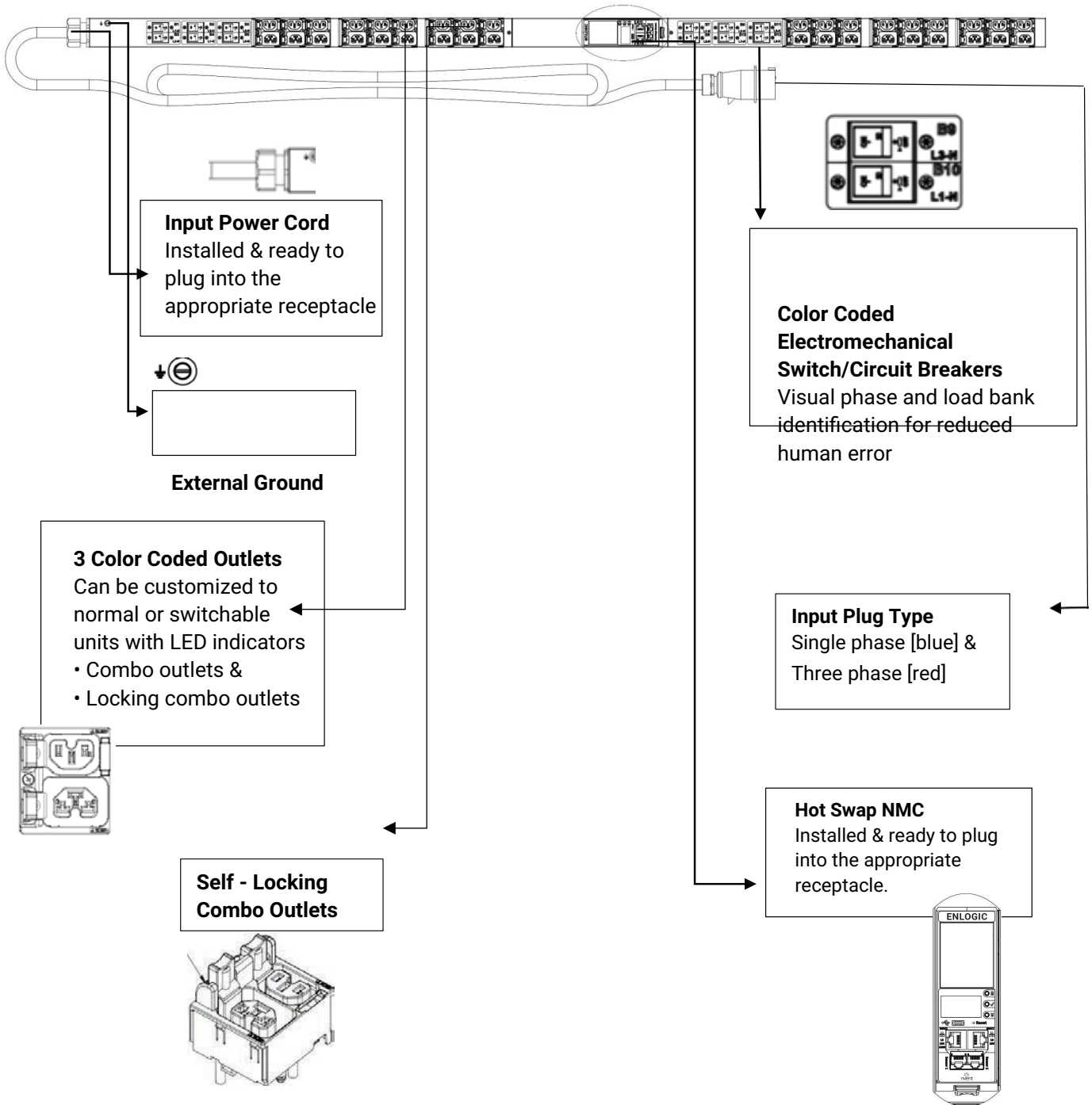
Single-Phase Models

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 16 A, will also use an outlet indicator LED in color Green.

IPDU & ITS COMPONENTS





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 Options



User Interactive Display/ OLED Screen with Navigation 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

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 1.3 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) (TLS1.3 encryption)
LDAP and RADIUS	Privilege assignment over LDAP and RADIUS

REMOTE AUTHENTICATION

Authentication Protocol	Supported
Open LDAP	YES Supported
RADIUS	YES Supported

LOGIN & PASSWORD POLICY

Communication Protocol	Supported Encryption
Strong Password	Supports case sensitive alphanumeric and symbols
Creating Password Exceptions	Supports ASCII
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 Hashing	Passwords are hashed for increased Cybersecurity. Users can now create passwords with no length constraints, such as 32 or 64 characters.

Password Exceptions	Supported
For Creating Passwords Supported character set from ASCII	Supports all special characters and symbols from the ASCII table [US English Keypad].

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://www.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 1.3

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 TLS1.3.

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.

HASHING PASSWORDS FOR INCREASED CYBERSECURITY

Password hashing aims to improve security since it increases the likelihood of a major data breach and puts data security at risk when produced or active passwords are kept on file. Depending on the algorithm chosen, hashing is the process of transforming data, such as text, numbers, and files, into a fixed-length string of letters and numbers as passwords.

The conversion of plain text to hashed values is an irreversible operation, once hashed, the original passwords cannot be recovered or generated and this enables increased security.

Hashing of passwords encompasses but is not limited to the following scenarios:

New User creation and validation

- Default users
- Existing User login validation
- Upload Configuration file
- Hot Swapping NMC

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 TLS1.3
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

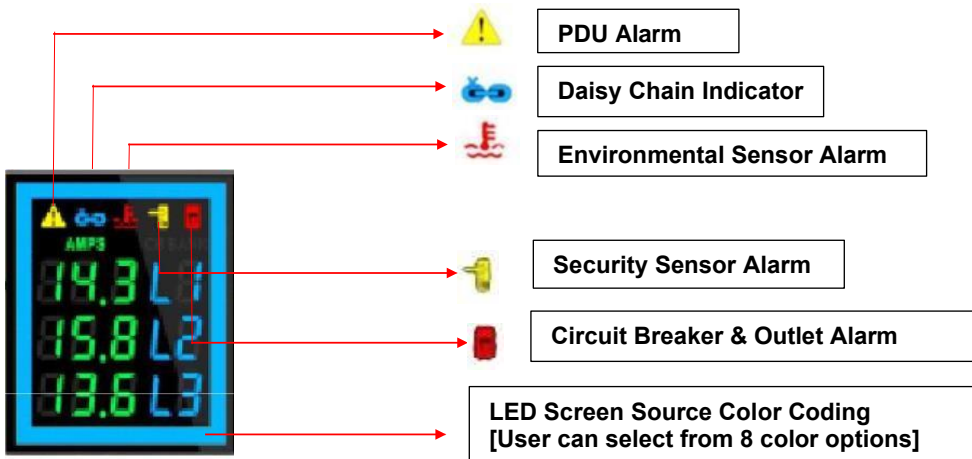
In this level information about the Current Input at each respective line, L1, L2 and L3.

- 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



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, Dry sensor, Alarm Beacon and Air flow 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.

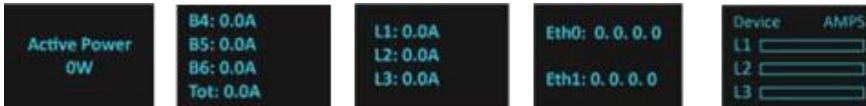
Note: The highlighted menu item is ready to be selected.

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.



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.



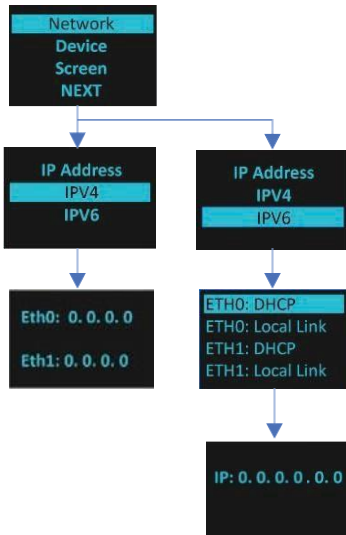
SETUP MENU

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



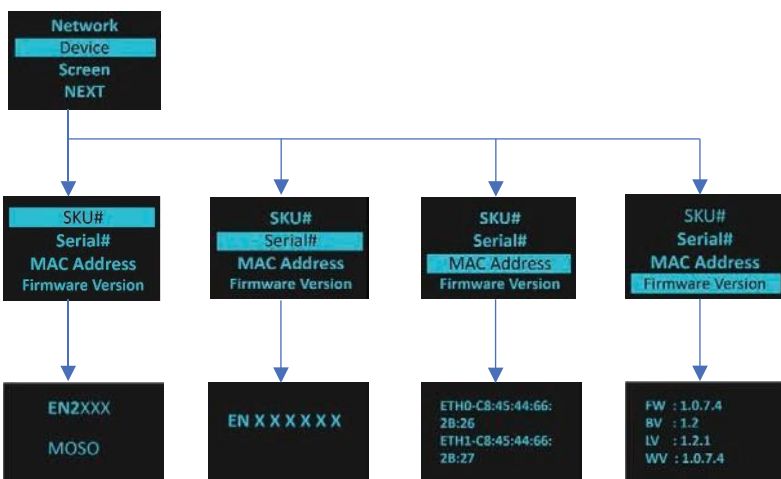
NETWORK SUBMENU

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.



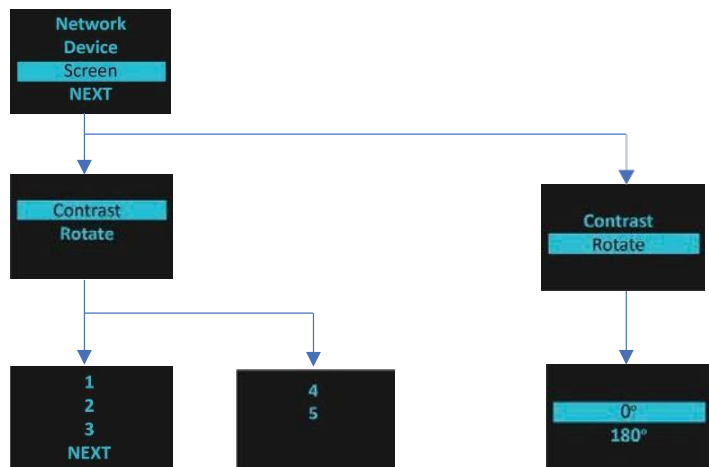
DEVICE SUBMENU

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.



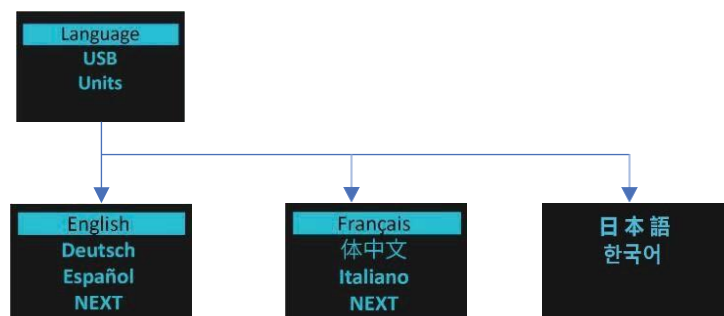
SCREEN SUBMENU

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.

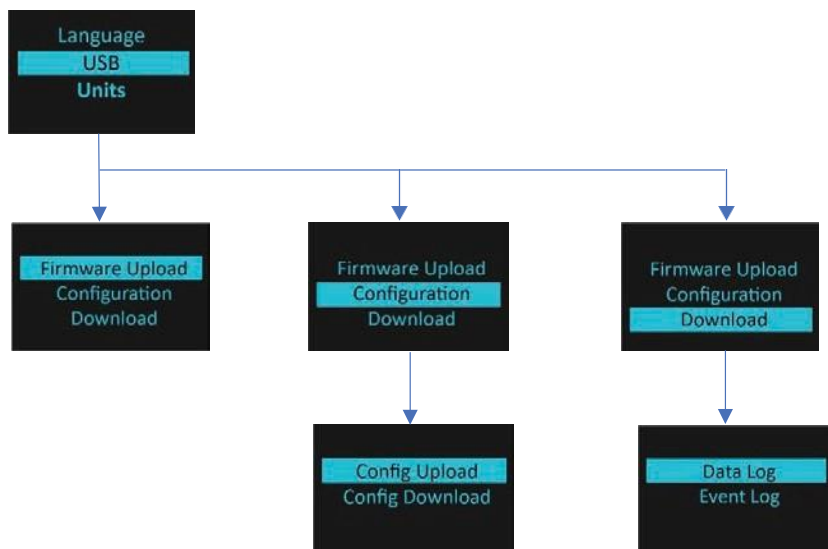


USB SUBMENU

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.

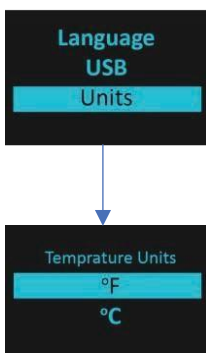
Note: If a USB drive is not present in the USB slot the PDU will enter normal operation.



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.



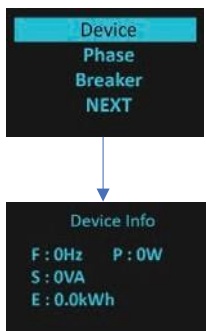
POWER MENU

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 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.



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.

Device
Phase
Breaker
NEXT



Summary
L1-L2
L2-L3
L3-L1

BREAKER SUBMENU

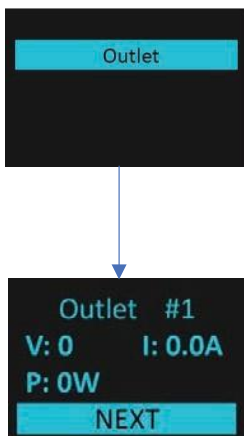
The **Breaker** submenu is to display power values for the breakers. Press **Select** to display the values of the first breaker. To go to the next breaker, Select **Next**. Press **Menu** to return to the previous menu.



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.

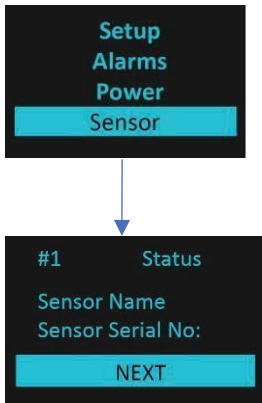
Note: Custom outlet names noted in the Web GUI do not make changes to the local display. This is done to make it easier to map to outlet numbers which can locally be seen on the outlets themselves.



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.

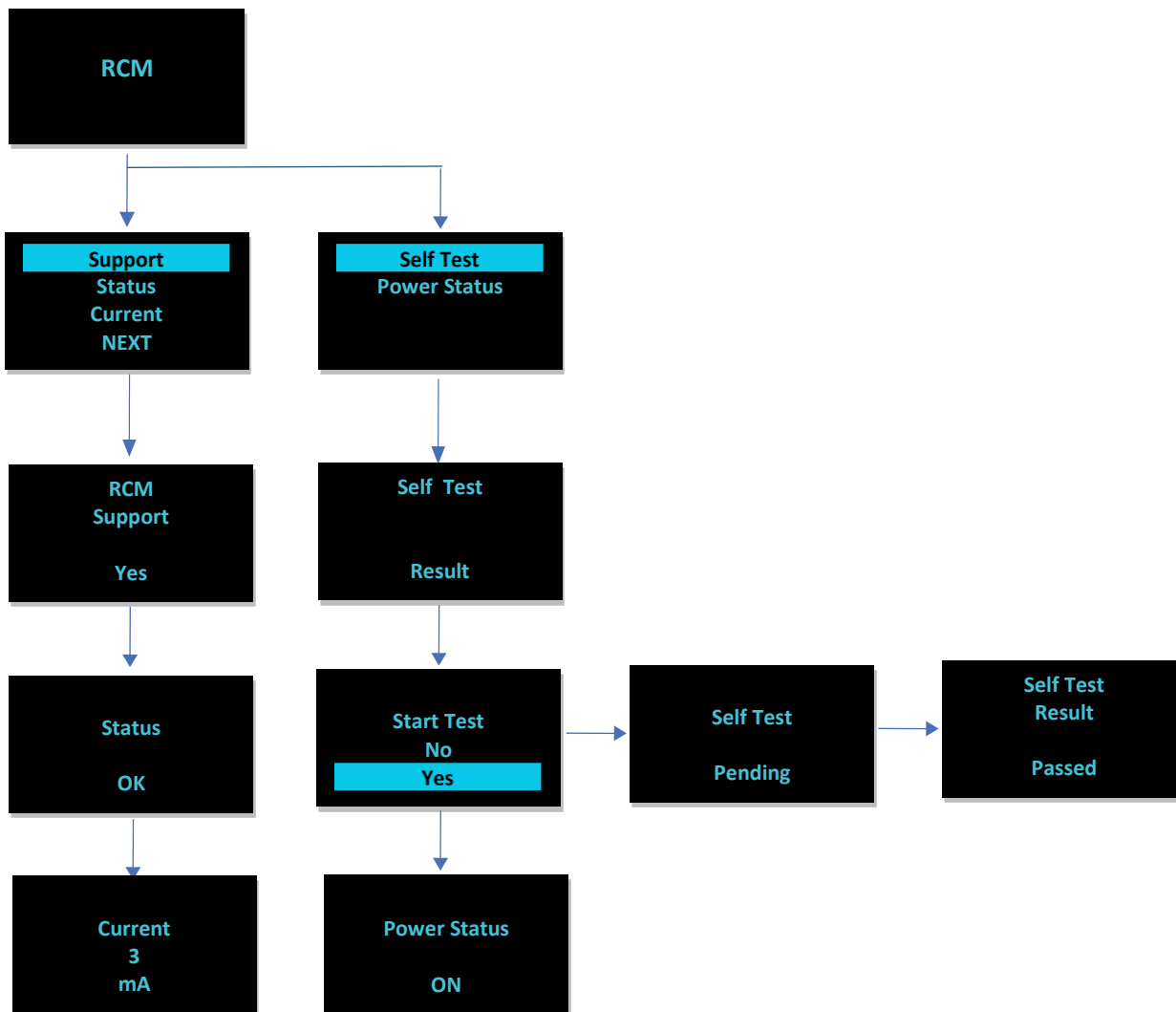
Note: Maximum of ten sensors are configured per PDU.



RCM MENU

The **RCM menu** is to display residual current monitoring support, status, RCM current, initiate on-demand self test and get power status. Press Select. This will display the RCM options. To go to the next screen, Select next. Press Menu to return to the previous menu.

Note: RMC menu is displayed only for SKU fitted with the RCM Module.



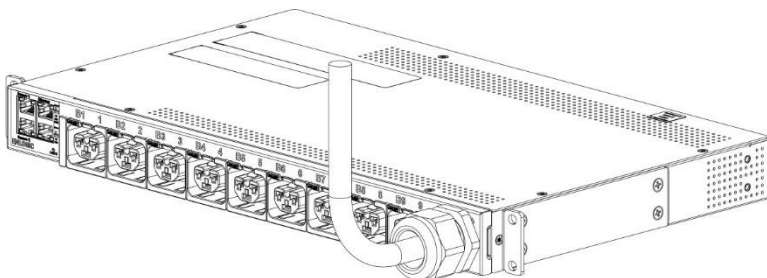
HORIZONTAL iPDU

Enlogic presents the new NMCs along with the new Horizontal Orientation iPDUs. This is a hardware and software option for customers who need a horizontal, small iPDU that could fit well within any kind of IT infrastructure enclosure. Some of the unique features of this iPDU are:

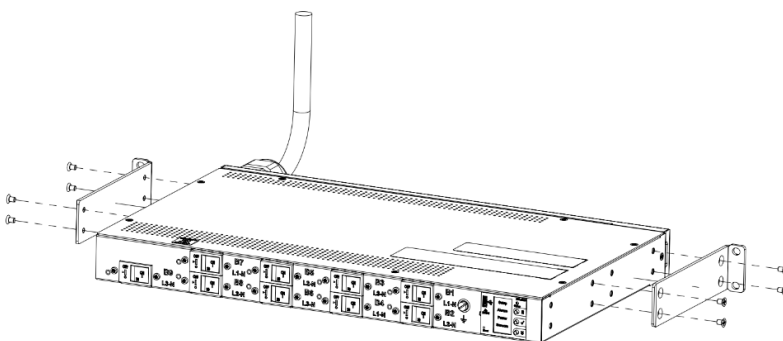
1. A single, highly visible "Status LED" with a color indicator for the horizontal NMCs. In contrast with vertical iPDUs, horizontal iPDU NMCs don't comprise of 7-segment display (that shows current and alarm values), instead, it comprises a status LED to indicate alarms/warnings. Green indicates no alarms, orange for warnings and red for critical alarms.
2. There are two sets of labeled Ethernet and sensor ports that are aligned horizontally.
3. All eight languages—French, Spanish, German, Chinese, Japanese, English, Korean, and Italian—are supported by the firmware, with relevant acronyms adapted to reflect the new orientation.
4. The updated firmware easily transitions to the horizontal orientation after identifying the kind of NMC. A CLI/SSH command is added to control the Status LED to on/off.

HORIZONTAL iPDU & its Components

- 1 Unit [1U] – Front View

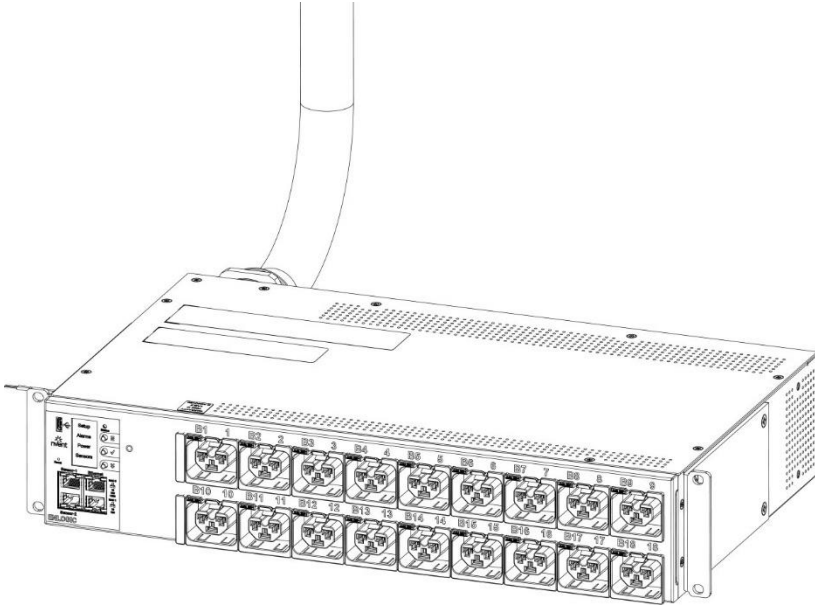


- 1 Unit [1U] – Backward View

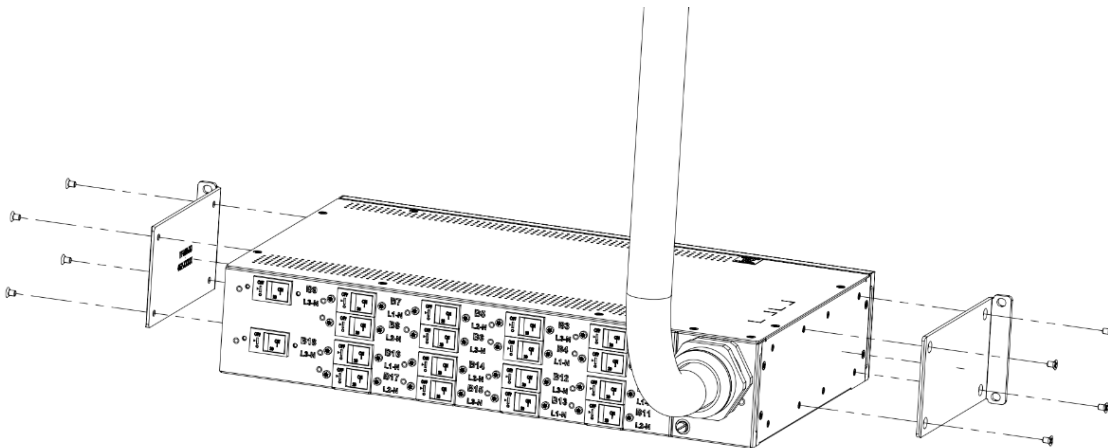


HORIZONTAL iPDU & its Components

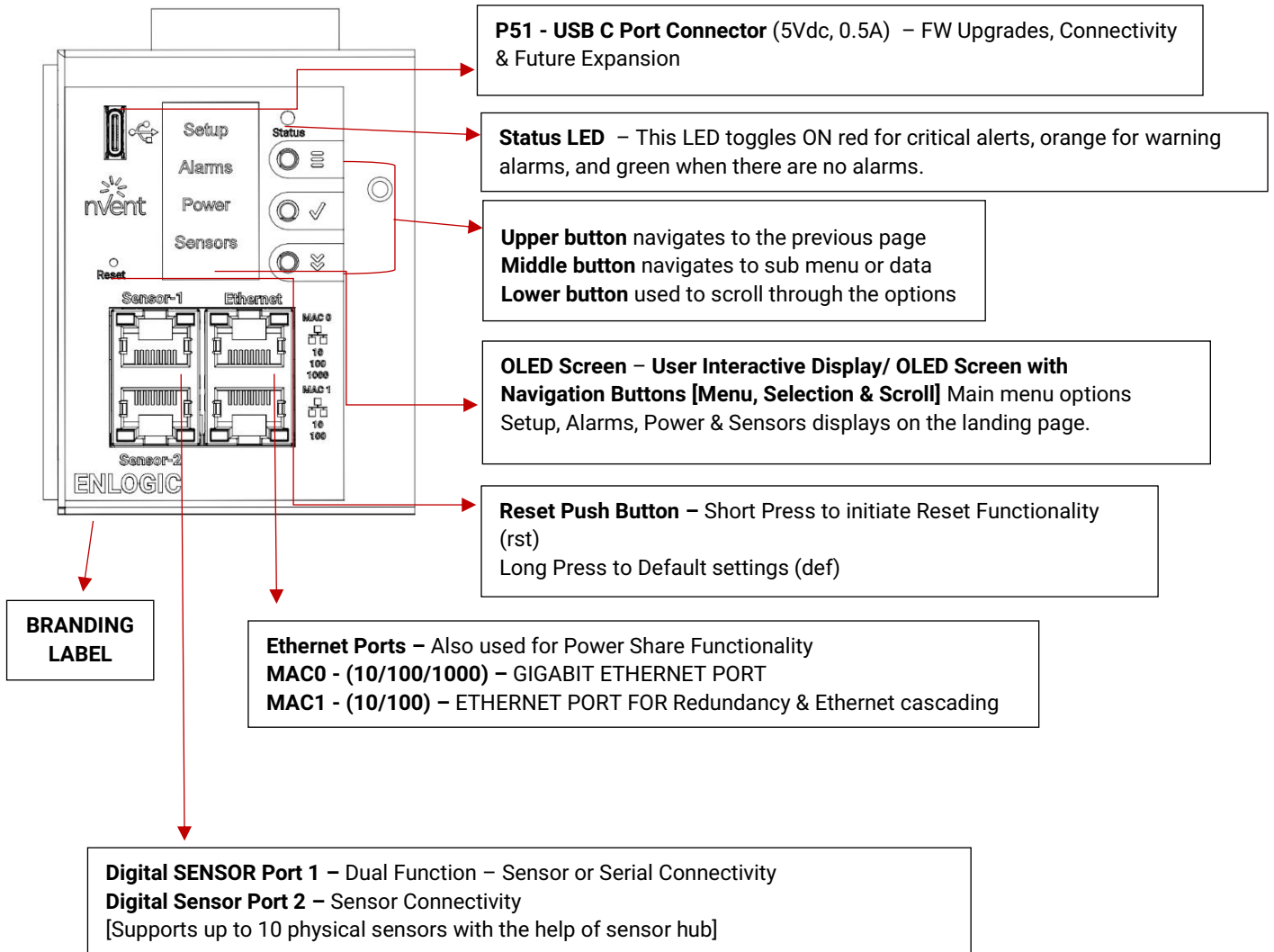
- 2 Units [2U]



- 2 Units [2U] – Backward View



Product Components NMC



DISPLAYS

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

1. The OLED screen will display a status bar, when the PDU operating system is loading.
2. OLED display: Set up, Alarms, Power, Sensors (click menu, select, and scroll to operate).

INTERFACES

There are five interfaces on all standard HORIZONTAL iPDUs, as specified below:

3. USB-C: Fast Configuration, Fast upload of firmware and download log files.
4. Ethernet Port 1: 1x Gigabit Ethernet (10/100/1000 Mbps) - Primary network port / Power Share.
5. Ethernet Port 2: 1x (10/100 Mbps) - Daisy chain / Power Share / RNA / Network.
6. Sensor-1: Primary Sensor Port / Serial Port –The Serial function is a user interface that enables the user to configure Features and update Firmware.
7. Sensor-2: Secondary Sensor Port – This port also can connect the sensors.
8. Note – Overall, the sensor ports support connecting up to total 10 sensors with the help of the sensor hub.

HORIZONTAL 1U/2U COMMANDS IN CLI

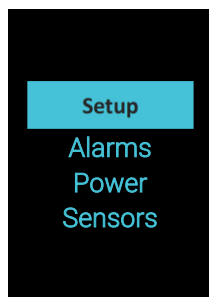
All Advantage Series/Secure CLI commands are applicable for Horizontal 1U/2U iPDUs except the specific command mentioned below:

Command	Description	Example
dev statusled [pduid/all] [on/off]	If pduid value entered, that particular PDUs LED is controlled, if all, LEDs of all nodes will be controlled.	EN2.0> dev statusled 1 on SUCCESS

MAIN MENU SELECTIONS

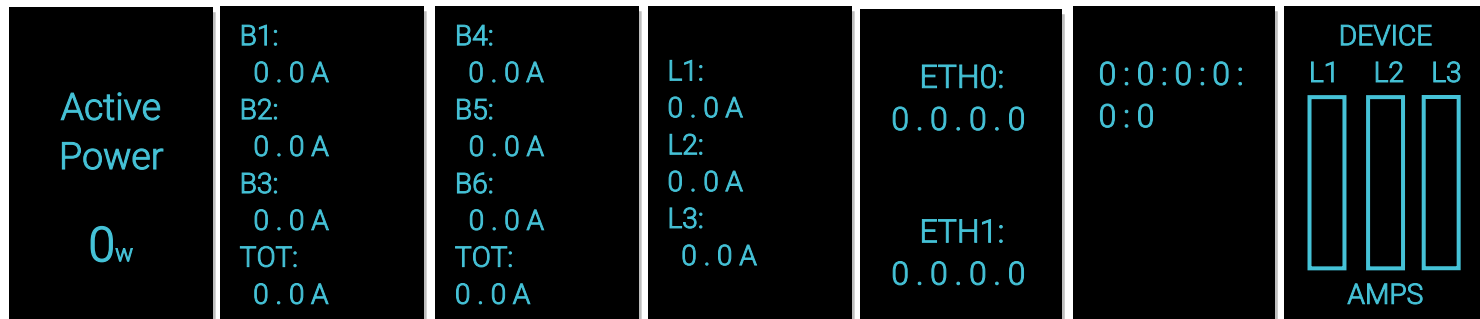
The Network Controller display has three modes:

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.



STANDBY MODE

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.

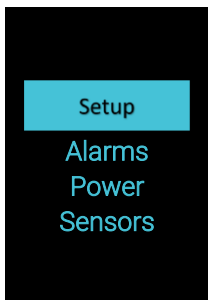


POWER SAVE MODE

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.

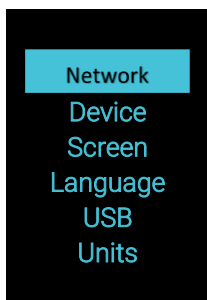
MAIN MENU SELECTIONS

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.



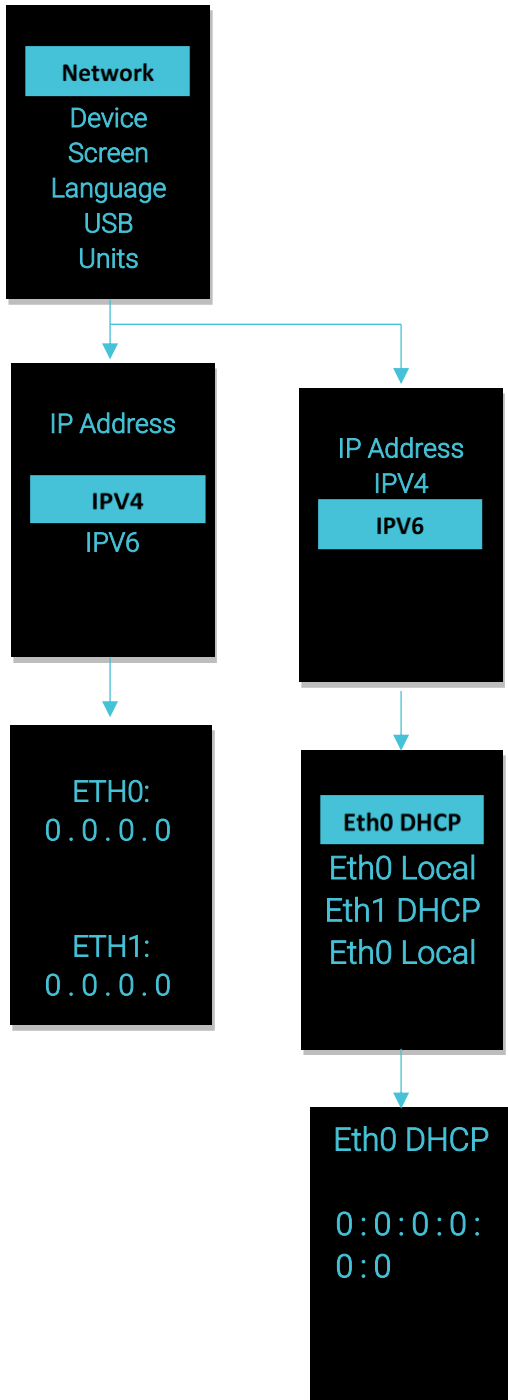
SETUP MENU

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



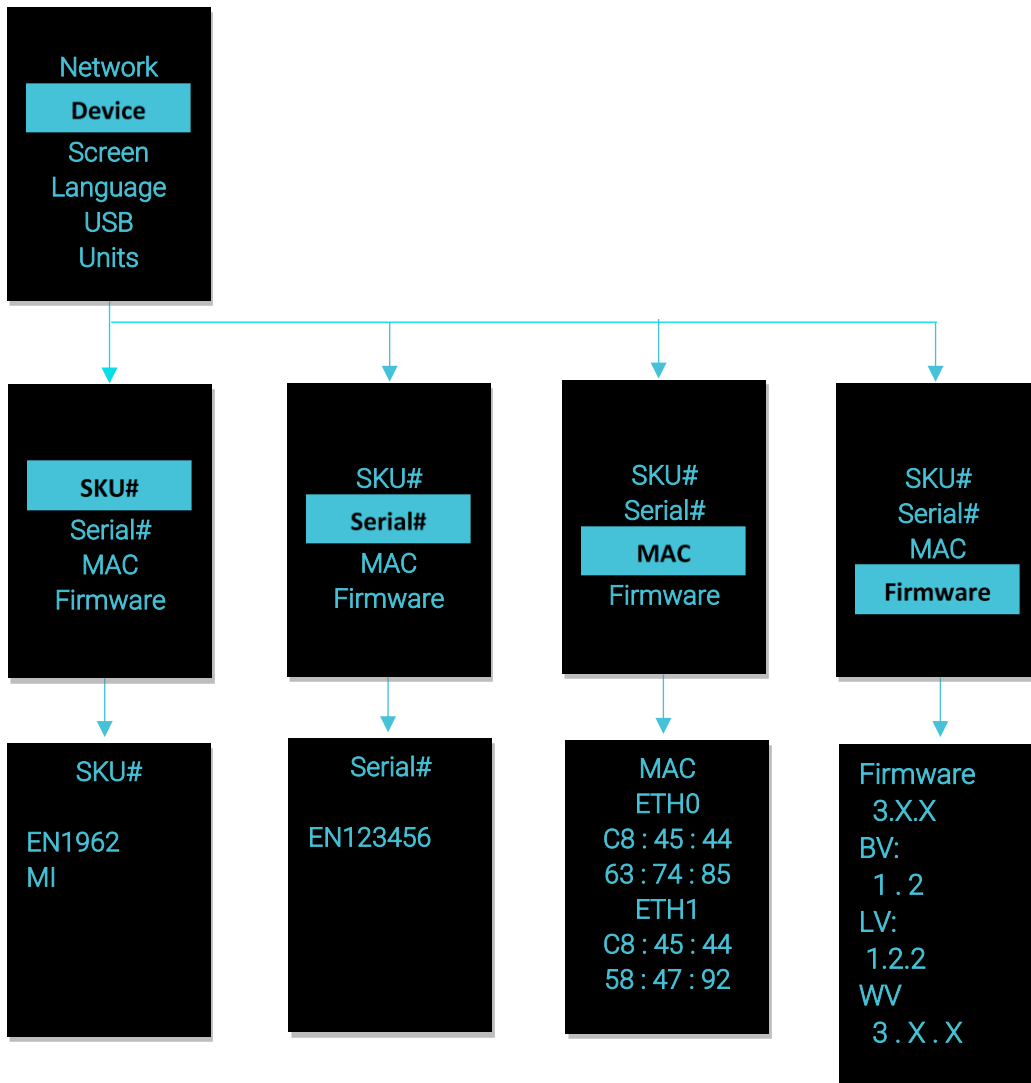
NETWORK SUBMENU

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.



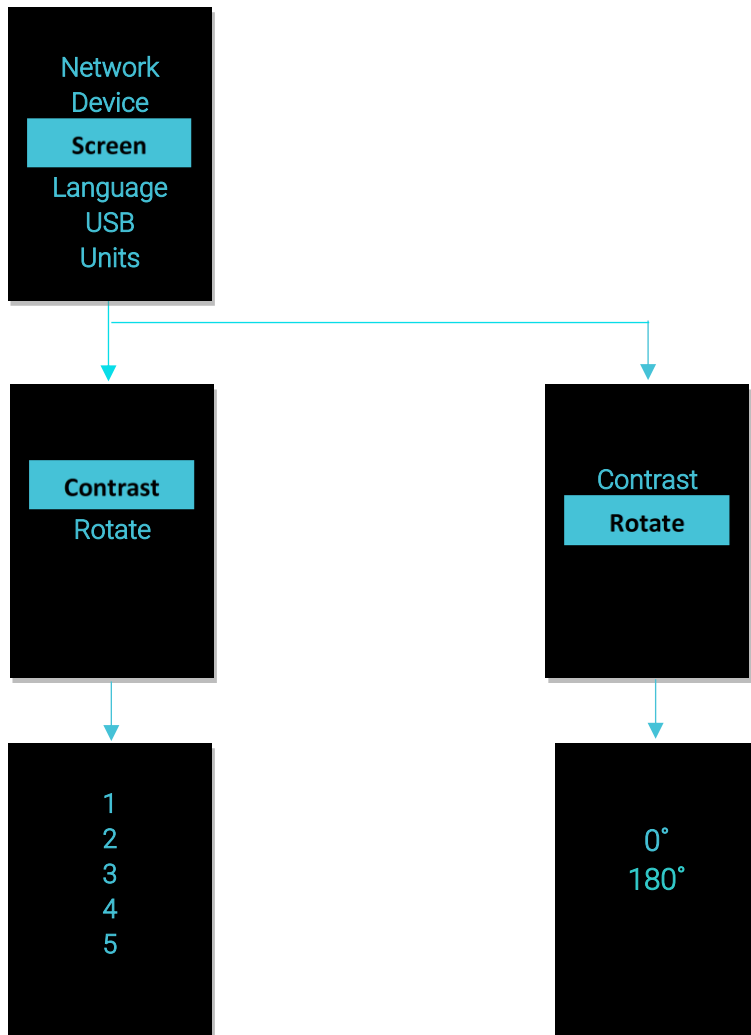
DEVICE SUBMENU

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.



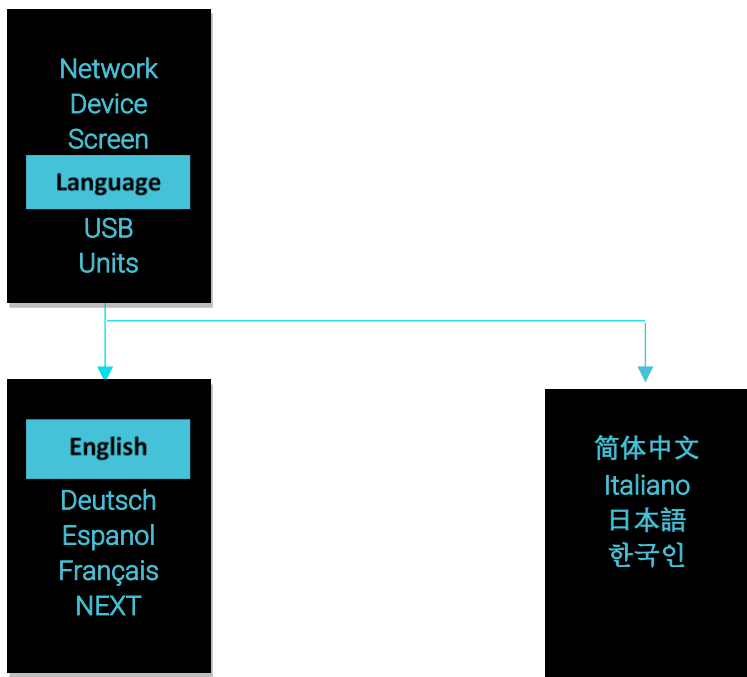
SCREEN SUBMENU

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

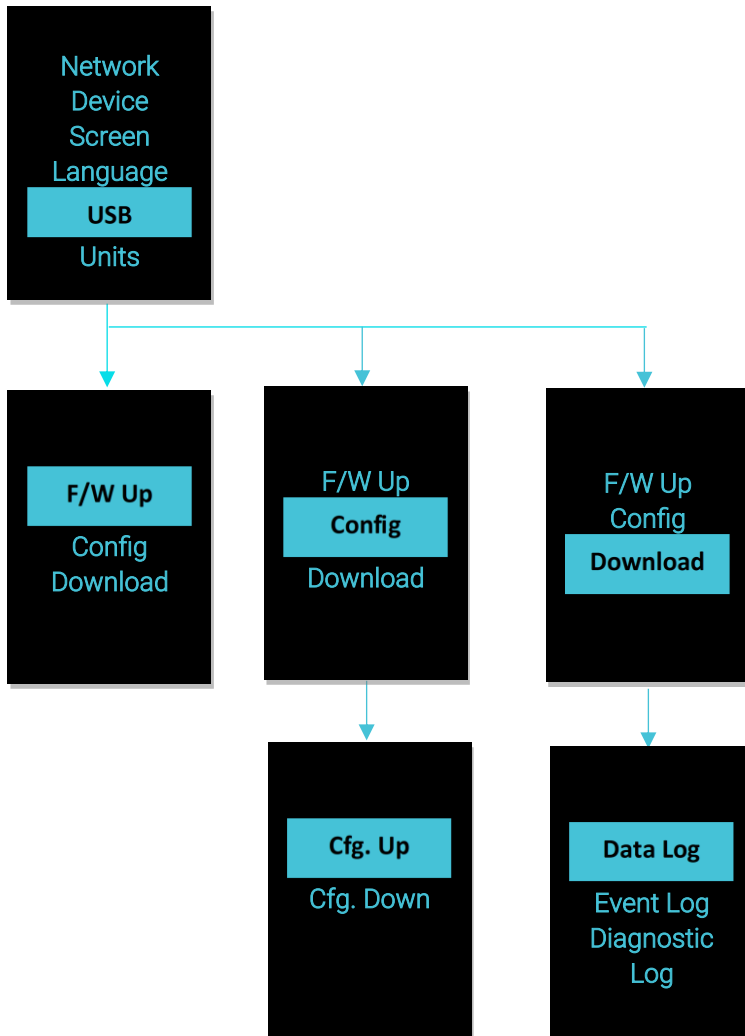
The Language submenu allows you to select the language you need to use. On the Setup menu, scroll down to highlight Language. Press Select to display the screens to select the submenu. After you select the values, press Select to set the values as displayed on the screen. Press Menu to return to the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

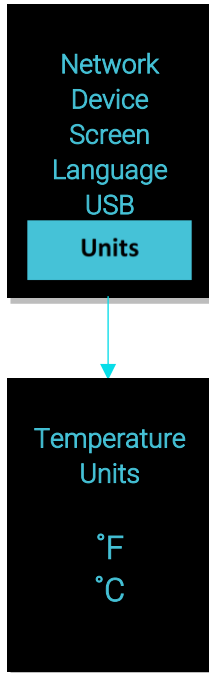
Note: If a USB drive is not present in the USB slot the PDU will enter normal operation.



UNITS SUBMENU

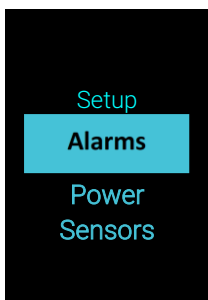
The Units submenu displays the temperature units. On the Setup menu, scroll down to highlight Units. Press Select to enter the Units Submenu. After you select the values, press Select to set the values as displayed on the screen. Press Menu to return to the previous menu.

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



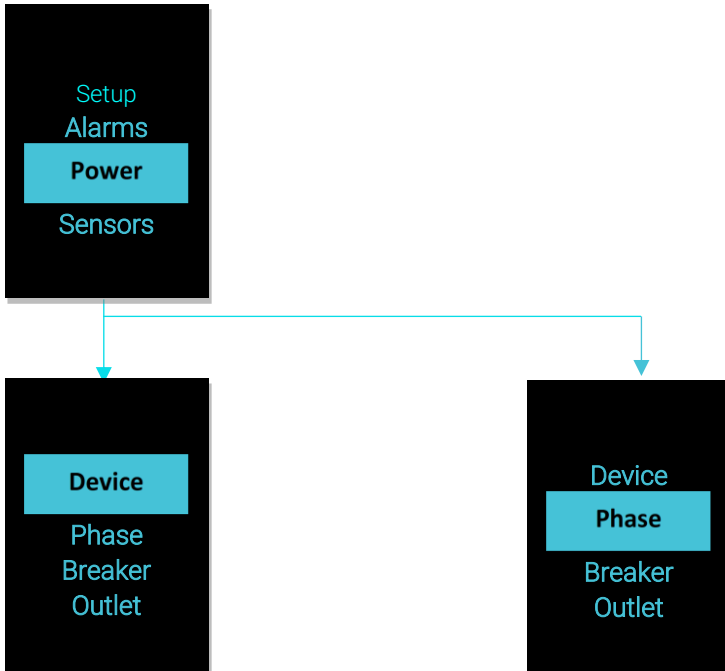
ALARMS SUBMENU

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.



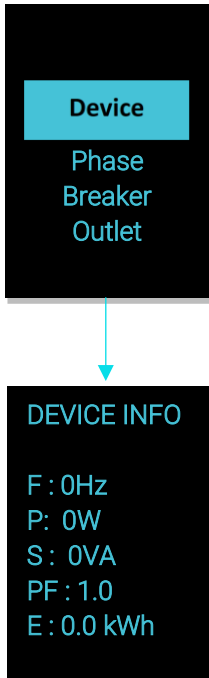
POWER SUBMENU

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.



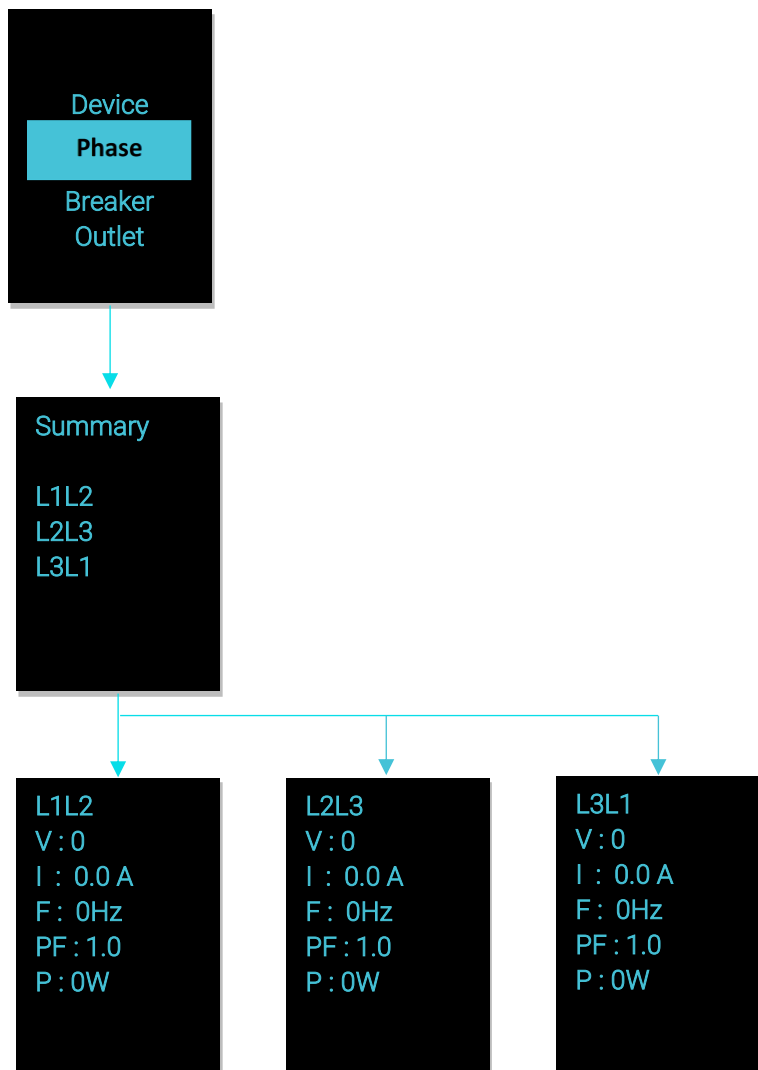
DEVICE SUBMENU

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.



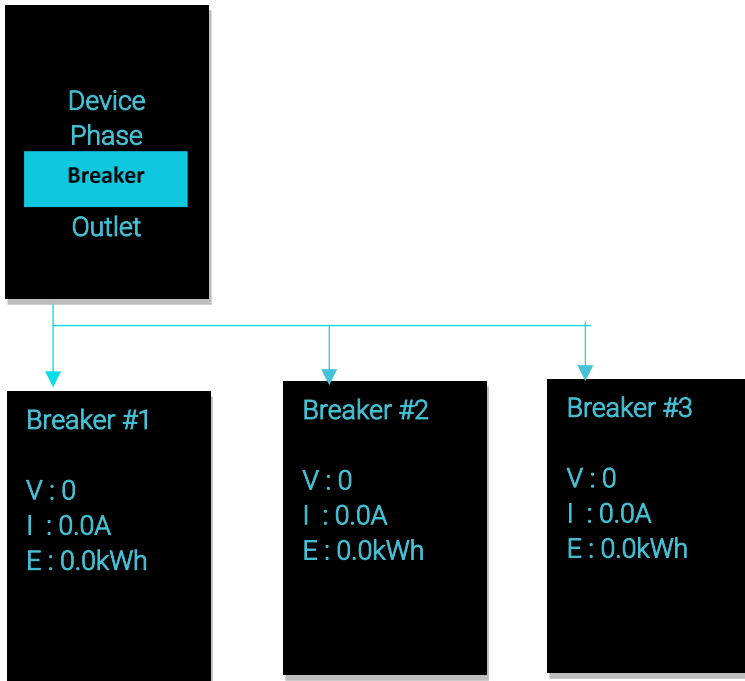
PHASE SUBMENU

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

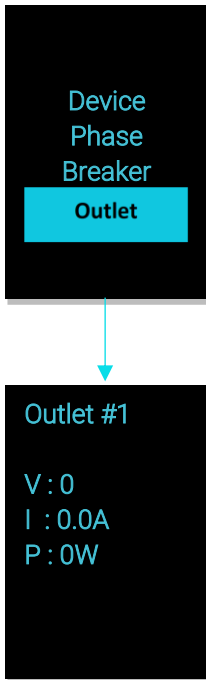
The Breaker submenu is to display power values for the breakers. Press Select to display the values of the first breaker. To go to the next breaker, Select Next. Press Menu to return to the previous menu.



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.

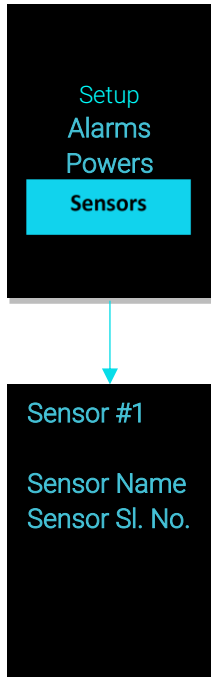
Note: Custom outlet names noted in the Web GUI do not make changes to the local display. This is done to make it easier to map to outlet numbers which can locally be seen on the outlets themselves.



SENSORS SUBMENU

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.

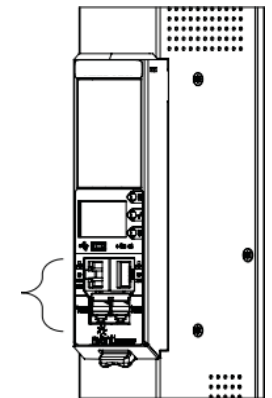
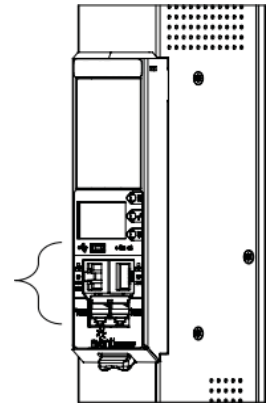


Ribbon Cable

INSTALLATION

Disconnect the NMC

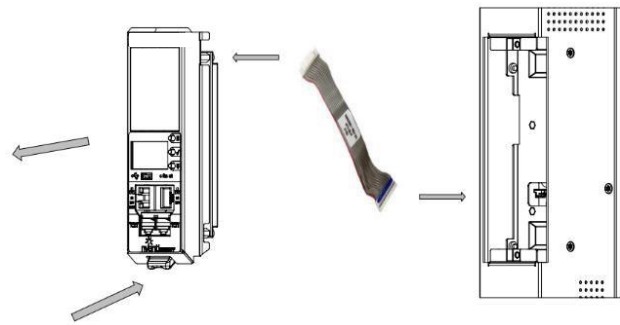
1. Write down the details of the ports and the RJ45 plugs connected, this will enable reconnecting them after installing the replacement NMC.



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.

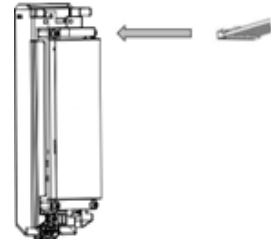
Note – Do not disconnect the Ribbon cable from the PDU back board.

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

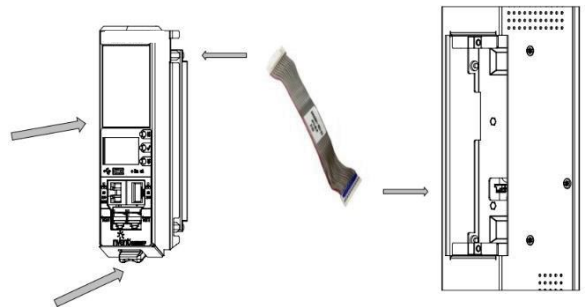
5. Plug the Ribbon cable into the connecting socket on the top section of the replacement NMC. Gently fold the Ribbon cable. Mount the NMC back into the PDU chassis.



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.



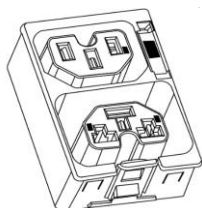
OUTLET UNITS

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

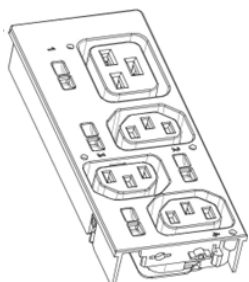
NAM & EAU

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

NAM & EAU

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:



C13 Outlet

NAM & EAU

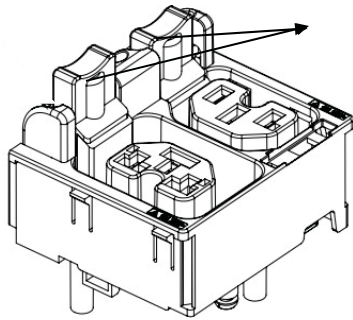
C19 Outlet

NAM & EAU

- 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.



Depress Release Button to Install the Plug

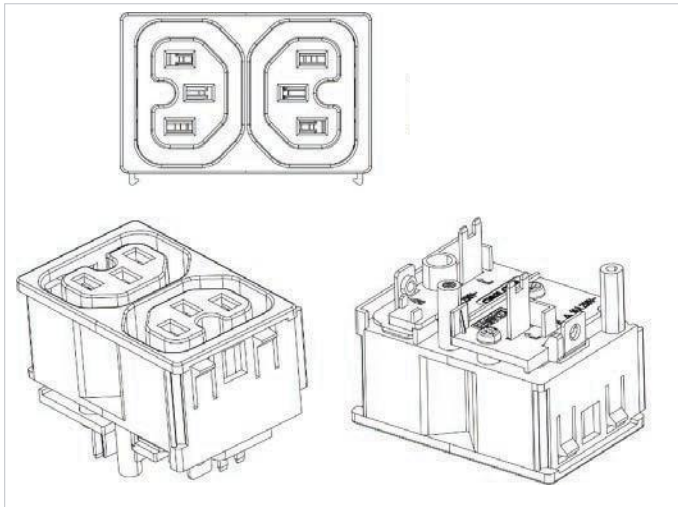
Locking Combo Outlet port features both the Combo Outlet C13/C15 [2 in 1] Outlet NAM & EAU and C13/C15/C19 [3-in-1] Outlet NAM & EAU with an additional locking port facility.

The specifications of these Locking Combo Outlet Units are :

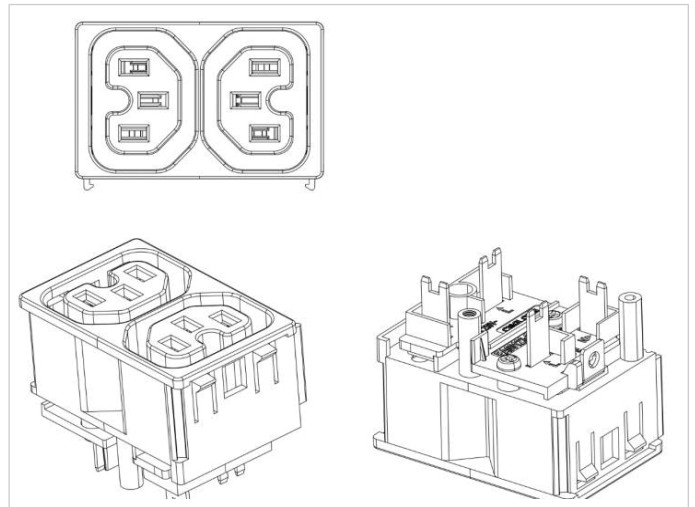
- The release button must be fully pressed [depress it] prior to installing the plug.
- Both type of plugs with and without locking clips can be inserted.
- The plugs can be installed just by pushing into the outlets directly without depressing release button.
- To unlock, fully depress release button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

NEWLY LAUNCHED OUTLETS & VARIANTS

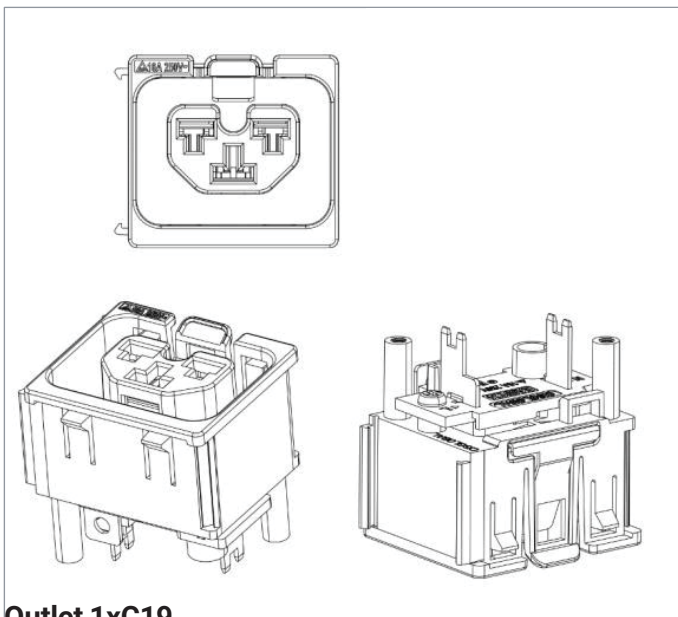
The Advantage Secure PDU features a new range of individual and combination Regular/Locking Outlet Port configurations.



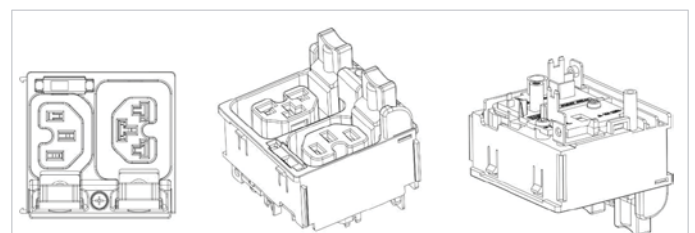
**Outlet 2xC13
Combo**



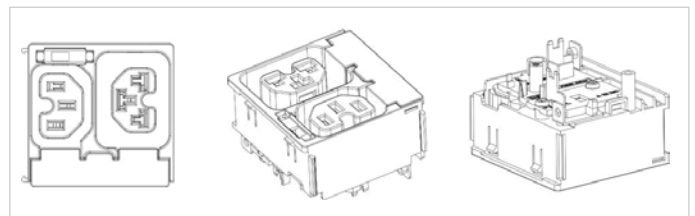
Outlet 2xC13 Combo



**Outlet 1xC19
Combo**



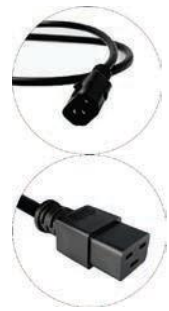
Outlet C13/ C19 Locking



Outlet C13/ C19 Combo

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 accidentally 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.





Getting Started

MOUNTING PDU IN SERVER CABINET

Enlogic iPDU's 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 PDU's 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.

Note: You may need to use a DB9 serial to USB connection cable for this step to connect via a serial port if a serial port is not available on your computer.

3. 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

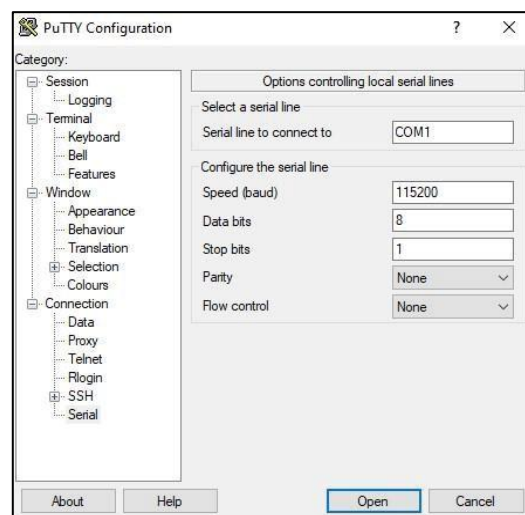
4. Use the default initial login indicated below.

Note: Username and Password are both case sensitive.

- Username: admin
- Password: 12345678

5. The EN2.0> prompt appears after you have logged in.
6. 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.

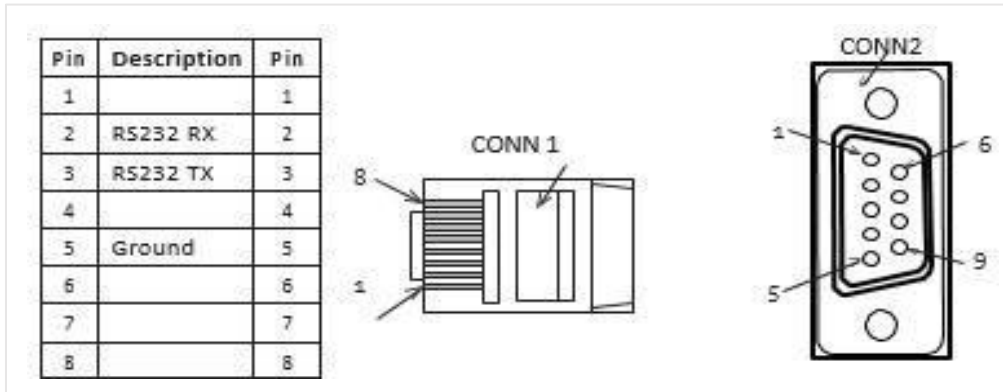
- For the Net eth0 and eth1 IPv4 DHCP configuration, configure the below parameter.
- net tcpip eth0dhcp
- net tcpip eth1dhcp
- Enter "Y" to validate and reboot the network management card.
- For the static IPv4 configuration, configure the below parameters.
- net tcpip eth0static x.x.x.x (ipaddress) 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:

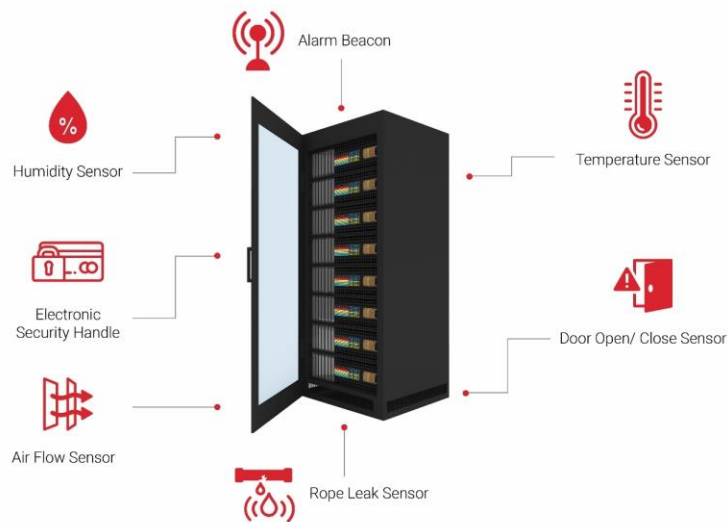
Refer to the **Web UI** section and **Command Line Interface** section for more information about managing the PDU.



CONNECTING SENSORS (OPTIONAL)

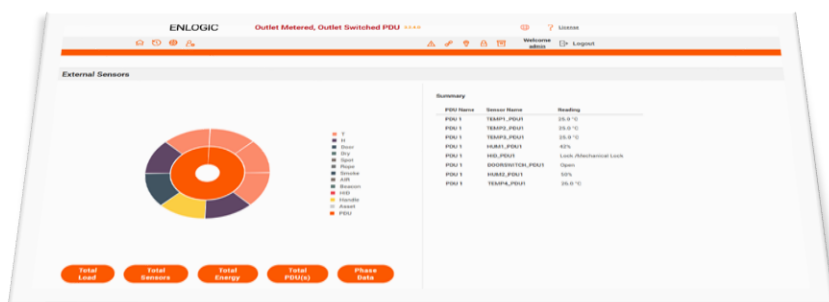
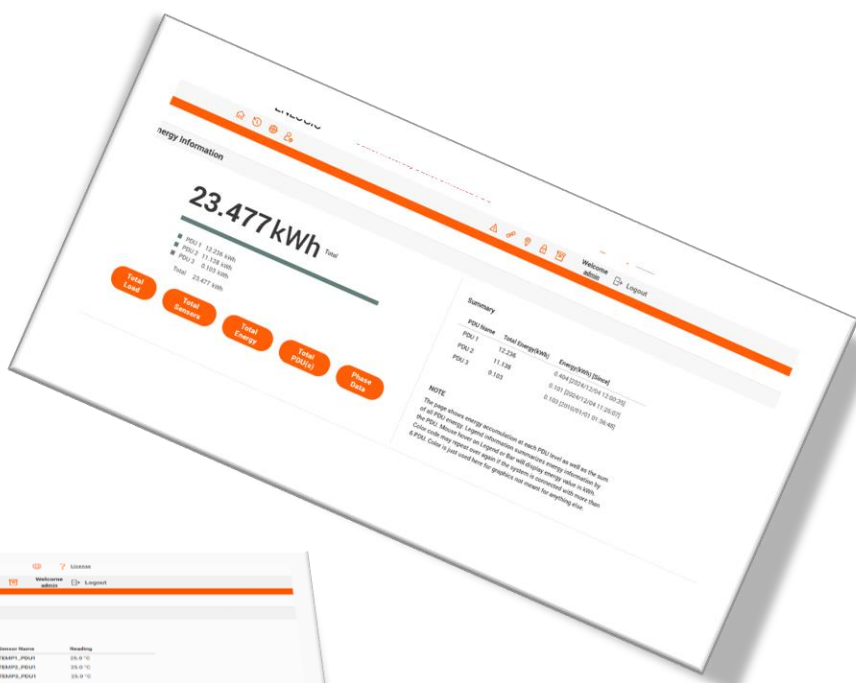
To enable the Advantage Secure device to detect Enlogic conditions, connect one or more sensors to the PDU sensor port 1 or 2. The maximum distance for sensor cabling, which is plugged into the device sensor port should not exceed 100 feet (30 m). The maximum number of sensor detection points should 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
Air flow Sensor	1	EA9205
Alarm Beacon Sensor	1	EA9101
RJ45-DB9 CABLE	1	EA9119
USB TO RS232 (RJ45-USB) CABLE	1	EA9128
HID RACK ACCESS Kit	1	EA9130
E-Handle (RFID) – no keypad available	2	EA9502
• E-Handle (with addition sensors of 3 Temperature + 1 Door)	6	
E-Handle (RFID & User PIN authentication) – with keypad	2	EA9500
• E-Handle (with addition sensors of 3 Temperature + 1 Door)	6	

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.



nvent ENLOGIC


Outlet Metered, Outlet Switched PDU






Username

Password

Log In

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.
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	°C	admin		
user	°C	user		
manager	°C	manager		


ENLOGIC
Outlet Metered, Outlet Switched PDU
License

Home Refresh Settings Profile
Warning Edit Light Lock Mail
Welcome admin Logout

° F
Add Role
Add User



Users

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

LDAP Configuration 


Enable	<input type="checkbox"/>
LDAP Server	
Security	none
Port	389
Type	OpenLDAP
Base DN	
Bind Password	****
Search User DN	
Login Name Attribute	
User Entry Object Class	

Radius Configuration


Enable	Server	Port	Secret	Action
<input type="checkbox"/>	1812	*****		
<input type="checkbox"/>	1812	*****		

Roles

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

Session Management 

Sign-In retries allowed	<input checked="" type="checkbox"/>
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	<input type="checkbox"/>
Enforce at least one upper case character	<input type="checkbox"/>
Enforce at least one numeric character	<input checked="" type="checkbox"/>
Enforce at least one special character	<input type="checkbox"/>

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

Save

NAVIGATING THROUGH THE WEB UI

The landing page, followed by the login page.






Outlet Metered, Outlet Switched PDU


Username

Password


Log In

ENLOGIC **Outlet Metered, Outlet Switched PDU**


 License

Welcome **admin**  Logout


Total Load



0 %
PDU#1



0 %
PDU#2



0 %
PDU#3

Total Load
Total Sensors
Total Energy
Total PDU(s)
Phase Data

Summary

PDU	Apparent Power(VA)	Active Power(W)	Power Factor
PDU 1	0	0	1.00
PDU 2	0	0	1.00
PDU 3	0	0	1.00

SINGLE USER MULTIPLE SESSIONS (SUMS)












The **Single User Multiple Session (SUMS)** feature allows users to use the same login credentials to configure and monitor parameters across multiple sessions without logging out previous sessions of the same user.

1. This functionality allows users to configure various parameters present on different web pages.
2. Once parameters are updated, the same values reflect across all sessions upon navigating to respective web pages, thereby enhancing efficiency.

The screenshot displays two tables from a web application. The left table is a log table with columns 'Type', 'Description', and 'Date & Time'. It contains multiple entries, including audit logs for user logins and configuration logs for various system settings. The right table is a network traffic table with columns 'Name', 'Status', 'Type', 'Initiator', 'Size', 'Time', and 'Fulfil'. It lists various API calls such as 'shrgetsensorlist', 'shrgetsensors', and 'shrgetsensors', along with their respective sizes and completion times.

3. The system supports up to 10 sessions via WEBUI and REDFISH, ensuring that performance remains largely unaffected by the increase in session numbers.
4. Multiple sessions allow a user to monitor all details using the same user login credentials in multiple sessions (using browser tabs/windows) and allows to configure different parameters present in different Web pages.

The screenshot shows a web dashboard with multiple browser tabs open. The main dashboard displays a 'Total Load' section with a circular gauge showing 0% load. Below this, there are three buttons labeled 'Total Load', 'Total Sensors', and 'Total Energy'. The dashboard also features a 'View Logs' section with a table of log entries. A network traffic table is visible in the background, showing various API calls and their details. The dashboard is titled 'Dashboard | Enlogic' and includes a 'Welcome admin' message and a 'Logout' button.

Icon	Description
	<p>Home Icon</p> <p>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.</p>
	<p>Logs icon</p> <p>Click this icon to view and download the logs and data logs of the PDU.</p>
	<p>Settings Icon</p> <p>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.</p>
	<p>User Settings Icon</p> <p>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.</p> <p>Also, configure the RADIUS and LDAP servers</p>
	<p>Alarms</p> <p>Click this Alarm icon to view the details of the active critical alarms and active warning alarms.</p> <p>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.</p> <p>Red – Critical Alarms Yellow – Warnings</p>
	<p>Link</p> <p>This Icon indicates the daisy-chain connection status alarms.</p>
	<p>Sensor Warning</p> <p>This icon represents the sensor related alarms like:</p> <ul style="list-style-type: none"> • Temp • Humidity • Dry
	<p>Status Alarms</p> <p>This icon indicates the Door and HID sensor status alarms.</p>
	<p>Status Alarms</p> <p>This icon indicates the CB and Outlet status alarms.</p>
	<p>Select a Language</p> <p>This icon allows the user to select a Language.</p> <p>Currently eight languages are available to choose: English, French, Italian, Korean, German, Spanish, Japanese and Chinese.</p>
	<p>Click this icon to download system diagnostic logs or navigate to the user guide.</p>

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

The screenshot shows the ENLOGIC dashboard interface. At the top, the header includes the logo 'ENLOGIC', the status 'Outlet Metered, Outlet Switched PDU', and a 'License' link. Below the header is a navigation bar with a 'Home' icon dropdown menu open, showing options like 'Dashboard', 'Identification', 'Control & Manage', 'Outlet Grouping', and 'Power Share'. The main content area is titled 'Total Load' and features three circular gauges for PDU#1, PDU#2, and PDU#3, each showing 0% load. To the right is a 'Summary' table with columns for PDU, Apparent Power(VA), Active Power(W), and Power Factor. At the bottom, there are five buttons: 'Total Load', 'Total Sensors', 'Total Energy', 'Total PDU(s)', and 'Phase Data'.

PDU	Apparent Power(VA)	Active Power(W)	Power Factor
PDU.1	0	0	1.00
PDU.2	0	0	1.00
PDU.3	0	0	1.00

TOTAL LOAD

This screenshot is identical to the one above, showing the ENLOGIC dashboard. The 'Total Load' section displays three gauges for PDU#1, PDU#2, and PDU#3, all at 0%. The 'Summary' table on the right provides power metrics for each PDU. The navigation bar and bottom buttons remain the same.

PDU	Apparent Power(VA)	Active Power(W)	Power Factor
PDU.1	0	0	1.00
PDU.2	0	0	1.00
PDU.3	0	0	1.00

TOTAL ENERGY

ENLOGIC
Outlet Metered, Outlet Switched PDU :
🌐 ? License

🏠 ⌛ ⚙️ 👤
⚠️ 🔗 🔦 🔒 🗑️
Welcome admin 🚪 Logout

Energy Information

23.477 kWh Total

- PDU 1 12.236 kWh
- PDU 2 11.138 kWh
- PDU 3 0.103 kWh

Total 23.477 kWh

Total Load
Total Sensors
Total Energy
Total PDU(s)
Phase Data

Summary

PDU Name	Total Energy(kWh)	Energy(kWh) [Since]
PDU 1	12.236	0.404 [2024/12/04 12:00:35]
PDU 2	11.138	0.101 [2024/12/04 11:26:07]
PDU 3	0.103	0.103 [2010/01/01 01:36:48]

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.

ENLOGIC
Outlet Metered, Outlet Switched PDU
🌐 ? License

🏠 ⌛ ⚙️ 👤
⚠️ 🔗 🔦 🔒 🗑️
Welcome admin 🚪 Logout

Energy Information

12.236 kWh PDU 1

- PDU 1 12.236 kWh
- PDU 2 11.138 kWh
- PDU 3 0.103 kWh

Total 23.477 kWh

Total Load
Total Sensors
Total Energy
Total PDU(s)
Phase Data

Summary

PDU Name	Total Energy(kWh)	Energy(kWh) [Since]
PDU 1	12.236	0.404 [2024/12/04 12:00:35]
PDU 2	11.138	0.101 [2024/12/04 11:26:07]
PDU 3	0.103	0.103 [2010/01/01 01:36:48]

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.

ENLOGIC
Outlet Metered, Outlet Switched PDU
🌐 ? License

🏠 ⌛ ⚙️ 👤
⚠️ 🔗 🔦 🔒 🗑️
Welcome admin 🚪 Logout

Energy Information

11.138 kWh PDU 2

- PDU 1 12.236 kWh
- PDU 2 11.138 kWh
- PDU 3 0.103 kWh

Total 23.477 kWh

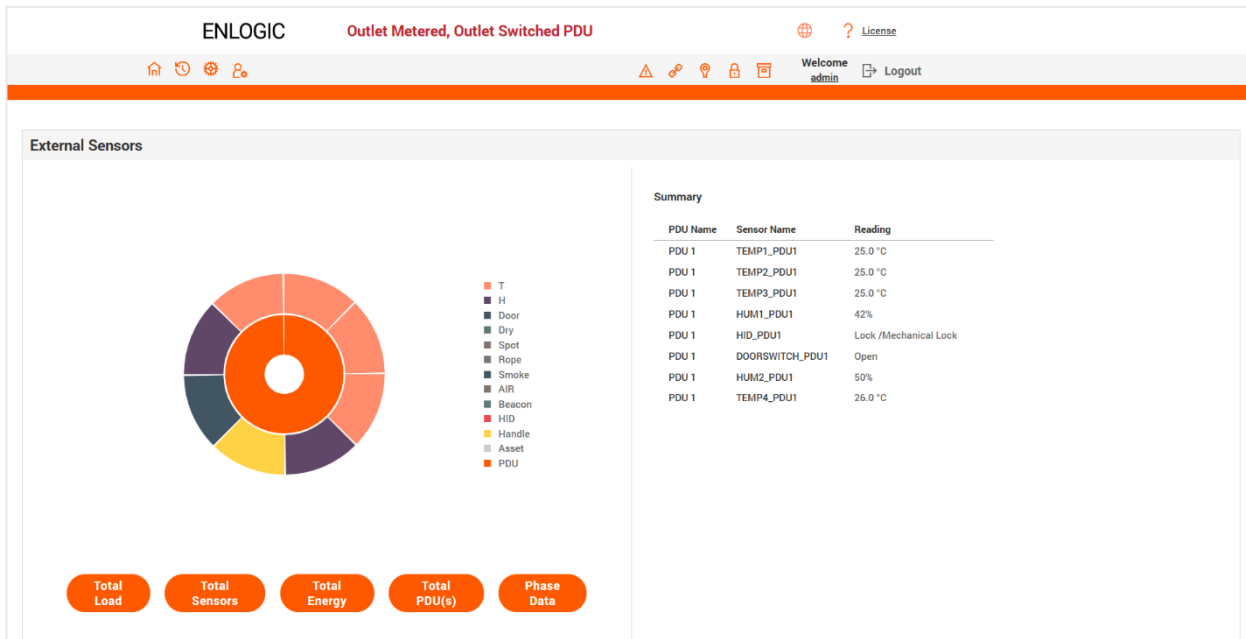
Total Load
Total Sensors
Total Energy
Total PDU(s)
Phase Data

Summary

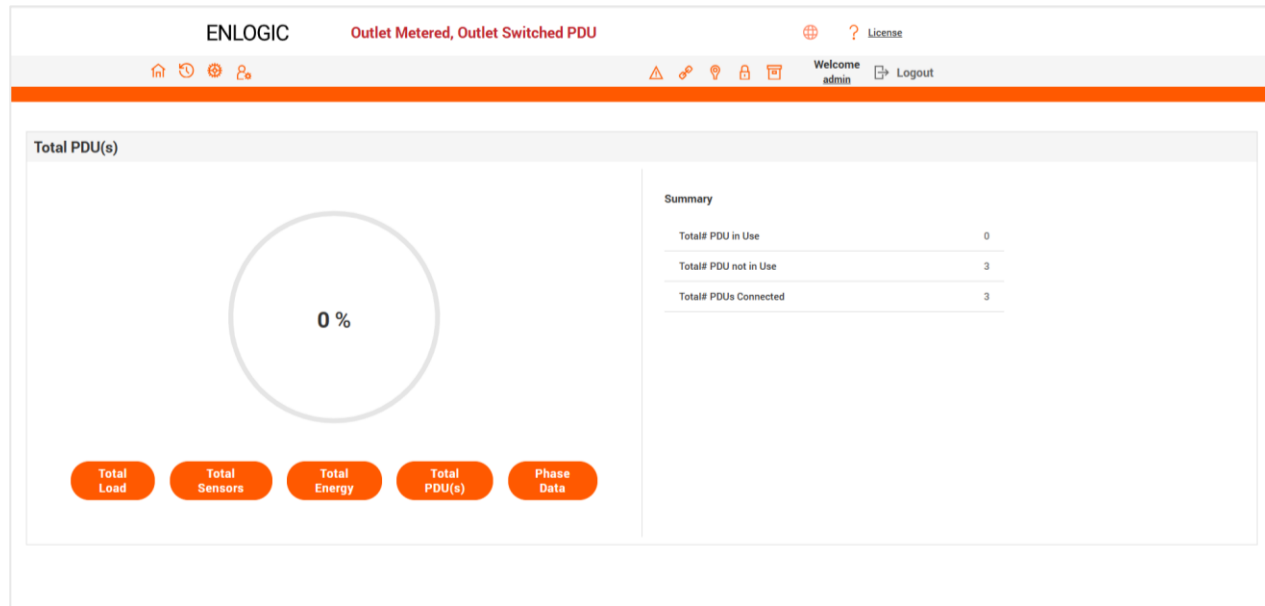
PDU Name	Total Energy(kWh)	Energy(kWh) [Since]
PDU 1	12.236	0.404 [2024/12/04 12:00:35]
PDU 2	11.138	0.101 [2024/12/04 11:26:07]
PDU 3	0.103	0.103 [2010/01/01 01:36:48]

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



TOTAL PDUS



PHASE DATA

ENLOGIC
Outlet Metered, Outlet Switched PDU
License

Home
Alerts
Lightbulb
Lock
Logout

Phase Data

PDU#	Phase	Current(A)	Voltage(V)	Apparent Power(VA)	Active Power(W)	Power Factor	Total Energy(kWh)
PDU 1	Phase 1	0.00	227.60	0.00	0.00	1.00	0.10
PDU 1	Phase 2	0.00	229.40	0.00	0.00	1.00	0.30
PDU 1	Phase 3	0.00	228.74	0.00	0.00	1.00	0.00
PDU 2	Phase 1	0.00	227.71	0.00	0.00	1.00	0.10
PDU 2	Phase 2	0.00	229.28	0.00	0.00	1.00	0.00
PDU 2	Phase 3	0.00	228.61	0.00	0.00	1.00	0.00
PDU 3	Phase 1	0.00	227.98	0.00	0.00	1.00	0.10
PDU 3	Phase 2	0.00	229.94	0.00	0.00	1.00	0.00
PDU 3	Phase 3	0.00	228.94	0.00	0.00	1.00	0.00

Total Load
Total Sensors
Total Energy
Total PDU(s)
Phase Data

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.

ENLOGIC
Outlet Metered, Outlet Switched PDU
License

Home
Alerts
Lightbulb
Lock
Logout

Identification

System Information

Name	Value	Name	Value
System Name		MAC Address	C8-47-44-66-28-35
Contact Name		IPv4 Address	10.20.15.82
Contact Email		IPv4 Link Local Address	fe80::6402:1084:fe03:7a99
Contact Phone		IPv6 Auto Configured Address	2001:1111:1111:1121:deba:84c6:9087:772f
Contact Location			

PDU Information

PDU#s 1-1


1

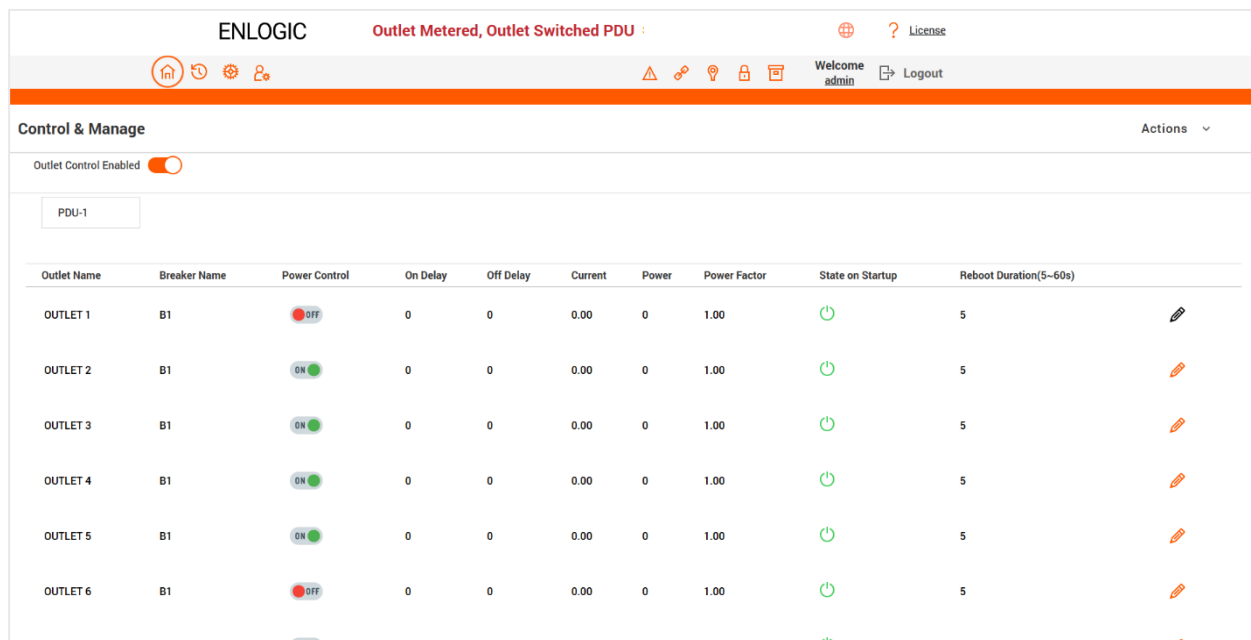
Name	-
Cable Location	-
Cable ID Position	-
Model	200-240V, 40A, 14.4kVA, 50/60Hz
Part Number	EM9591
Serial Number	
Boot Version	1.3
Web Version	3.0.6
Firmware Version	3.2.4.D
Hardware Version	
PDU Power Rating (VA)	14.4
PDU Input Rating (A)	40
PDU Breaker Rating (A)	20

External Sensors	Sensor Name	Serial Number	Sensor ID	PDU	Location
Temperature	TEMP1_PDU1	AWELK0247	1	PDU#1	
Temperature	TEMP2_PDU1	AWELK0247	2	PDU#1	
Temperature	TEMP3_PDU1	AWELK0247	3	PDU#1	
Humidity	HUM1_PDU1	AWELK0247	4	PDU#1	
Smoke	MLC_PDU1	NI1250043	5	PDU#1	Hot Aisle
Door	DOORSWITCH_PDU1	NI1250043	6	PDU#1	Hot Aisle
Humidity	HUM2_PDU1	NI1250043	7	PDU#1	Hot Aisle
Temperature	TEMP4_PDU1	NI1250043	8	PDU#1	Hot Aisle

CONTROL AND MANAGE

In this page, the user can view and control the **Power Outlets & Circuit Breakers** of the PDUs. On this page information about the Outlets belonging to each CB are displayed together.

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.

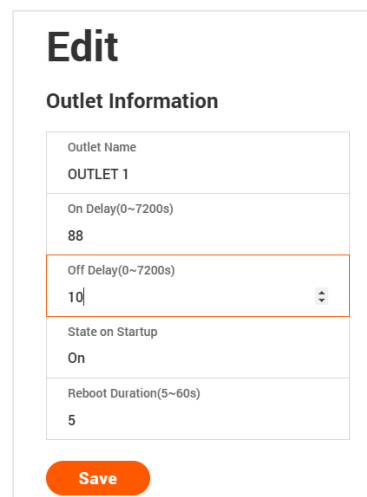


The screenshot shows the ENLOGIC 'Control & Manage' interface. At the top, there's a navigation bar with 'ENLOGIC', 'Outlet Metered, Outlet Switched PDU', and a 'License' link. Below that, a secondary bar contains navigation icons and 'Welcome admin' with a 'Logout' button. The main section is titled 'Control & Manage' and features a toggle for 'Outlet Control Enabled' which is currently turned on. A dropdown menu shows 'PDU-1'. Below this is a table with columns: Outlet Name, Breaker Name, Power Control, On Delay, Off Delay, Current, Power, Power Factor, State on Startup, and Reboot Duration(5-60s). The table lists six outlets (OUTLET 1 to OUTLET 6) all associated with breaker 'B1'. OUTLET 1 and OUTLET 6 are in an 'OFF' state, while the others are 'ON'. Each row has an edit icon in the final column.

Outlet Name	Breaker Name	Power Control	On Delay	Off Delay	Current	Power	Power Factor	State on Startup	Reboot Duration(5-60s)
OUTLET 1	B1	OFF	0	0	0.00	0	1.00	🔌	5
OUTLET 2	B1	ON	0	0	0.00	0	1.00	🔌	5
OUTLET 3	B1	ON	0	0	0.00	0	1.00	🔌	5
OUTLET 4	B1	ON	0	0	0.00	0	1.00	🔌	5
OUTLET 5	B1	ON	0	0	0.00	0	1.00	🔌	5
OUTLET 6	B1	OFF	0	0	0.00	0	1.00	🔌	5

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)



The screenshot shows the 'Edit Outlet Information' form. It has a title 'Edit' and a subtitle 'Outlet Information'. The form contains several input fields: 'Outlet Name' with the value 'OUTLET 1', 'On Delay(0~7200s)' with the value '88', 'Off Delay(0~7200s)' with the value '10', 'State on Startup' with the value 'On', and 'Reboot Duration(5~60s)' with the value '5'. A red 'Save' button is located at the bottom of the form.

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

This step will Reset Total energy values to zero for CB and Phase for that PDU in all interfaces.

The screenshot shows the ENLOGIC interface for 'Outlet Metered, Outlet Switched PDU'. The top navigation bar includes 'ENLOGIC', 'Outlet Metered, Outlet Switched PDU', a globe icon, a 'License' link, and a 'Welcome admin' message with a 'Logout' button. Below the navigation bar, there are icons for home, refresh, settings, and user profile. The main section is titled 'Control & Manage' and features a toggle for 'Outlet Control Enabled' which is currently turned on. A dropdown menu labeled 'Actions' is open, showing 'Reset PDU Energy' and 'Edit Breaker' options. Below this, a table lists six outlets with their respective breaker names, power control status, delays, current, power, power factor, state on startup, and reboot duration.

Outlet Name	Breaker Name	Power Control	On Delay	Off Delay	Current	Power	Power Factor	State on Startup	Reboot Duration(5-60s)
OUTLET 1	B1	OFF	0	0	0.00	0	1.00	🔌	5
OUTLET 2	B1	ON	0	0	0.00	0	1.00	🔌	5
OUTLET 3	B1	ON	0	0	0.00	0	1.00	🔌	5
OUTLET 4	B1	ON	0	0	0.00	0	1.00	🔌	5
OUTLET 5	B1	ON	0	0	0.00	0	1.00	🔌	5
OUTLET 6	B1	OFF	0	0	0.00	0	1.00	🔌	5

To Edit Breaker names, Click on the Edit Breaker option from the drop-down menu.

This screenshot is identical to the previous one, but the 'Edit Breaker' option in the 'Actions' dropdown menu is highlighted, indicating it has been selected.

The 'Edit' form is titled 'Edit Breakers Name' and contains a list of input fields for Breaker#1 through Breaker#6. Each field currently contains the value 'B1'. A 'Save' button is located at the bottom of the form.

Breaker Name
Breaker#1 B1
Breaker#2 B2
Breaker#3 B3
Breaker#4 B4
Breaker#5 B5
Breaker#6 B6

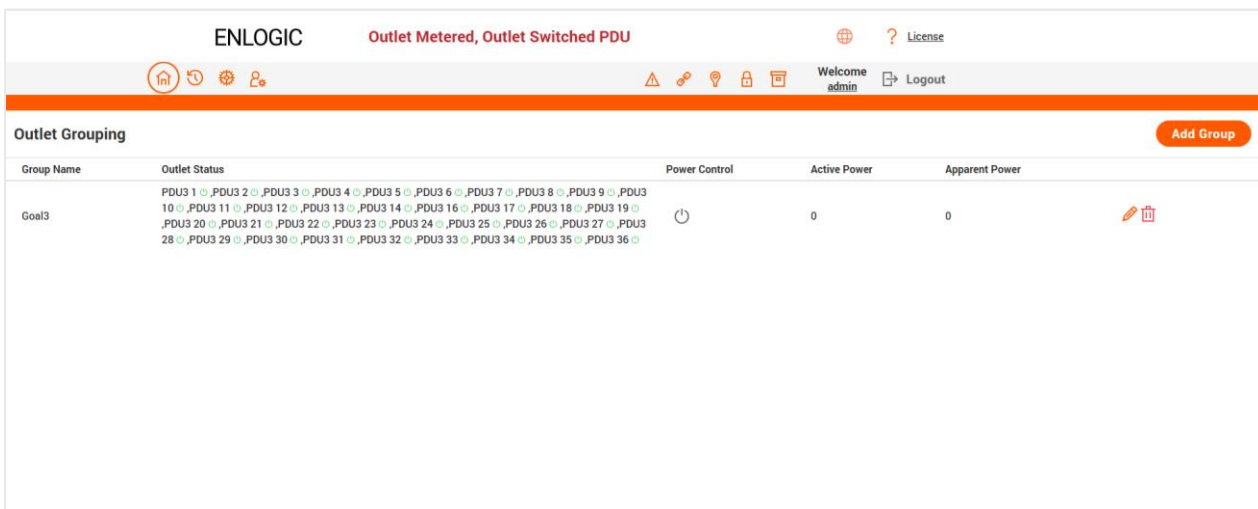
Save

OUTLET GROUPING

Outlet grouping makes it simple for the user to group the outlets of interest from any of the PDUs in the daisy chain configuration, monitor, and control the entire group. Control involves turning on, off, and rebooting the outlets without delays.

Note : Users can create a maximum number of 64 outlet groups. The maximum number of outlets in each group also are set to 64.

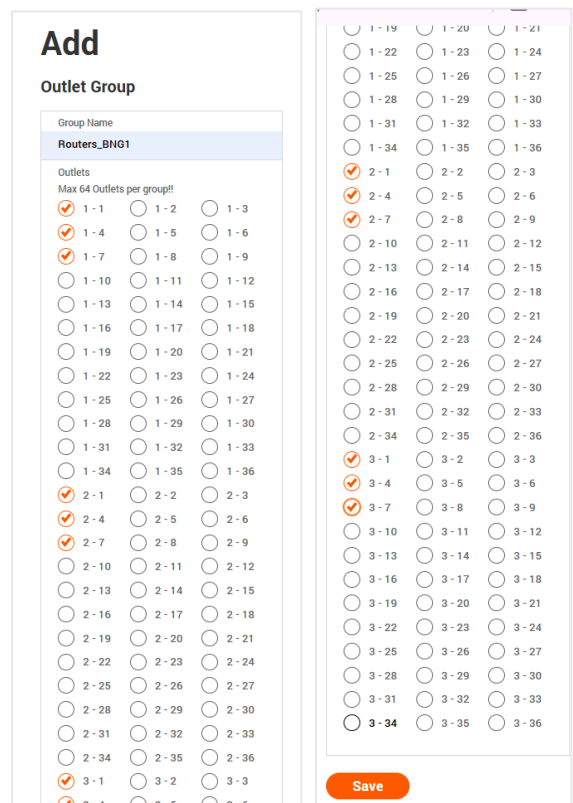
1. Click on the Home icon to dropdown the Home menu.
2. Select Outlet Grouping.



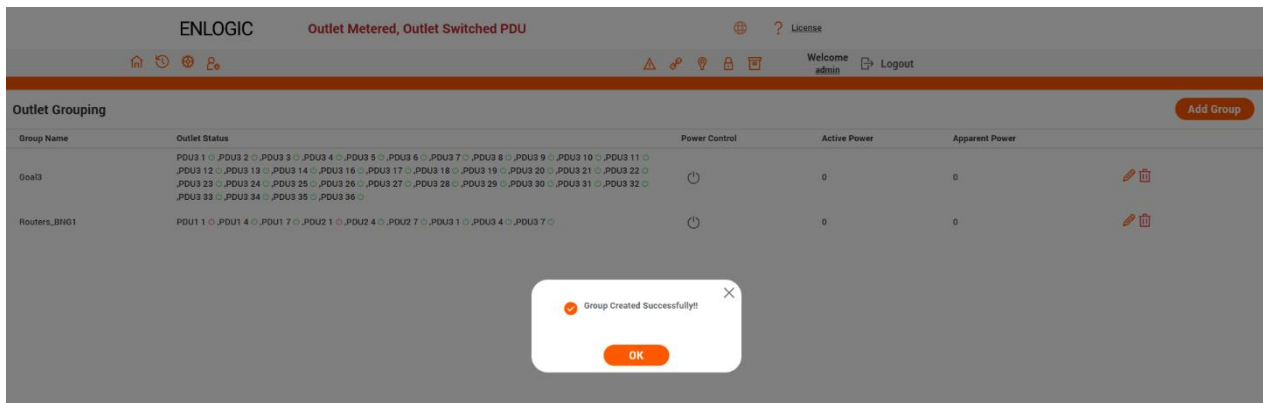
3. To start grouping outlets. Click on Add Group button.
4. Select the **Outlets** to be grouped. Click on the corresponding radio button and select the outlets. Scroll down if the outlets needs to be selected from all/any PDU in the daisy chain setup.
5. The syntax of the items listed is: **PDU_ID – Outlet index**.
Example 1: 1-16 represents outlet index 16 of 1st PDU in the daisy chain.

Example 2: 4-32 represents outlet index 32 of 4th PDU in the daisy chain.

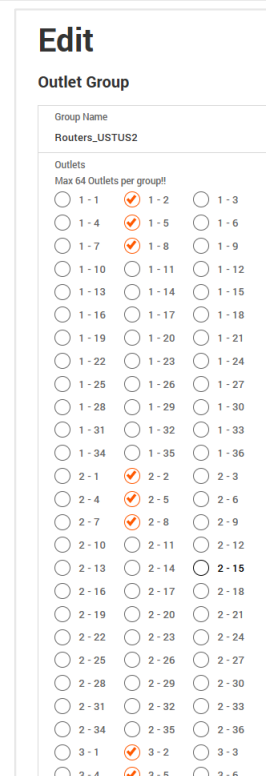
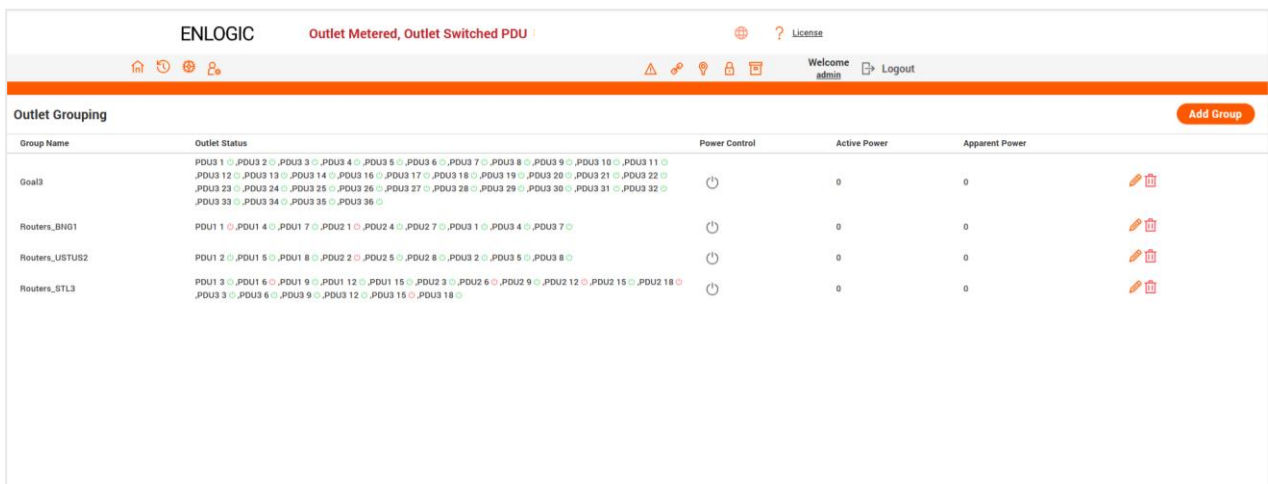
6. Click Save.



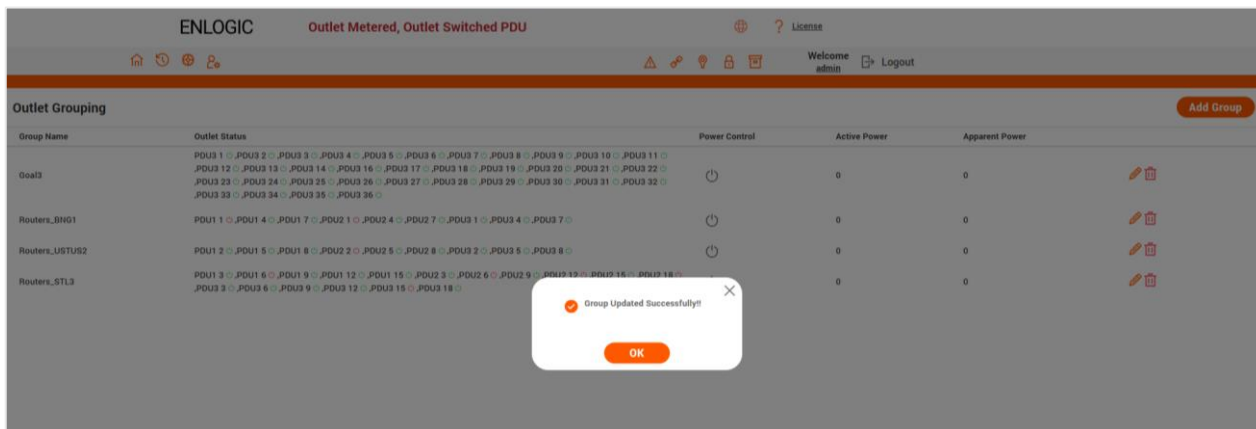
7. The Outlet Groups are created successfully.



8. To edit the Outlet Group, click on the  icon. Add or modify the group information. Click Save.



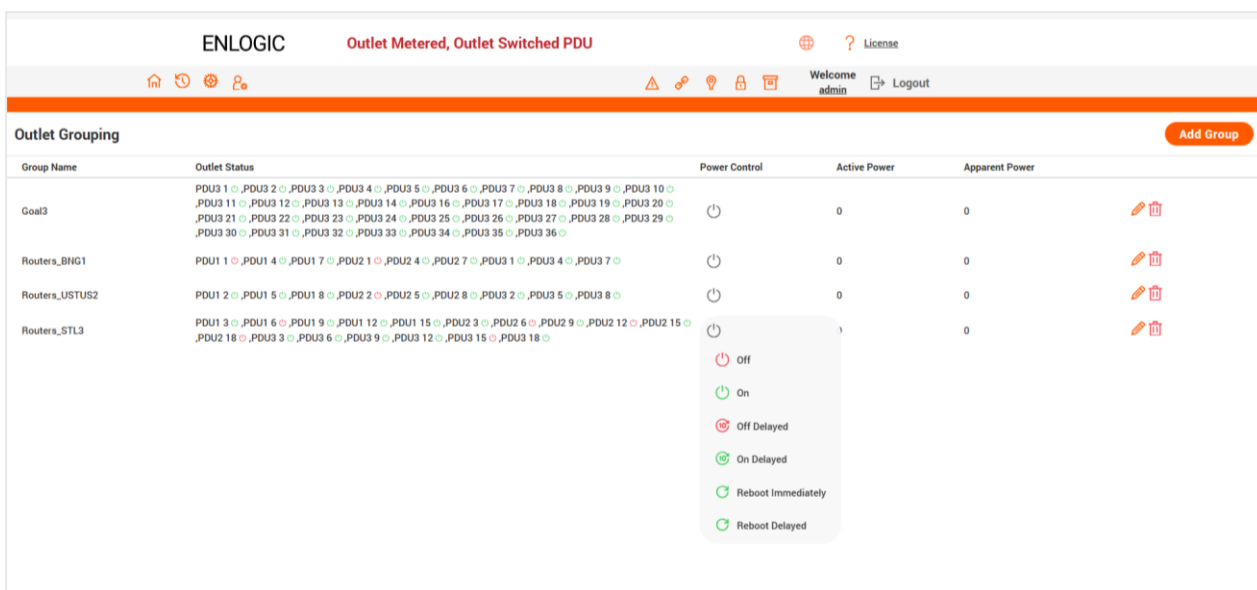
9. Click Save. The Group is updated successfully.



10. Click on the  icon to delete any group. Click Delete and the group is deleted.

11. For every outlet group, a set of Power Control options can be executed as shown in the image below. Click the options in the drop down menu and the action will be completed successfully.

Note - Active Power and Apparent Power columns display the respective values across each group created. The power values are computed by summing up the power associated with each of the outlets in the group.



OUTLET GROUPING USING SNMP INTERFACE

To add a new Group:

12. Access the pduOutletGroupSwitchedNames OID, click on Value field, click SET option and then type the group name of the new group.
13. Access the pduOutletGroupMemberID OID associated with the PDU ID that contains the outlets that need to be selected. Then, click the value field, select SET, and type in the outlet IDs that need to be grouped.
14. For each PDU ID from which an outlet needs to be added to the group, repeat STEP 2 again.
15. Note: For adding a group successfully, at least one sub-OID of the pduOutletGroupMemberID OID and pduOutletGroupSwitchedNames must be SET. After a group has been successfully formed, pduOutletGroupSwitchedCount gets incremented. The group count will not be increased and the group addition will be deemed unsuccessful if any of the aforementioned OIDs are not set.

To modify a Group:

- Group names and PDU/outlet IDs can be edited. The user can change all or some of the outlets that correspond to certain PDU IDs, provided that the total number of outlets in a group does not exceed 64 numbers. The group count is unaffected when group information is modified.

To delete a Group:


- There are two methods to go about this.
- Any group name deletion results in the group's total deletion. The group count is decreased by this action.
- A group can also be deleted by removing all values that have previously been set across all pduOutletGroupMemberID sub-OIDs.
- Note: A group cannot be deleted even if one sub-OID of the pduOutletGroupMemberID contains outlet numbers. As a result, all sub-OID data must be cleared.

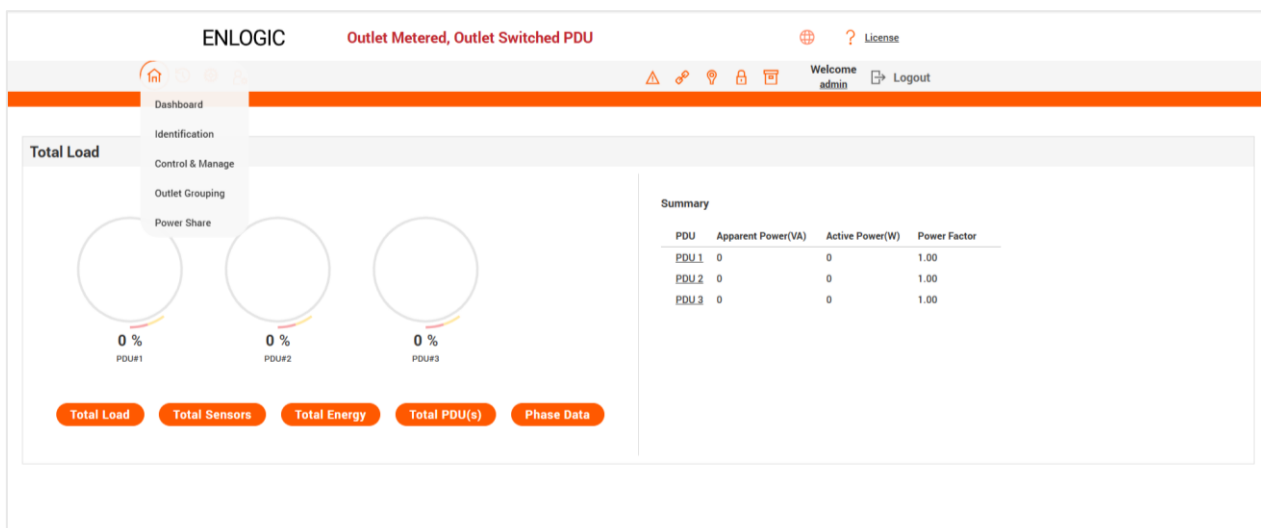
To control Grouped Outlets:

- Click on value field of pduOutletGroupSwitchedControl OID of the corresponding group that needs to be controlled and select the drop down menu to choose one of the 6 options- ON/OFF/REBOOT/ONDELAY/OFFDELAY/REBOOTDELAY.
- Display Active and Apparent Power:
- pduOutletGroupSwitchedActivePower and pduOutletGroupSwitchedApparentPower OIDs return the power values of corresponding outlet group to be monitored.

POWER SHARE

In this page, the user can view and control the Power Share details of the PDUs.

- Click on the Home icon to dropdown the Home menu
- Select Power Share.
- Click on the  icon.



27. Enable the Power Share feature for specific PDU. Click Save.

The screenshot shows the ENLOGIC web interface for an "Outlet Metered, Outlet Switched PDU". The page title is "Power Share" and the sub-header is "PDUs 1-3". The interface is divided into three columns, one for each PDU (PDU #1, PDU #2, and PDU #3). Each column contains the following settings:

Setting	PDU #1	PDU #2	PDU #3
Power Share	✓	✓	✓
Power Supply Mode	Main Power	Main Power	Main Power
Power Share Output	ON	ON	ON
Backup Protection	ON	ON	ON

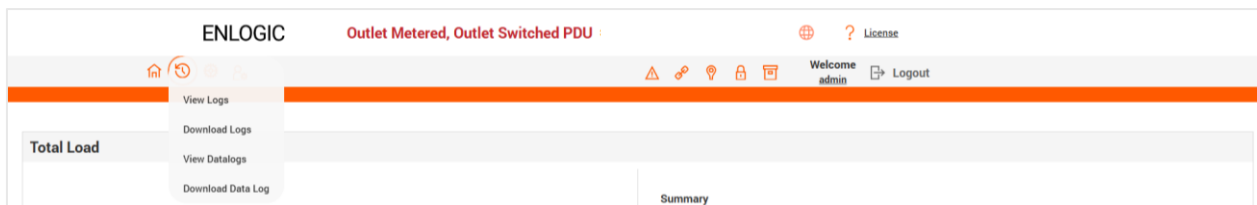
The "Power Share" status is indicated by a checkmark (✓) in each column. The "Power Share Output" and "Backup Protection" settings are indicated by green "ON" buttons with a power symbol.

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.



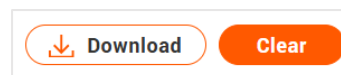
Click on the **System Administration** icon to dropdown the menu.

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

The screenshot shows the 'View Logs' page in the ENLOGIC interface. At the top right, there are 'Download' and 'Clear' buttons. Below is a table with three columns: 'Type', 'Description', and 'Date & Time'.

Type	Description	Date & Time
Audit Log	User admin of PDU 1 from host 10.20.14.239 logged in	2010/01/01, 06:34:34
Audit Log	User admin of PDU 1 from host 10.20.14.239 time out	2010/01/01, 06:13:40
Configuration Log	OutletGroup configuration of Routers_USTUS2 is changed	2010/01/01, 06:01:30
Configuration Log	OutletGroup configuration is changed to Routers_STL3	2010/01/01, 06:00:18
Configuration Log	OutletGroup configuration is changed to Routers_USTUS2	2010/01/01, 05:59:46
Configuration Log	OutletGroup configuration is changed to Routers_BNG1	2010/01/01, 05:59:03
Audit Log	User admin of PDU 1 from host 10.20.14.239 logged in	2010/01/01, 05:41:26
Audit Log	User admin of PDU 1 from host 10.20.14.239 time out	2010/01/01, 05:25:12
Audit Log	User admin of PDU 1 from host 10.20.14.239 logged in	2010/01/01, 05:03:20
Audit Log	User admin of PDU 1 from host 10.20.14.239 time out	2010/01/01, 04:54:12
Audit Log	User admin of PDU 1 from host 10.20.14.239 time out	2010/01/01, 04:46:35
Configuration Log	TemperatureScale configuration is changed to CELSIUS from	2010/01/01, 04:42:11
Configuration Log	TemperatureScale configuration is changed to CELSIUS from CELSIUS	2010/01/01, 04:42:00
Audit Log	User admin of PDU 1 from host 10.20.14.239 logged in	2010/01/01, 04:40:35
Audit Log	User admin of PDU 1 from host 10.20.14.239 logged in	2010/01/01, 04:36:17
Audit Log	User admin of PDU 1 from host 10.20.14.254 logged out	2010/01/01, 04:35:49
Audit Log	User admin of PDU 1 from host 10.20.14.254 logged in	2010/01/01, 04:35:39
Event Log	Loss on Relay 3, 5, of PDU 3 occurred	2010/01/01, 02:52:58
Event Log	Upstream power of PDU 2 cleared lost warning	2010/01/01, 02:52:42
Event Log	Power share output of PDU 2 enable	2010/01/01, 02:52:42
Event Log	Main power of PDU 2 cleared failure alarm,switched main power supply	2010/01/01, 02:52:42
Event Log	Upstream power of PDU 2 is lost	2010/01/01, 02:52:38

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.

The screenshot shows the ENLOGIC interface for 'Outlet Metered, Outlet Switched PDU'. The 'View Logs' section contains a table with the following data:

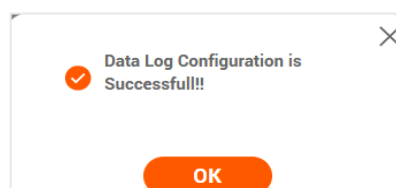
Type	Description	Date & Time
Audit Log	User admin of PDU 1 from host 10.20.14.239 logged in	2010/01/01, 06:34:34
Audit Log	User admin of PDU 1 from host 10.20.14.239 time out	2010/01/01, 06:13:40
Configuration Log	OutletGroup configuration of Routers_USTUS2 is changed	2010/01/01, 06:01:30
Configuration Log	OutletGroup configuration is changed to Routers_STL3	2010/01/01, 06:00:18
Configuration Log	OutletGroup configuration is changed to Routers_USTUS2	2010/01/01, 05:59:46
Configuration Log	OutletGroup configuration is changed to Routers_BNG1	2010/01/01, 05:59:03
Audit Log	User admin of PDU 1 from host 10.20.14.239 logged in	2010/01/01, 05:41:26
Audit Log	User admin of PDU 1 from host 10.20.14.239 time out	2010/01/01, 05:25:12
Audit Log	User admin of PDU 1 from host 10.20.14.239 logged in	2010/01/01, 05:03:20
Audit Log	User admin of PDU 1 from host 10.20.14.239 time out	2010/01/01, 04:54:12
Audit Log	User admin of PDU 1 from host 10.20.14.239 time out	2010/01/01, 04:46:35
Configuration Log	TemperatureScale configuration is changed to CELSIUS	2010/01/01, 04:42:11
Configuration Log	TemperatureScale configuration is changed to CELSIUS from CELSIUS	2010/01/01, 04:42:00
Audit Log	User admin of PDU 1 from host 10.20.14.239 logged in	2010/01/01, 04:40:35
Audit Log	User admin of PDU 1 from host 10.20.14.239 logged in	2010/01/01, 04:26:17
Audit Log	User admin of PDU 1 from host 10.20.14.254 logged out	2010/01/01, 04:35:49
Audit Log	User admin of PDU 1 from host 10.20.14.254 logged in	2010/01/01, 04:35:39
Event Log	Loss on Relay 3, 5, of PDU 3 occurred	2010/01/01, 02:52:58
Event Log	Upstream power of PDU 2 cleared lost warning	2010/01/01, 02:52:42
Event Log	Power share output of PDU 2 enable	2010/01/01, 02:52:42
Event Log	Main power of PDU 2 cleared failure alarm,switched main power supply	2010/01/01, 02:52:42
Event Log	Upstream power of PDU 2 is lost	2010/01/01, 02:52:38

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. Click Save.
- **Download Data Log**: to download the data logs
- **Clear Data Log**: to delete/clear the logs.

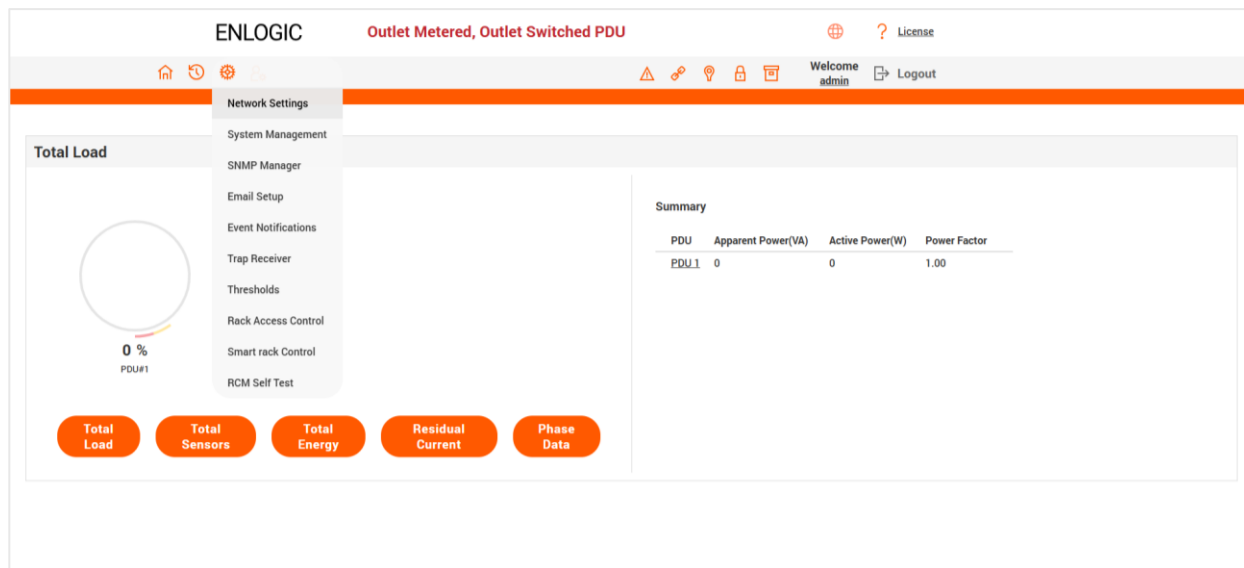
The 'Edit Data Log Configuration' dialog box includes the following elements:

- Edit** (Section Header)
- Data Log Configuration** (Section Header)
- Enable** (Toggle switch, currently turned on)
- Log Interval(1-1440 Minutes)** (Input field with value 25)
- Save** (Button)



SETTINGS

Click on settings icon allows the user to setup the Network Settings, System Management, SNMP Manager, Email Setup, Event Notifications, Trap Receiver, Thresholds, Rack Access Control, Smart Rack Control and RCM Self Test .



NETWORK SETTINGS

This page allows the management of IP Configuration, Web Configuration, RESTapi Configuration, DNS Configuration, SSH/FTP's 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.

ENLOGIC Outlet Metered, Outlet Switched PDU

Welcome admin Logout

Network Settings

Set Certificate Key Change Link Speed Syslog Configuration Syslog Setting

Ethernet-0 IP Configuration		Ethernet-1 IP Configuration		Domain Name System	
Network Mode	IPv4/IPv6	Network Mode	IPv4/IPv6	Manually Override Servers	×
Boot Mode IPv4	DHCP	Boot Mode IPv4	DHCP	Primary DNS Server	0.0.0.0
Boot Mode IPv6	Autoconfig	Boot Mode IPv6	Autoconfig	Secondary DNS Server	0.0.0.0
IPv4 Address	10.20.15.62	IPv4 Address	0.0.0.0	Edit HostName/Domain	×
Network Mask	255.255.255.128	Network Mask	0.0.0.0	Host Name	
Default Gateway	10.20.15.1	Default Gateway	0.0.0.0	Domain Name(IPv4/IPv6)	
IPv6 Link Local Address	fe80::6492:1d9d:4e33:7a99	IPv6 Link Local Address			
IPv6 Global Configured Address	2001::1111:1111:1121:debe:84c6:9887:772f	IPv6 Global Configured Address			
LLDP	×	LLDP	×		
Authentication	NO Authentication	Authentication	NO Authentication		

Web/RESTapi Access Configuration		SSH/FTPs Configuration	
Web Access	http&https	SSH Access	✓
Web Port	80/443	SSH Port	22
Redirection	✓	FTPs Access	✓
RESTapi Access	×	FTPs Port	21
Certificate	View Certificate	Telnet Access	×
		Telnet Port	23

Network Time Protocol(NTP)		Date/Time Settings		Daylight Saving Time	
Enable	×	Date	2024/12/10	Enable	×
Primary NTP Server	0.0.0.0	Time	14:47:44	Start Month	{ } { } {00}
Secondary NTP Server	0.0.0.0	Date Format	YYYY/MM/DD	End Month	{ } { } {00}

802.1x Authentication

802.1X is an authentication protocol that ensures secure network access through an ethernet port. With the release of FW 3.2.4, the iPDU's now integrate IEEE 802.1X authentication, which is disabled by default. This protocol can be configured independently on each LAN port to provide secure access for the iPDU. It verifies an ethernet port's identity using credentials or certificates. The 802.1X protocol uses the certificate uploaded from the Certificate Repository to authenticate the user. The iPDU supports EAP-TLS, PEAP-TLS, and PEAP-MSCHAPv2 as authentication methods.

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

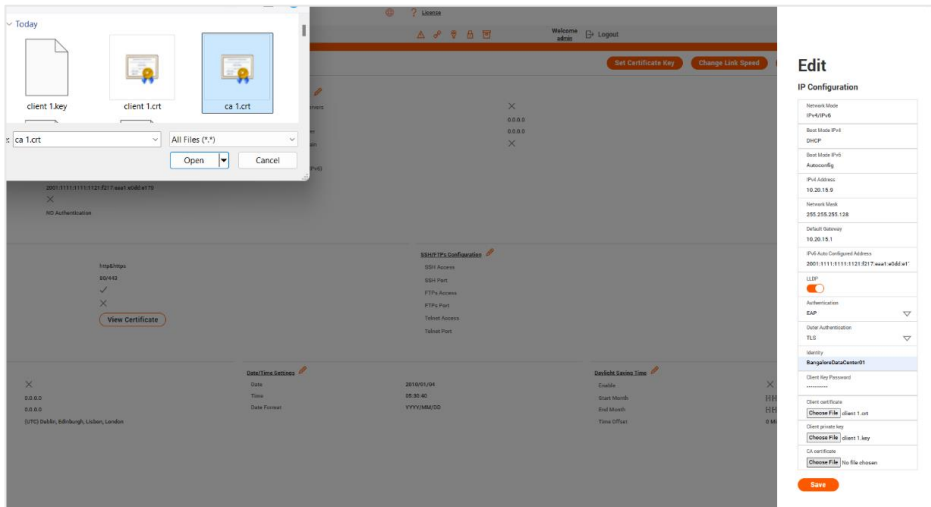
- Network Mode
- Boot Mode
- Boot Mode Ipv6
- IPv4 Address
- Network Mask
- Default Gateway
- IPv6 Auto Configured Address
- LLDP
- Authentication
 - EAP
 - No Authentication

Edit

IP Configuration

Network Mode	IPv4/IPv6
Boot Mode IPv4	DHCP
Boot Mode IPv6	Autoconfig
IPv4 Address	10.20.15.62
Network Mask	255.255.255.128
Default Gateway	10.20.15.1
IPv6 Auto Configured Address	2001::1111:1111:1121:debe:84c6:9887:77
LLDP	<input checked="" type="checkbox"/>
Authentication	No Authentication ▼
EAP	<input type="checkbox"/>
No Authentication	<input checked="" type="checkbox"/>

- Select Authentication type as **EAP**
- Two types of Outer Authentication **TLS** or **PEAP**.
- Select TLS and Upload the Client Certificate, Client Private Key and CA certificate for authentication.
- Update the Identity and Client Key Passphrase.



Edit

IP Configuration

Network Mode	IPv4/IPv6
Boot Mode IPv4	DHCP
Boot Mode IPv6	Autoconfig
IPv4 Address	10.20.15.62
Network Mask	255.255.255.128
Default Gateway	10.20.15.1
IPv6 Auto Configured Address	2001:1111:1111:1121:debe:84c6:9887:77
LLDP	<input checked="" type="checkbox"/>
Authentication	EAP
Outer Authentication	TLS
Client Key Password	
Client certificate	<input type="button" value="Choose File"/> No file chosen
Client private key	<input type="button" value="Choose File"/> No file chosen
CA certificate	<input type="button" value="Choose File"/> No file chosen

- Click Save
- In the confirmation screen, approve the change.
- Click Apply.

Confirmation

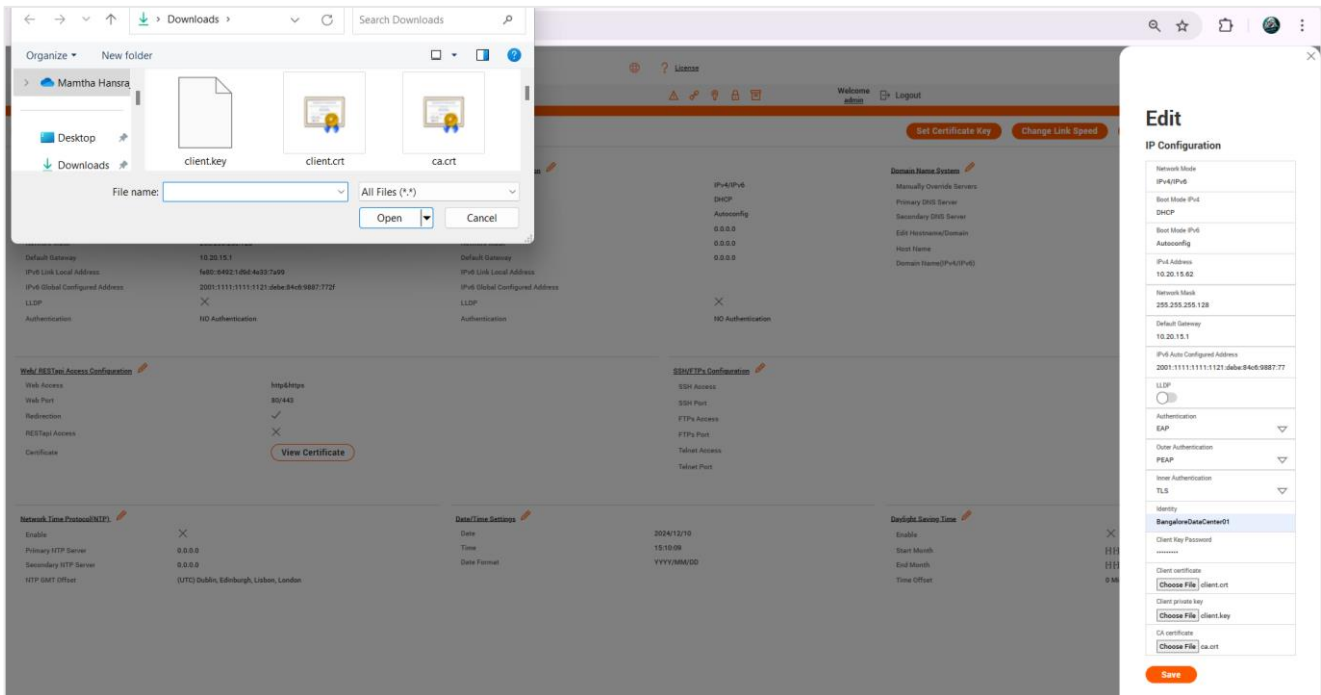
After changing the setting, you will need to reset the Network Card to take effect.

Do you really want to apply changes now?

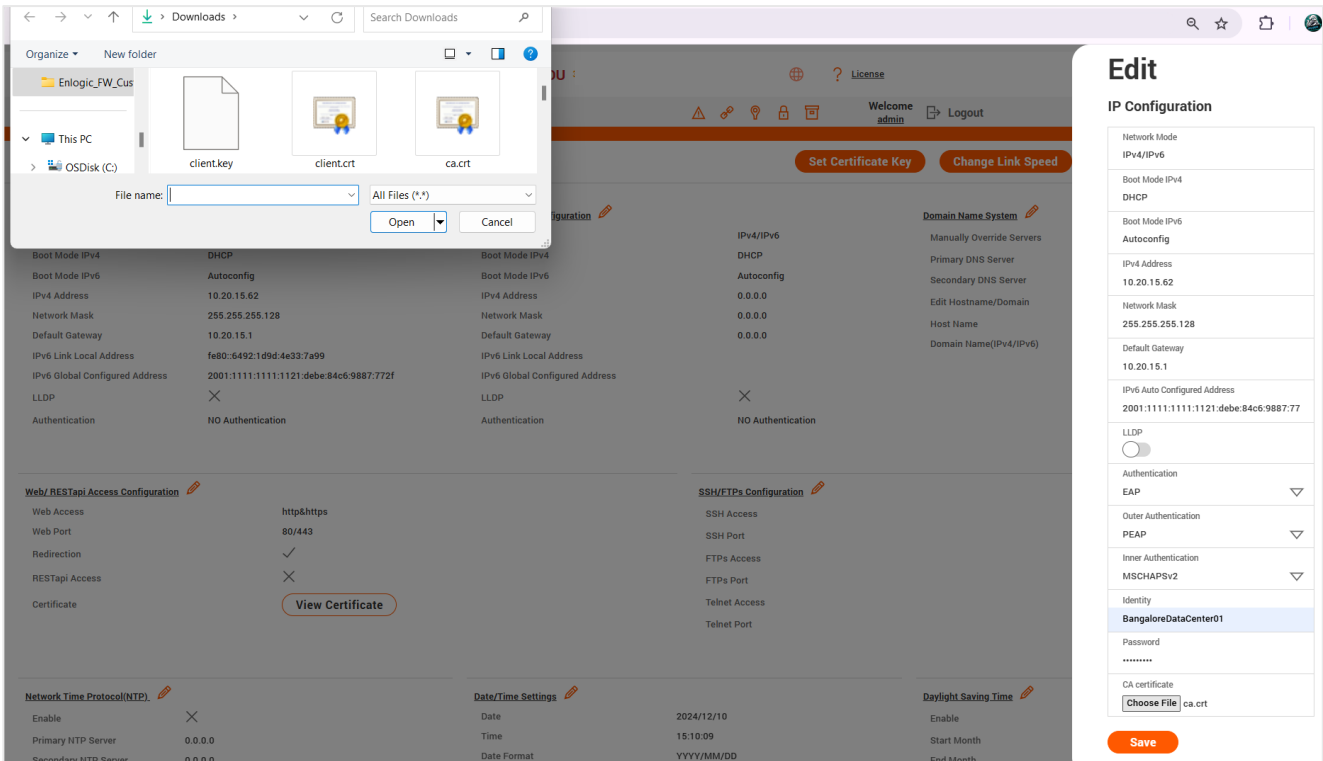
The Network Card will be reset in a few seconds. You will be redirected to the login page within 25 seconds. If redirection does not work, use this link to the login page.

[Click Here](#)

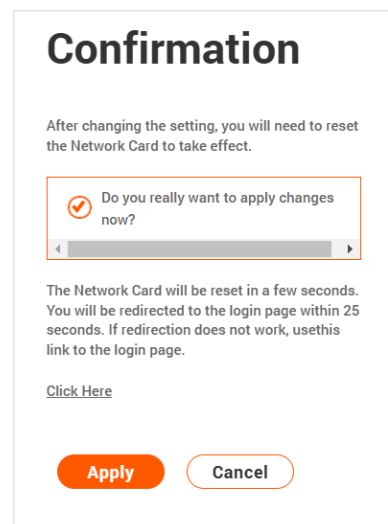
- Select Authentication type as **EAP**.
- Two types of Outer Authentication **TLS or PEAP**.
- Select **PEAP**.
- Select **TLS or MSCHAPScv2** as the Inner Authentication.
- Select TLS and Upload the Client Certificate, Client Private Key and CA certificate for authentication.
- Update the **Identity**.
- Update **Client Key Paraphrase** if required.



- Select PEAP.
- Select MSCHAPScv2 as the Inner Authentication.
- Update the CA certificate for authentication.
- Update the Identity and Password are mandatory.



- Click Save.
- In the confirmation screen, approve the change.
- Click Apply.



WEB/RESTAPI ACCESS CONFIGURATION

1. By default, accessing the PDU uses HTTPS port setting.
2. Click the icon to edit/change the **Web/RESTapi Access Configuration** information below:
3. Web Access (HTTP or HTTPS)
4. **HTTP Port** (Default 80 for HTTP)
5. **HTTPS Port** (443 for HTTPS)
6. Toggle ON/OFF the Redirection to enable HTTP to HTTPS **Redirection**
7. Enable RESTapi Access
8. To access the HTTPS settings, upload the **SSL Certificate** and **SSL Certificate Key** provided by Enlogic
9. Click **Save** button to complete the settings.


Edit

Web/ RESTapi Access Configuration

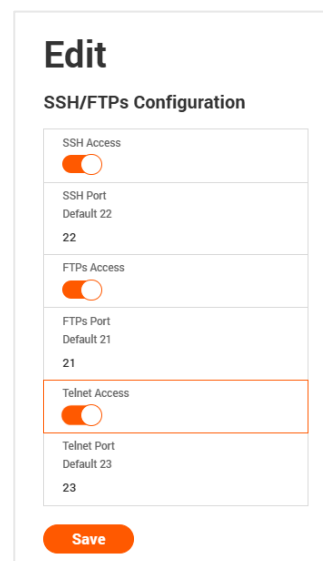
Web Access
Http & Https
HTTP Port Default 80 for Http 80
HTTPS Port Default 443 for Https 443
Redirection <input checked="" type="checkbox"/>
RESTapi Access Disable
Disable
Enable
SSL Certificate <input type="button" value="Choose File"/> No file chosen
SSL Certificate Key <input type="button" value="Choose File"/> No file chosen

SSH/FTPS CONFIGURATION

Edit the SSH/FTPS configuration Settings information below:

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


1. Enable SSH Access.
2. **SSH Port** (Default 22).
3. Enable FTPs Access.
4. **FTPs Port** (Default 21).
5. Enable Telnet Access.
6. Telnet Port (Default 23).
7. Click Save button to complete the settings.



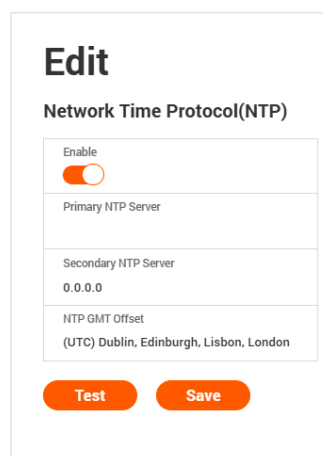
The screenshot shows the 'Edit SSH/FTPs Configuration' form. It contains four sections, each with a toggle switch and a port number: 'SSH Access' (checked, 22), 'FTPs Access' (checked, 21), 'Telnet Access' (checked, 23), and 'Telnet Port' (23). A 'Save' button is at the bottom.

NETWORK TIME PROTOCOL (NTP)

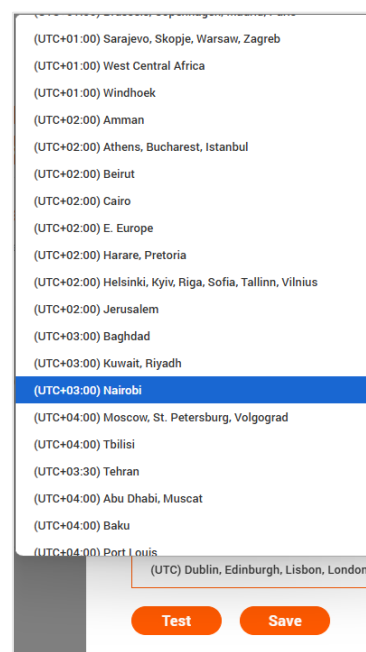
You can link the PDU to a Network Time Protocol (NTP) server and let it set the date and time.

Click the  icon to edit/change the NTP Setting information below:

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



The screenshot shows the 'Edit Network Time Protocol(NTP)' form. It includes an 'Enable' toggle (checked), a 'Primary NTP Server' field, a 'Secondary NTP Server' field with the value '0.0.0.0', and an 'NTP GMT Offset' dropdown menu showing '(UTC) Dublin, Edinburgh, Lisbon, London'. 'Test' and 'Save' buttons are at the bottom.



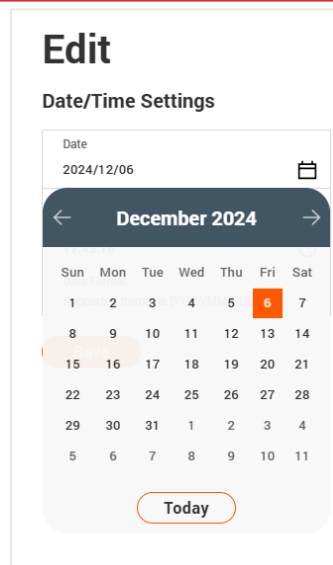
The screenshot shows a list of NTP GMT Offset options. The options are: (UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb; (UTC+01:00) West Central Africa; (UTC+01:00) Windhoek; (UTC+02:00) Amman; (UTC+02:00) Athens, Bucharest, Istanbul; (UTC+02:00) Beirut; (UTC+02:00) Cairo; (UTC+02:00) E. Europe; (UTC+02:00) Harare, Pretoria; (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius; (UTC+02:00) Jerusalem; (UTC+03:00) Baghdad; (UTC+03:00) Kuwait, Riyadh; (UTC+03:00) Nairobi (highlighted in blue); (UTC+04:00) Moscow, St. Petersburg, Volgograd; (UTC+04:00) Tbilisi; (UTC+03:30) Tehran; (UTC+04:00) Abu Dhabi, Muscat; (UTC+04:00) Baku; (UTC+04:00) Port Louis; (UTC) Dublin, Edinburgh, Lisbon, London. 'Test' and 'Save' buttons are at the bottom.

DATE/TIME SETTING

You can manually set the internal clock on the PDU.

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

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



Edit

Date/Time Settings

Date
2024/12/06

December 2024

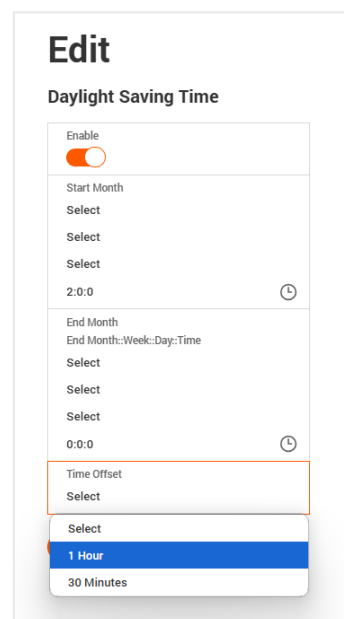
Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

Today

DAYLIGHT-SAVING TIME

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

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



Edit

Daylight Saving Time

Enable

Start Month
Select

Select

Select

2:0:0

End Month
End Month::Week::Day::Time
Select

Select

Select

0:0:0

Time Offset
Select

Select

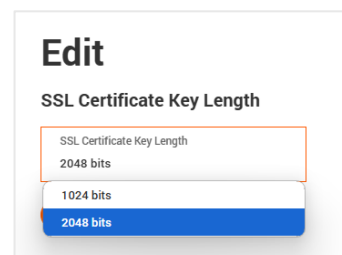
1 Hour

30 Minutes

6. 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.

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



Edit

SSL Certificate Key Length

SSL Certificate Key Length
2048 bits

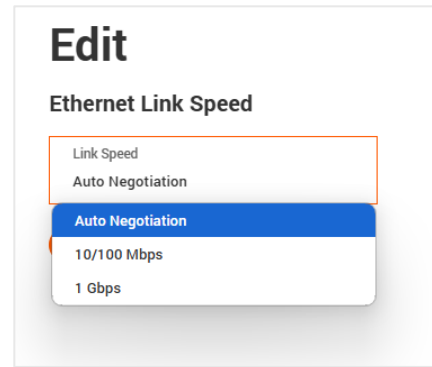
1024 bits

2048 bits

Change Link Speed

Below are the steps to change the Ethernet link speed.

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



Edit

Ethernet Link Speed

Link Speed

Auto Negotiation

Auto Negotiation

10/100 Mbps

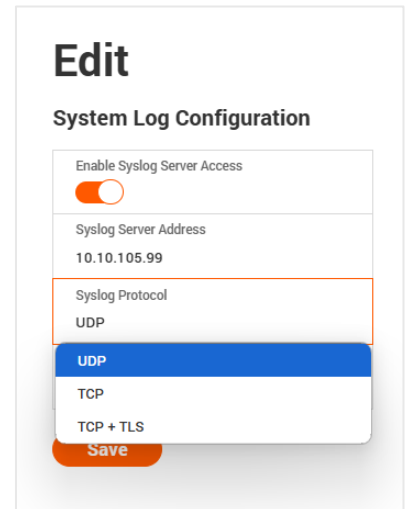
1 Gbps

SYSLOG CONFIGURATION

In relation to cybersecurity incidents, Office of Management and Budget (OMB) Syslog requires an Implementation where syslog's are required and must adhere to the M-21-31 memorandum requirements specified by the Federal Government's Investigative and Remediation Capabilities. This memorandum outlines the logs that agencies need to keep and maintain for necessary retention periods.

Below are the steps to configure the Syslog.

1. Click Syslog Configuration button.
2. Enable the Enable Syslog Server Access.
3. Type the Syslog Server Address.
4. Select the Syslog Protocol from the dropdown menu >> UDP /TCP /TCP+TLS.
5. If selecting TCP+TLS option, upload a valid TLS certificate.
6. Select Syslog Server Port number.
7. Click Save button to complete setting.



Edit

System Log Configuration

Enable Syslog Server Access

Syslog Server Address

10.10.105.99

Syslog Protocol

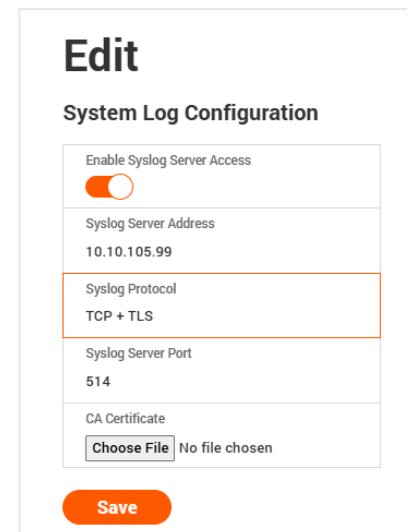
UDP

UDP

TCP

TCP + TLS

Save



Edit

System Log Configuration

Enable Syslog Server Access

Syslog Server Address

10.10.105.99

Syslog Protocol

TCP + TLS

Syslog Server Port

514

CA Certificate

Choose File No file chosen

Save

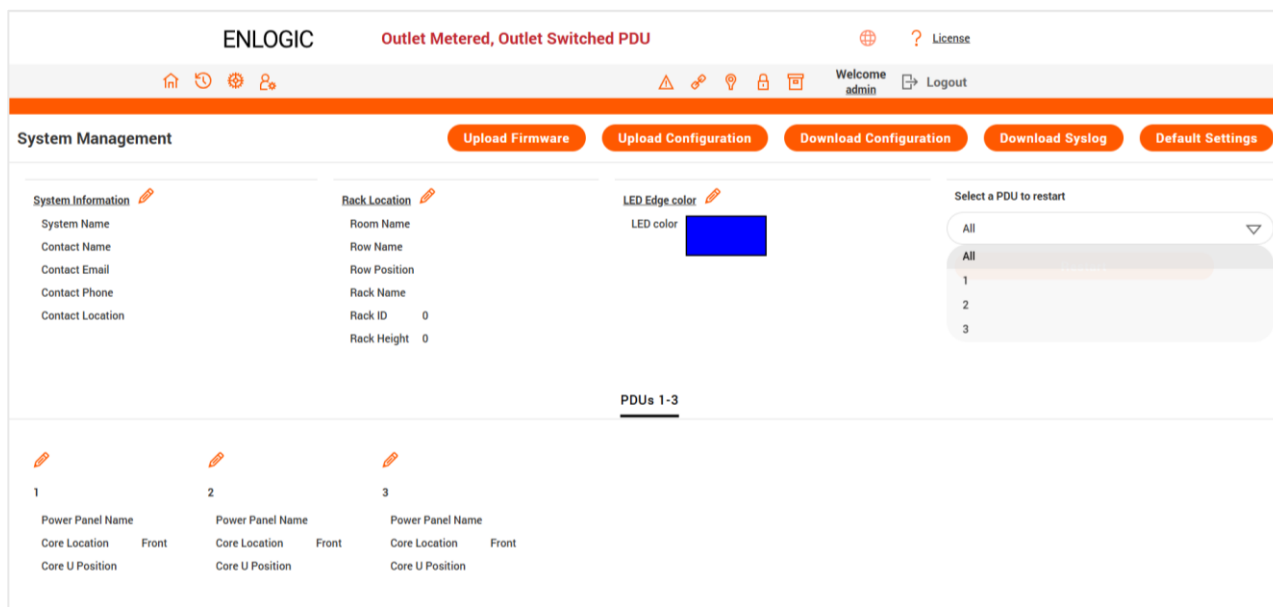
The admin can retrieve these logs from the syslog server, which provides information about events, but are not limited to the following fields:

1. User Sessions.
2. Login attempt with result on any interface (do not log passwords).
3. Logoff on any interface.
4. Session timeout on any interface.
5. Configuration Change - Any configuration change through any interface.
6. Any state change/ control operation on any interface Includes outlet control.
7. Any user or system alarm conditions.
8. Thresholds.
9. Alarms Network Connection Changes or Failures.
10. Other System Alarms.
11. Startup / shutdown events Include FW version.
12. FW Update.
13. Log attempt with new and old version identifiers.
14. Log update failures with reason.
15. Logging Transport Traps Must support notification of any logging failures through SNMP traps.
16. Any failure to connect with syslog collector.
17. Failure to authenticate syslog collector.
18. Failure of device to authenticate with syslog collector.
19. Error during session.
20. Disconnect prior to completion of session.

SYSTEM MANAGEMENT

The features of **uploading firmware, uploading configuration, and downloading configuration** are all available to the user on the Systems Management page. Additionally, the user has the option to reset and set the **Default Settings** of the Master and Node PDUs. The user can also **Restart** both the Master and Node PDUs.

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



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	Bangalore_Data_Center_Manyata
Contact Name	Admin
Contact Email	admin@envent.com
Contact Phone	
Contact Location	Bangalore Manyata

Save


4. Click on the  icon to edit the Rack Location Information below:
5. Enter the **Room Name** to identify the cabinet or room where the PDU is located.
6. Enter the **Row Name** where the PDU is located on the rack.
7. Enter the **Row Position** where the PDU is located on the rack.
8. Enter the **Rack Name** where the PDU is located.
9. Enter the **Rack ID** for identification of rack.
10. Enter the **Rack Height** where the PDU is located on the rack.
11. Click **Save** button to complete setting.

Edit

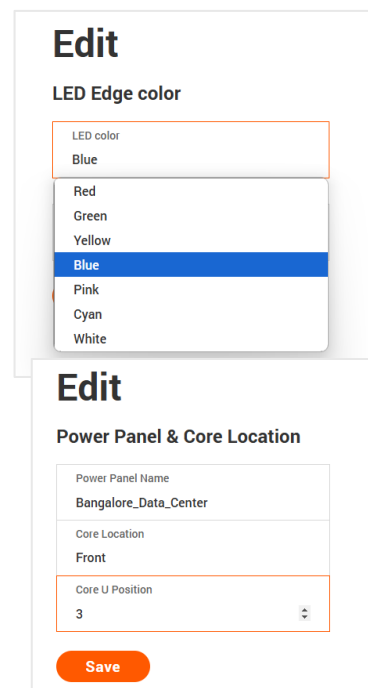
Rack Location

Room Name	Bangalore_Data_Center_Rack10
Row Name	Row_15
Row Position	12:ED
Rack Name	Router
Rack ID	12
Rack Height	0


Save

12. 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.
13. Click the  icon to edit/change the **LED Edge Color** information below:

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



The screenshot shows two stacked configuration panels. The top panel is titled 'Edit' and 'LED Edge color'. It has a text input field containing 'Blue' and a dropdown menu with options: Red, Green, Yellow, Blue (highlighted), Pink, Cyan, and White. The bottom panel is also titled 'Edit' and 'Power Panel & Core Location'. It contains three input fields: 'Power Panel Name' with the value 'Bangalore_Data_Center', 'Core Location' with the value 'Front', and 'Core U Position' with the value '3'. A 'Save' button is located at the bottom right of this panel.

14. 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.




15. Click the buttons on the top right corner of the screen to:
- Upload **Firmware** from a file.
 - Upload **Configuration** from a file.
 - Download **Configuration** file.
 - Download **Syslog**..
 - Reset to **Default Settings**

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.
4. Enable the SNMP General. Click on the  on.
 - Enable the **SNMP**
 - Specify the **SNMP** version
5. Click Save button to complete the settings.
6. To secure the link between the PDU and the MIB Browser.

SNMP General

Enable

SNMP Version
V1/2c&V3

Save

7. Click the  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

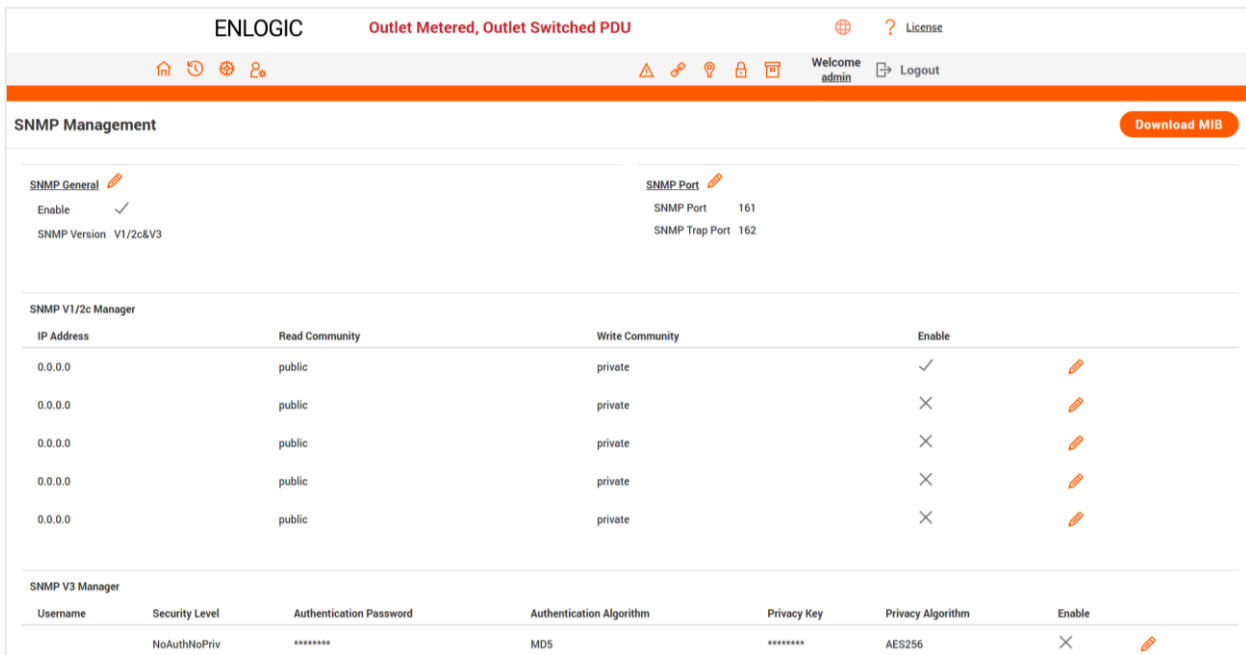
SNMP Port

SNMP Port
161

SNMP Trap Port
162

Save


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




ENLOGIC Outlet Metered, Outlet Switched PDU

Home Refresh Settings Users Alerts Settings Welcome admin Logout

SNMP Management [Download MIB](#)






SNMP General 

Enable
SNMP Version V1/2c&V3


SNMP Port 

SNMP Port 161
SNMP Trap Port 162

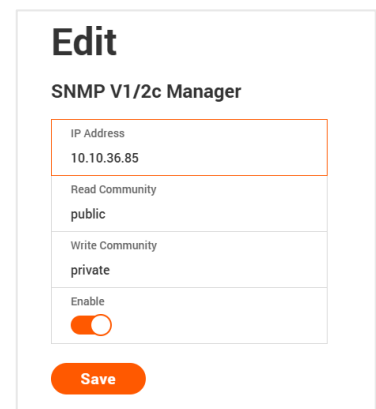
SNMP V1/2c Manager

IP Address	Read Community	Write Community	Enable	
0.0.0.0	public	private	<input checked="" type="checkbox"/>	
0.0.0.0	public	private	<input type="checkbox"/>	
0.0.0.0	public	private	<input type="checkbox"/>	
0.0.0.0	public	private	<input type="checkbox"/>	
0.0.0.0	public	private	<input type="checkbox"/>	

SNMP V3 Manager

Username	Security Level	Authentication Password	Authentication Algorithm	Privacy Key	Privacy Algorithm	Enable	
NoAuthNoPriv	*****	*****	MD5	*****	AES256	<input type="checkbox"/>	

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



Edit

SNMP V1/2c Manager

IP Address
10.10.36.85

Read Community
public

Write Community
private

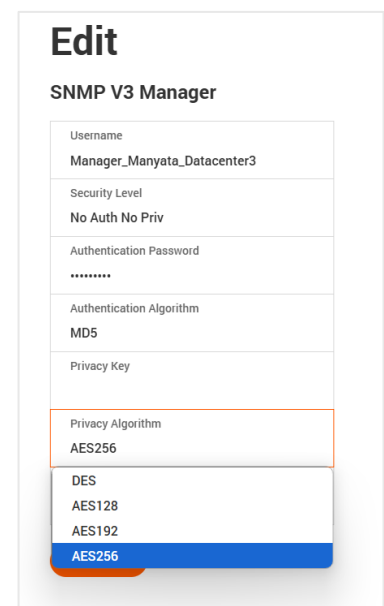
Enable

Save

13. 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:

14. Username
 - Assign the Security Level from the dropdown menu.
15. AuthNoPriv: Authentication and no privacy
16. **AuthPriv**: Authentication and privacy.
17. Type a new unique password as the **Authentication Password**.
18. Select the Authentication Algorithm.
 - MD5
 - SHA



Edit

SNMP V3 Manager

Username
Manager_Manyata_Datacenter3

Security Level
No Auth No Priv

Authentication Password

Authentication Algorithm
MD5

Privacy Key

Privacy Algorithm
AES256


DES
AES128
AES192
AES256

19. Type a new unique password as the **Privacy Key**
20. Select the Privacy Algorithm.
 - DES
 - AES-128
 - AES-192
 - AES-256
21. **Enable** the SNMP V3.
22. Click **Save** button to complete setting.
23. To download the latest MIB file, Click on **Download MIB**

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.

3. To set the SMTP server settings to receive Emails and notifications.
4. Click the  icon to edit/change the **SMTP Account Settings** below:
 - 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.
5. On the top- right side of the **Email Setup** page, Click the below options as required. Click Save.

Edit

SMTP Account Settings

Email Server Address	Bangalore_mailserver
Sender Address	admin@event.com
Port	25
Username	admin
Password	*****
Number of Sending Retries	3
Time Interval Between Sending Retries(in Minutes)	6
Server Requires Authentication	<input checked="" type="checkbox"/>

Save

Edit

Email Recipients

Email Address	admin@event.com
Enable	<input checked="" type="checkbox"/>

Save

Send Test Email

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.

Test Email Recipients

Recipient Email Address	manager_techsupport@event.com
-------------------------	-------------------------------

Send

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.

Events	Email	SNMP Trap	Syslog
Critical Alarm	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Warning Alarm	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Circuit Breaker Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Outlet Power Control Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
External Sensor Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
PDU Configuration File Imported/Exported	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firmware Update	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network Card Reset/Start	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communication Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Daisy Chain Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Enter Bootloader Mode	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Activity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Password/Settings Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Role Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LDAP/Radius Error	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Smart Rack Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Power Sharing Status Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Configuration Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Outlet Group Control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Overload Prevention	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. 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.

SNMPV1 Trap Receiver			
Name	Host	Community	Enable
trap	10.20.14.235	public	✓
		public	×
		public	×
		public	×
		public	×

SNMPv3 Trap Server							
Name	Host	Security Level	Authentication Password	Authentication Algorithm	Privacy Key	Privacy Algorithm	Enable
		NoAuthNoPriv	*****	MD5	*****	AES256	×
		NoAuthNoPriv	*****	MD5	*****	AES256	×
		NoAuthNoPriv	*****	MD5	*****	AES256	×
		NoAuthNoPriv	*****	MD5	*****	AES256	×
		NoAuthNoPriv	*****	MD5	*****	AES256	×

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	Bangalore_Manayata_01
Host	10.10.25.36
Community	public
Enable	<input checked="" type="checkbox"/>

Save

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.

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.

SNMPv1 Trap Receiver							
Name	Host	Community	Enable				
Bangalore_Manayata_01	10.10.25.36	public	✓	✎			
Bangalore_Manayata_02	10.10.25.38	public	✓	✎			

SNMPv3 Trap Server							
Name	Host	Security Level	Authentication Password	Authentication Algorithm	Privacy Key	Privacy Algorithm	Enable
Bangalore_Manayata_01	10.10.25.36	NoAuthNoPriv	*****	MD5	*****	AES256	✓
		NoAuthNoPriv	*****	MD5	*****	AES256	✗
		NoAuthNoPriv	*****	MD5	*****	AES256	✗

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,

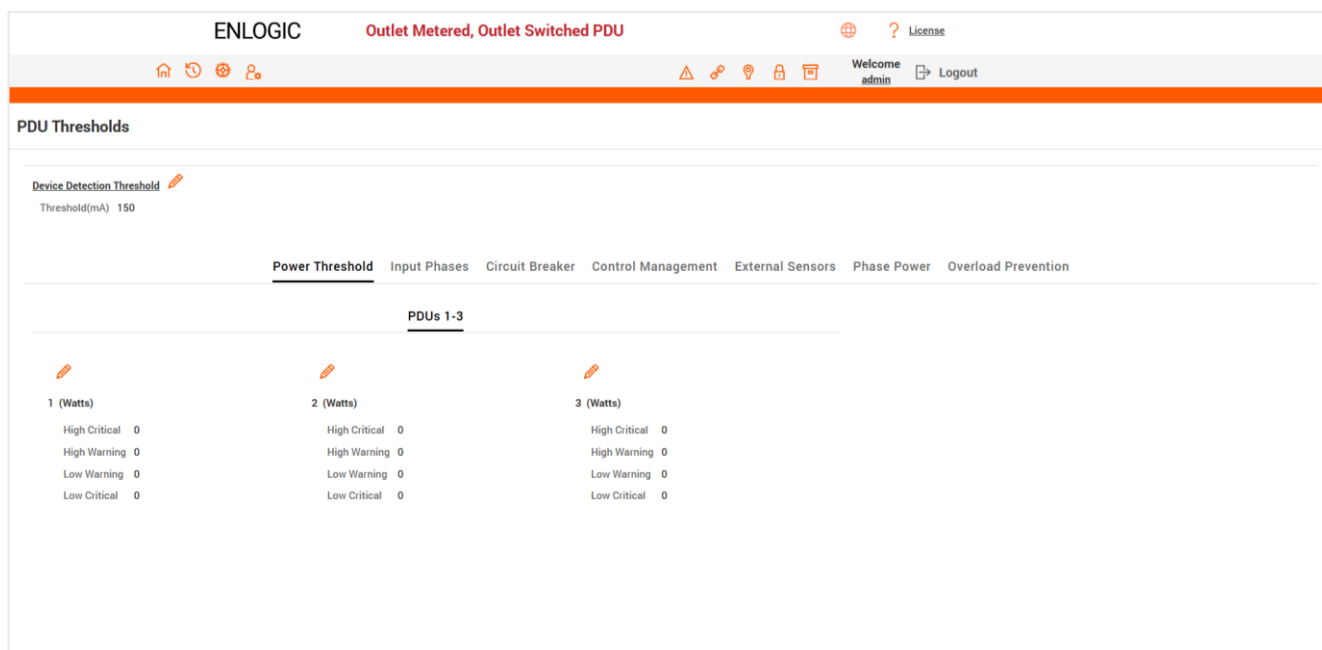
1. Click on the **Settings** icon to dropdown the Settings menu.
2. Select **Thresholds** to view information.

POWER THRESHOLD

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 the  icon edit/change the Power Threshold Setting.



The screenshot displays the ENLOGIC interface for PDU Thresholds. The page title is "ENLOGIC Outlet Metered, Outlet Switched PDU". The navigation bar includes a home icon, a settings icon, and a user profile icon. The main content area is titled "PDU Thresholds" and features a "Device Detection Threshold" section with a value of 150 mA. Below this, there are tabs for "Power Threshold", "Input Phases", "Circuit Breaker", "Control Management", "External Sensors", "Phase Power", and "Overload Prevention". The "Power Threshold" tab is active, showing a table of settings for three PDUs (1, 2, and 3 Watts). Each PDU has four rows of settings: High Critical, High Warning, Low Warning, and Low Critical, all with a value of 0. Each setting row has an edit icon to its left.

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

3. In the **PDU Power Threshold Setting** dialog boxes, change the fields as needed:

- High Critical (W)
- Enable High Critical (W)
- High Warning (W)
- Enable High Warning (W)
- Low Warning (W)
- Enable Low Warning (W)
- Low Critical (W)
- Enable Low Critical (W)
- Reset Threshold (W)
- 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 80
Enable High Critical <input checked="" type="checkbox"/>
High Warning 755
Enable High Warning <input checked="" type="checkbox"/>
Low Warning 25
Enable Low Warning <input checked="" type="checkbox"/>
Low Critical 25
Enable Low Critical <input checked="" type="checkbox"/>
Reset Threshold 100
Alarm State Change Delay (Samples) 25

Save

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,


24. Choose the **Input Phases** tab in the PDU Threshold page.

25. Click the  icon to edit/change the Phase Current Settings.

ENLOGIC
Outlet Metered, Outlet Switched PDU
License

Home Refresh Settings Profile
Alerts Settings Lock Logout







PDU Thresholds

Device Detection Threshold 

Threshold(mA) 150

Power Threshold
Input Phases
Circuit Breaker
Control Management
External Sensors
Phase Power
Overload Prevention

1
2
3

Phase Current	Reading(A)	Low Critical	Low Warning	High Warning	High Critical	
Phase1	0.00	0.00	0.00	22.00	28.00	
Phase2	0.00	0.00	0.00	22.00	28.00	
Phase3	0.00	0.00	0.00	22.00	28.00	
Phase Voltage	Reading(V)	Low Critical	Low Warning	High Warning	High Critical	
Phase1	227.84	180.00	190.00	250.00	260.00	
Phase2	229.25	180.00	190.00	250.00	260.00	
Phase3	228.77	180.00	190.00	250.00	260.00	

3. In the **Input Phase Current Alarm Setting** dialog boxes, change the fields as needed:

- Low Critical (A)
- Enable Low Critical (A)
- Low Warning (A)
- Enable Low Warning (A)
- High Warning (A)
- Enable High Warning (A)
- High Critical (A)
- Enable 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

Edit

Input phases current alarm setting

Low Critical (A)	20
Enable Low Critical	<input checked="" type="checkbox"/>
Low Warning (A)	15
Enable Low Warning	<input checked="" type="checkbox"/>
High Warning (A)	22
Enable High Warning	<input checked="" type="checkbox"/>
High Critical (A)	28
Enable High Critical	<input checked="" type="checkbox"/>
Reset Threshold (A)	1
Alarm State Change Delay (Samples)	0

Save

6. Click the  icon to edit/change the Phase Voltage Settings

7. In the **Input Phase Voltage Alarm Setting** dialog boxes, change the fields as needed:

- Low Critical (V)
- Enable Low Critical (V)
- Low Warning (V)
- Enable Low Warning (V)
- High Warning (V)
- Enable High Warning (V)
- High Critical (V)
- Enable 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.

Edit

Input phases voltage alarm setting

Low Critical (V)	180
Enable Low Critical	<input checked="" type="checkbox"/>
Low Warning (V)	190
Enable Low Warning	<input checked="" type="checkbox"/>
High Warning (V)	215
Enable High Warning	<input checked="" type="checkbox"/>
High Critical (V)	225
Enable High Critical	<input checked="" type="checkbox"/>
Reset Threshold (V)	2
Alarm State Change Delay (Samples)	0

Save

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.

Breaker	Low Critical	Low Warning	High Warning	High Critical	
1	0.00	0.00	11.00	14.00	
2	0.00	0.00	11.00	14.00	
3	0.00	0.00	11.00	14.00	
4	0.00	0.00	11.00	14.00	
5	0.00	0.00	11.00	14.00	
6	0.00	0.00	11.00	14.00	

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)
- Enable Low Critical (A)
- Low Warning (A)
- Enable Low Warning (A)
- High Warning (A)
- Enable High Warning (A)
- High Critical (A)
- Enable High Critical (A)
- Reset Threshold (A)
- Alarm State Change Delay (samples)

2. Click **Save** button to complete the setting.

3. Repeat the steps for all PDUs.

Edit

Bank

Low Critical (A)	25
Enable Low Critical	<input checked="" type="checkbox"/>
Low Warning (A)	20
Enable Low Warning	<input checked="" type="checkbox"/>
High Warning (A)	11
Enable High Warning	<input checked="" type="checkbox"/>
High Critical (A)	14
Enable High Critical	<input checked="" type="checkbox"/>
Reset Threshold (A)	1
Alarm State Change Delay (Samples)	0

Save

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.

ENLOGIC Outlet Metered, Outlet Switched PDU

Home Settings Profile ? License

Welcome admin Logout

PDU Thresholds

Device Detection Threshold Threshold(mA) 150

Power Threshold Input Phases Circuit Breaker **Control Management** External Sensors Phase Power Overload Prevention

PDU-1

Name	Low Critical	Low Warning	High Warning	High	
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	
OUTLET 7	0	0	0	0	
OUTLET 8	0	0	0	0	
OUTLET 9	0	0	0	0	
OUTLET10	0	0	0	0	
OUTLET11	0	0	0	0	

2. Click the icon to edit/change the Control Management Settings,

- Low Critical (W)
- Set Low Critical (W)
- Low Warning (W)
- Set Low Warning (W)
- High Warning (W)
- Set High Warning (W)
- High Critical (W)
- Set 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)	19
Set Lower Critical	<input checked="" type="checkbox"/>
Low Warning (W)	20
Set Lower Warning	<input checked="" type="checkbox"/>
High Warning (W)	75
Set High Warning	<input checked="" type="checkbox"/>
High Critical (W)	80
Set High Critical	<input checked="" type="checkbox"/>
Reset Threshold (W)	25
Alarm State Change Delay (Samples)	1

Save


EXTERNAL SENSORS

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.

The screenshot shows the ENLOGIC PDU Threshold page. At the top, there's a navigation bar with 'ENLOGIC' and 'Outlet Metered, Outlet Switched PDU'. Below that, a secondary navigation bar contains various icons and 'Welcome admin' with a 'Logout' button. The main content area is titled 'PDU Thresholds' and features a 'Device Detection Threshold' of 150 mA. A secondary navigation bar includes 'Power Threshold', 'Input Phases', 'Circuit Breaker', 'Control Management', 'External Sensors' (selected), 'Phase Power', and 'Overload Prevention'. The 'External Sensors' section displays eight sensor configurations in a grid:

External Sensors(1.1)		External Sensors(1.2)		External Sensors(1.3)		External Sensors(1.4)	
Name	TEMP1_PDU1	Name	TEMP2_PDU1	Name	TEMP3_PDU1	Name	HUM1_PDU1
Type	Temperature	Type	Temperature	Type	Temperature	Type	Humidity
Low Critical	15	Low Critical	15	Low Critical	15	Low Critical	20
Low Warning	34	Low Warning	34	Low Warning	33	Low Warning	50
High Warning	35	High Warning	35	High Warning	36	High Warning	60
High Critical	36	High Critical	36	High Critical	38	High Critical	80

External Sensors(1.6)		External Sensors(1.7)		External Sensors(1.8)	
Name	DOORSWITCH_PDU1	Name	HUM2_PDU1	Name	TEMP4_PDU1
Type	Door	Type	Humidity	Type	Temperature
Value	Off	Low Critical	10	Low Critical	0
		Low Warning	10	Low Warning	0

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

The 'Edit External Sensors(1:1)' dialog box shows the following configuration:

High Critical	36
Enable High Critical	<input checked="" type="checkbox"/>
High Warning	35
Enable High Warning	<input checked="" type="checkbox"/>
Low Warning	34
Enable Low Warning	<input checked="" type="checkbox"/>
Low Critical	15
Enable Low Critical	<input checked="" type="checkbox"/>

Save

PHASE POWER

The Phase Power page displays the Active Power and Apparent Power for each PDU Phase-wise.

PDU Thresholds						
Device Detection Threshold						
Threshold(mA) 150						
Power Threshold	Input Phases	Circuit Breaker	Control Management	External Sensors	Phase Power	Overload Prevention
PDU#1						
Active Power(W)	Low Critical	Low Warning	High Warning	High Critical		
Phase1	0.00	0.00	0.00	0.00		
Phase2	0.00	0.00	0.00	0.00		
Phase3	0.00	0.00	0.00	0.00		
Apparent Power(VA)	Low Critical	Low Warning	High Warning	High Critical		
Phase1	0.00	0.00	0.00	0.00		
Phase2	0.00	0.00	0.00	0.00		
Phase3	0.00	0.00	0.00	0.00		

1. Choose the **Phase Power** tab in the PDU Threshold page.
2. Click the icon to edit the Alarms both for Active and Apparent Power for each phase separately.

- Low Critical (W)
- Enable Low Critical (W)
- Low Warning (W)
- Enable Low Warning (W)
- High Warning (W)
- Enable High Warning (W)
- High Critical (W)
- Enable 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

Phase Active Power alarm setting

Low Critical (W)	20
Enable Low Critical	<input checked="" type="checkbox"/>
Low Warning (W)	25
Enable Low Warning	<input checked="" type="checkbox"/>
High Warning (W)	75
Enable High Warning	<input checked="" type="checkbox"/>
High Critical (W)	80
Enable High Critical	<input checked="" type="checkbox"/>
Reset Threshold (W)	75
Alarm State Change Delay	1

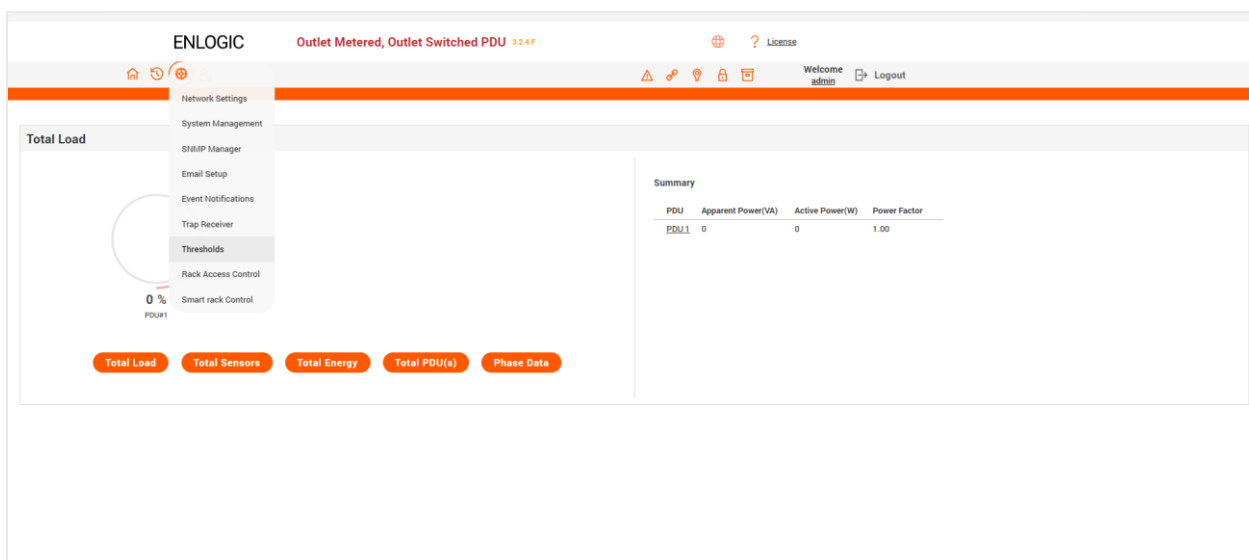
Save

OVERLOAD PREVENTION (OLP)

The Overload Prevention feature manages the load of an iPDU strategically by turning off non-loaded outlets to maintain the overall load within a specified threshold range (between lower and upper threshold values). When the load connected to the PDU increases and exceeds the upper threshold, the feature turns off the respective outlet(s) to mitigate the surge. By default, this threshold is set to half of the PDU's rated load, but it can be configured by an authorized user.

This page allows you to configure the Overload Prevention thresholds.


1. Click on the Settings icon to dropdown the Settings menu.
2. From the dropdown, select Thresholds to view information.



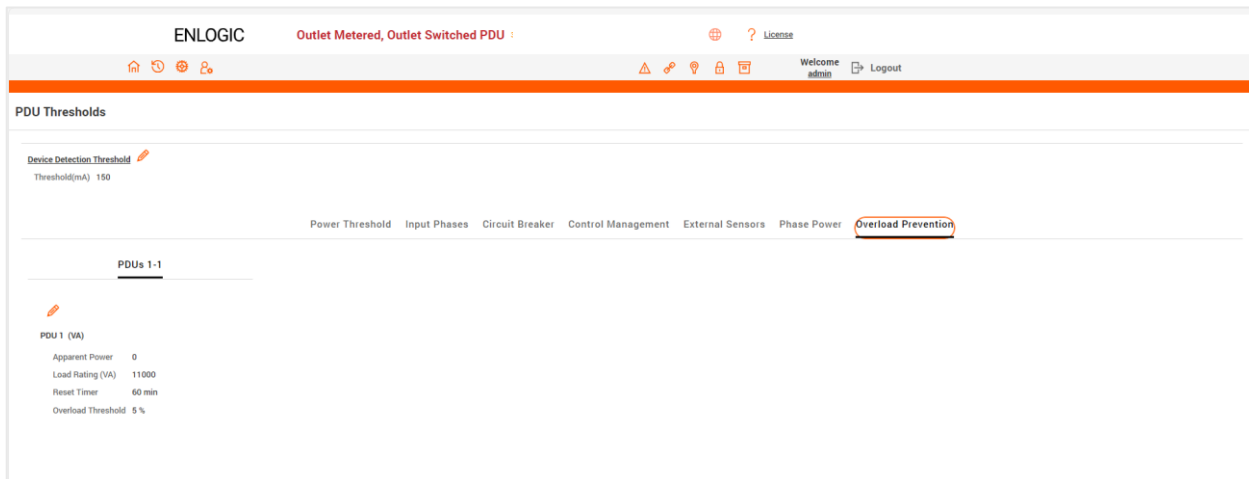
The screenshot displays the ENLOGIC web interface for an "Outlet Metered, Outlet Switched PDU 3.2.4.F". The page features a navigation menu on the left with "Thresholds" selected. The main content area includes a "Total Load" section with a gauge showing 0% and a "Summary" table with the following data:

PDU	Apparent Power(VA)	Active Power(W)	Power Factor
PDU.1	0	0	1.00

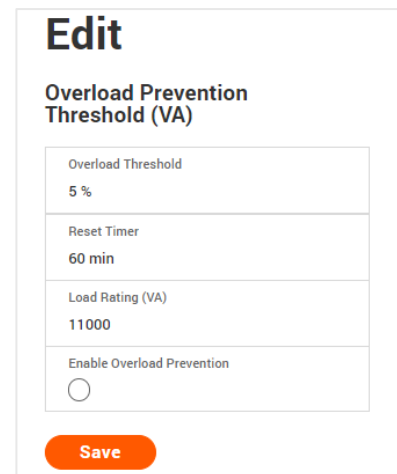
At the bottom of the interface, there are buttons for "Total Load", "Total Sensors", "Total Energy", "Total PDU(s)", and "Phase Data".

3. Click on the Overload Prevention tab to display the PDU parameters to be set.
4. Click on the edit  icon to customize the parameters.

- In the Edit screen, enter the following:



- Overload Threshold – Enter the percentage value and it ranges from 5% to 30%, in increments of 5%.
- Reset Timer – The reset duration can be set to 30, 60, 90, or 120 minutes.
- Load Rating – The default value shall be 50% of the PDU’s Power rated capacity.
- Enable/Disable Overload Prevention.
- Click Save. The data is saved successfully.



Note - Provided the Overload threshold and Load Rating (User Settable Rating Capacity) parameter values, the system automatically computes the upper and lower thresholds.

Note: The system throws an error for a given Load rating, if the corresponding Upper Threshold exceeds the Max. PDU rating. Minimum acceptable value for Load Rating is 1 VA.

- When the PDU apparent power is below lower threshold, normal operation takes place and there happens no change in the outlet state (Refer to Scenario 1 in below example).
- When apparent power lies in between Lower and Upper thresholds, all the unused outlets are turned off and an event/warning alarm will be triggered to alert the user (Refer to Scenario 2 in below example).
- When power rating is above upper threshold, all unused outlets (refer to Scenario 3) /last connected outlet (refer to Scenario 4) that is responsible for the spike are turned off and an event/critical alarm will be triggered to alert the user.
- When the apparent power falls below the lower threshold, reset timer starts. After the reset time has elapsed, all the turned off outlets are turned on.
- Note: Disabling the OLP feature also turns on all the outlets turned off during OLP mode. Outlets turned off manually remain in OFF state only and don’t get affected by OLP feature/mode.
- Outlets control is restricted when the system is in OLP mode.
- Note: Generally, here last connected outlet in the sense which has the last increase/spike in load power.

Example:

Consider the Following parameters

PDU Max. power rating = 20000VA

Default Load Rating (USRC) = 10000VA (50% of max. power rating)

Threshold value = 10%

Therefore,

- Upper Threshold = Load Rating (USRC) + (10% of Load Rating) = 11000 VA
- Lower Threshold = Load Rating (USRC) - (10% of Load Rating) = 9000 VA

Scenario 1: Apparent Power less than Lower Threshold of 9000 VA

OLP feature	Outlet No.	Outlet State	Load in VA
Disabled	1	ON	1000
	2	ON	2000
	3	ON	2000
	4	ON	3000
	5	ON	0
	6	ON	0
	7	ON	0
	8	OFF	0
Total Load			8000 VA

Now, OLP feature is enabled, and an additional load is connected.

OLP feature	New load connected in VA	Result
Enabled	1000 to 2999	Scenario 2
	3000 to 20000 (Max PDU rating)	Scenario 4

Scenario 2: Apparent Power greater than Lower Threshold of 9000 VA & less than Upper Threshold of 11000 VA. Assuming a load of 2000 VA connected to one of the unloaded outlets say, outlet 5. This leads to turning OFF outlets 6 and 7 thereby no new loads can further be connected.

OLP feature	Outlet No.	Outlet State	Load in VA
Enabled	1	ON	1000
	2	ON	2000
	3	ON	2000
	4	ON	3000
	5	ON	2000
	6	OFF	0
	7	OFF	0
	8	OFF	0
Total Load			10000 VA

Scenario 3: Apparent power exceeding 11000 VA from threshold range (10000 VA)

OLP feature	Outlet No.	Outlet State	Load in VA
Enabled	1	ON	1000
	2	ON	2000
	3	ON	2000
	4	ON	5000
	5	ON	2000
	6	OFF	0
	7	OFF	0
	8	OFF	0
Total Load			12000

Out of the already loaded outlets, if one of the outlets say outlet 4, got a sudden spike from 3000 VA to 5000 VA making the overall PDU load to increase from 10000 VA to 12000 VA, instead of outlet 5 (last connected outlet), the outlet on which load spike occurred is turned off (here outlet 4). Now, no new load can be connected to any of the unloaded outlets (here outlets 6,7,8).

Scenario 4: Apparent power exceeding 11000 VA from less than 9000 VA (lower threshold value)

OLP feature	Outlet No.	Outlet State	Load in VA
Enabled	1	ON	1000
	2	ON	2000
	3	ON	2000
	4	ON	3000
	5	OFF	3500
	6	OFF	0
	7	OFF	0
	8	OFF	0
Total Load			11500

Outlet 5 (the last connected outlet) turns OFF to mitigate the overload.

Outlets 6 and 7 turned OFF by OLP feature remains in OFF state until reset timer delay elapses before turning ON.

Outlet 8 that is already in OFF state continues to remain in OFF state.

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.

PDU	Card ID	Aisle	User	Date/Time	Action
1	12345678	Cold Aisle	11	12/10/2024 8:31:10	✗

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

3. Actions
4. New

To Assign new Rack Access to the PDU

Remote Control

Used to perform Lock, Unlock and Close functions.

AutoLock Settings

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

HANDLE AND COMPATIBLE CARD TYPES

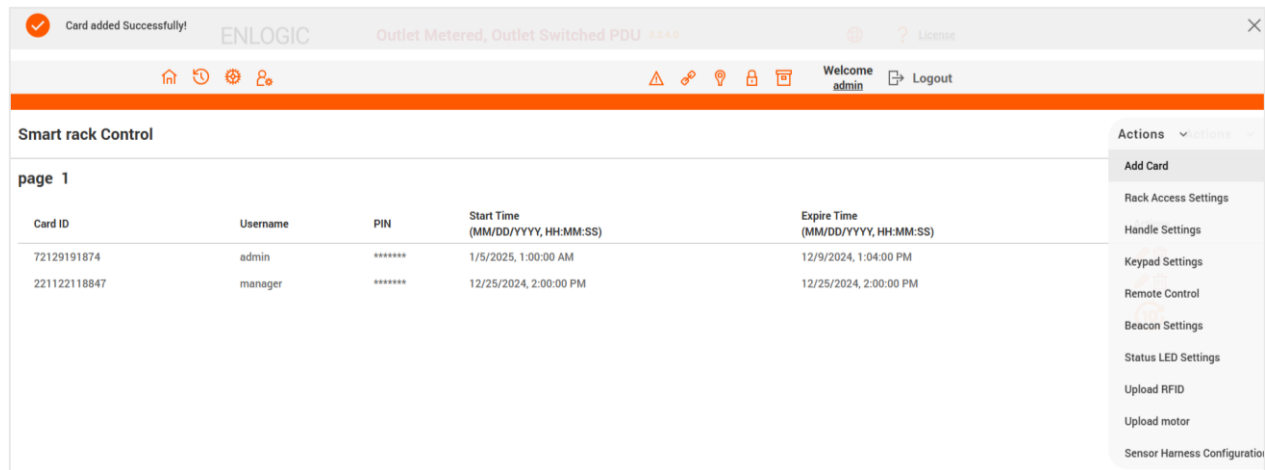
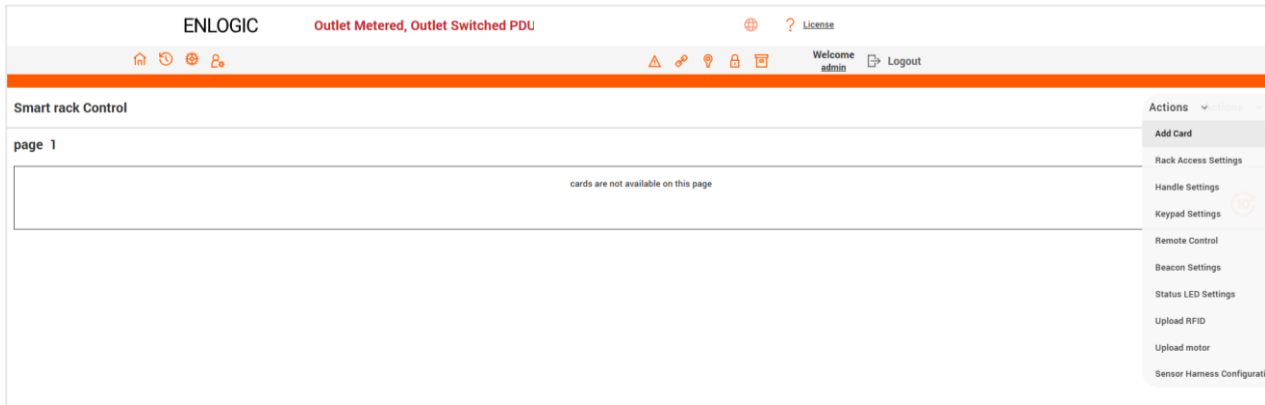
Below are the card lists which are supported on the different swing handle,


1. MYFARE[®] Classic 4K
2. MYFARE[®] Plus 2K
3. MYFARE[®] DESFire 4K
4. HID[®] iCLAS

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.



3. On the top-right side of the Rack Access Control page, Click the **Actions** button to drop down the menu options:
4. To add card details, select **Add Card**.
5. Click the  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
 - Enable **Start Time**
 - Enable **Expire Time**
 - Click **Save** button to complete setting.

Add Card

Card ID 221122118847
Username manager
PIN Please set PIN length in Keypad Setting. Default length is 0
Temporary User <input checked="" type="checkbox"/>
Start Time Start time is optional for Temporary Users. System time is consider if not provided. 12/25/2024 2:00 pm
Expire Time Expire time is applicable only for Temporary Users. 12/25/2024 2:00 pm

Save

6. 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.

The screenshot shows a web interface titled "Edit" with a sub-header "Rack Access Settings". It contains a form with the following fields: "Aisle Control" (Hot/Cold Standalone), "Autolock Time(Sec)" (10), "Door Open Time(Sec)" (10), "Max. Door Open Time(Sec)" (100), and "Work Mode" (RFID & keypad (dual auth)). An orange "Save" button is located at the bottom.

7. To edit handle settings, select **Rack Access Settings**.

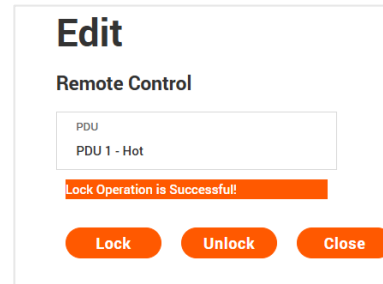
- Enter **Handle name** for identification.
- Enter **ACU Name** for identification.
- The **Firmware Version, Reader Version and Hardware Version** are non- editable fields and are filled by default in their respective Versions.
- Enter **Serial number** of the handle.
- Click Save button to complete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

The screenshot shows a web interface titled "Edit" with a sub-header "Handle Settings". It contains a form with the following fields: "Handle" (PDU 1 - Hot), "ACU Name" (IHIDACU), "Firmware Version" (app ver 4.2), "Reader Version" (rfid ver 1.5), "Hardware Version" (hw ver 6944), and "Serial" (N012590A3). An orange "Save" button is located at the bottom.

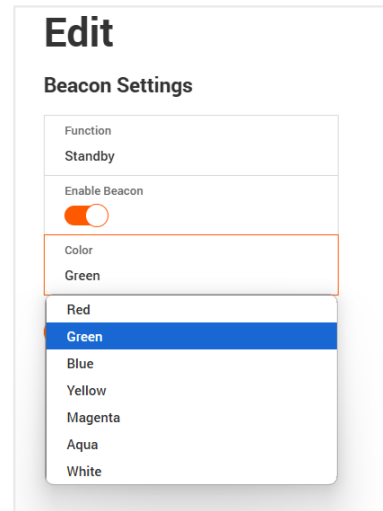
8. Select **Keypad Settings** to configure the keypad. Click Save button to complete setting.

The screenshot shows a web interface titled "Edit" with a sub-header "Keypad Settings". It contains a form with a toggle switch (turned on) and a "Pin Length" field (4). An orange "Save" button is located at the bottom.

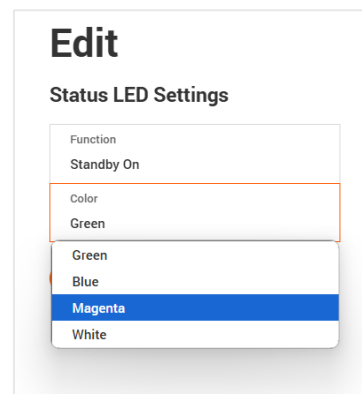
9. Select **Remote Control** to perform **Lock**, **Unlock** and **Close** functions.



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



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



12. Select **Upload RFID** to upgrade the handle RFID firmware. Under the Choose Reader file, click Choose File and select 'reader.bin' file. Select the PDU id from the drop down menu. Click Upload button to start updating the firmware.

Upload RFID

Choose Reader File

Choose File No file chosen

PDU

PDU 1 - Hot

PDU 1 - Hot

Upload

13. Select **Upload Motor** to upgrade the handle motor firmware. Under the Choose motor file, click Choose File and select 'motor.bin' file. Select the PDU id from the drop down menu. Click Upload button to start updating the firmware.

Upload motor

Choose motor File

Choose File No file chosen

PDU

PDU 1 - Hot

PDU 1 - Hot

Upload

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

Edit

Sensor Harness Configuration

Sensor

PDU 1 - Hot

Harness

No Sensor

No Sensor

1 Temperature + 1 Door

3 Temperature + 1 Door

RESIDUAL CURRENT MONITORING (RCM)

Residual Current Monitoring (RCM) is a safety mechanism used in electrical systems to detect residual currents and identify potential risks. The new firmware version supports the monitoring of residual currents, which helps prevent electric shocks, fires, and equipment damage by enabling early fault detection and timely intervention. Enlogic PDUs now include RCM capabilities, are guided by the IEC 62020-1:2020 RCM standards.

Dashboard

If the SKU is equipped and enabled with an RCM module, the Dashboard displays the Residual Current information.

The screenshot shows the ENLOGIC dashboard for an "Outlet Metered, Outlet Switched PDU". The top navigation bar includes the ENLOGIC logo, a globe icon, a "License" link, and a "Welcome admin" message with a "Logout" button. Below the navigation bar, there are several icons for home, refresh, settings, and users. The main content area is titled "Total Load" and features a circular gauge showing "0 %" for "PDU#1". To the right of the gauge is a "Summary" table with the following data:

PDU	Apparent Power(VA)	Active Power(W)	Power Factor
PDU.1	0	0	1.00

At the bottom of the dashboard, there are five orange buttons: "Total Load", "Total Sensors", "Total Energy", "Residual Current", and "Phase Data".

The screenshot shows the ENLOGIC dashboard for an "Outlet Metered, Outlet Switched PDU". The top navigation bar is identical to the previous screenshot. The main content area is titled "RCM" and displays a table with the following data:

PDU#	PDU Name	Current(mA)	Alarm Status	Comm's Status	Self Test Status
PDU 1		3	✓	✓	✓

At the bottom of the dashboard, there are five orange buttons: "Total Load", "Total Sensors", "Total Energy", "Residual Current", and "Phase Data".

Identification

If the SKU is equipped and enabled with an RCM module, the Identification page displays the RCM firmware version, Hardware version and the RCM serial information.

The screenshot shows the ENLOGIC web interface for an 'Outlet Metered, Outlet Switched PDU 3.2.4.D'. The page is titled 'Identification' and contains two main sections: System Information and PDU Information.

Name	Value	Name	Value
System Name		MAC Address	C9-45-44-31-45-55
Contact Name		IPv4 Address	10.20.15.58
Contact Email		IPv6 Link Local Address	fe80::490c:6292:820c:423c
Contact Phone		IPv6 Auto Configured Address	2001:3111:1111:1121:8b4f:d015:4f3f:d3b0
Contact Location			

PDU Information

PDU 1-1

1	
Name	
Core Location	-
Core U Position	
Model	346-415V, 32A, 22.0kVA, 50/60Hz
Part Number	EH6872
Serial Number	W9KP0037
Boot Version	1.2
Web Version	3.0.6
Firmware Version	3.2.4.D
Hardware Version	3.0
PDU Power Rating (kVA)	22
PDU Input Rating (A)	32
PDU Breaker Rating (A)	20
RCM Firmware Version	53
RCM Hardware Version	16
RCM Serial	PDURCM2

Residual Current Monitoring Self Test Configuration

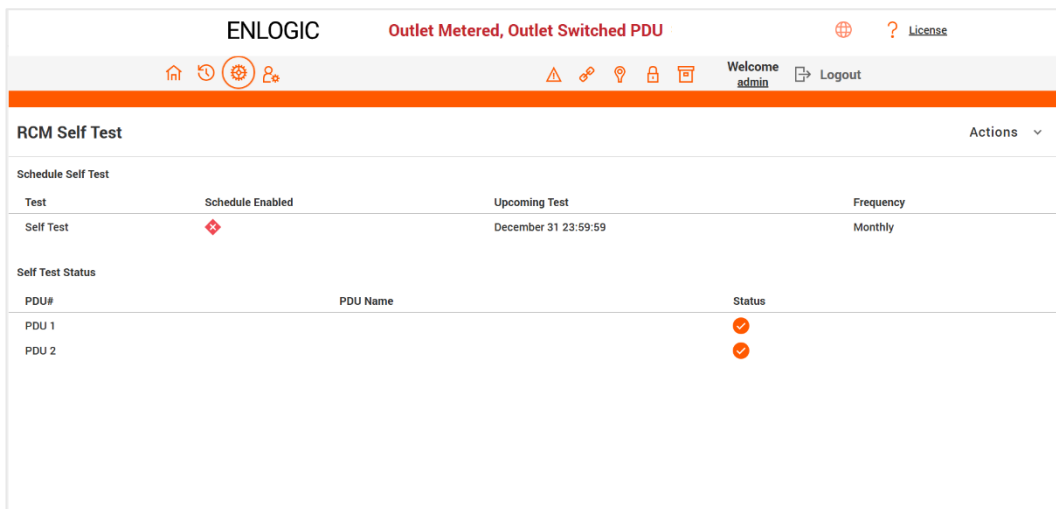
1. Click on Settings icon, select RCM Self Test from the dropdown menu. This option is available exclusively for PDUs equipped and enabled with an RCM module.

The screenshot shows the ENLOGIC web interface for an 'Outlet Metered, Outlet Switched PDU'. The 'Settings' menu is open, and 'RCM Self Test' is selected. The main content area shows a 'Total Load' gauge at 0% and a 'Summary' table.

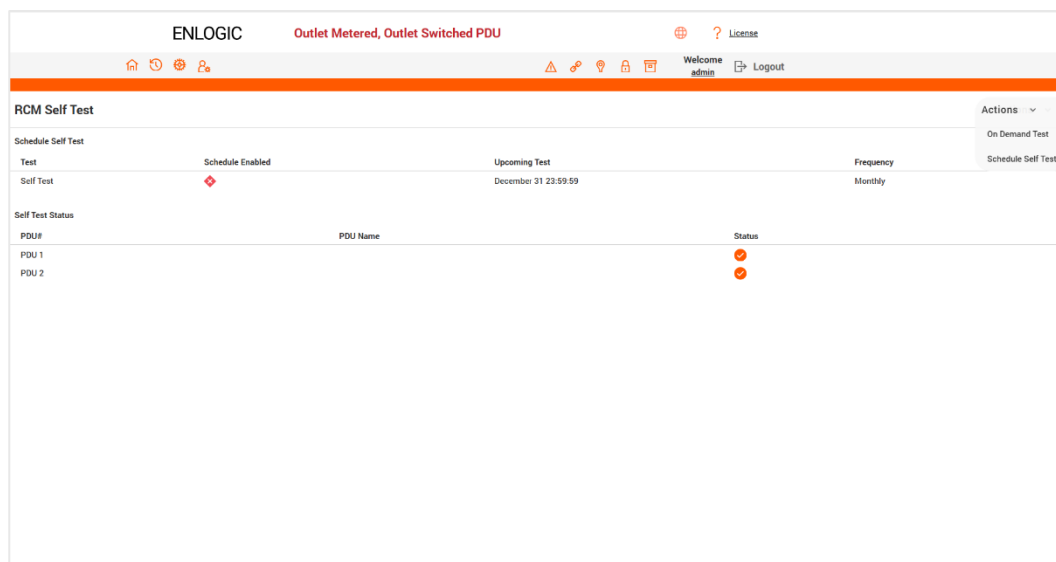
PDU	Apparent Power(VA)	Active Power(W)	Power Factor
PDU.1	0	0	1.00
PDU.2	0	0	1.00

On-Demand Self Test

2. In the RCM Self Test Page, choose the Actions option located on the right-hand side.

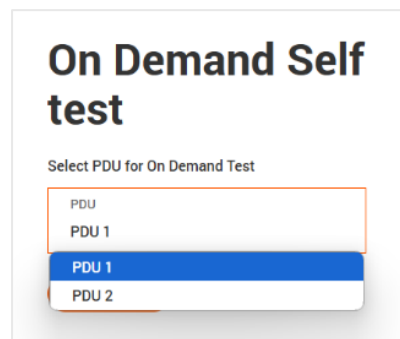


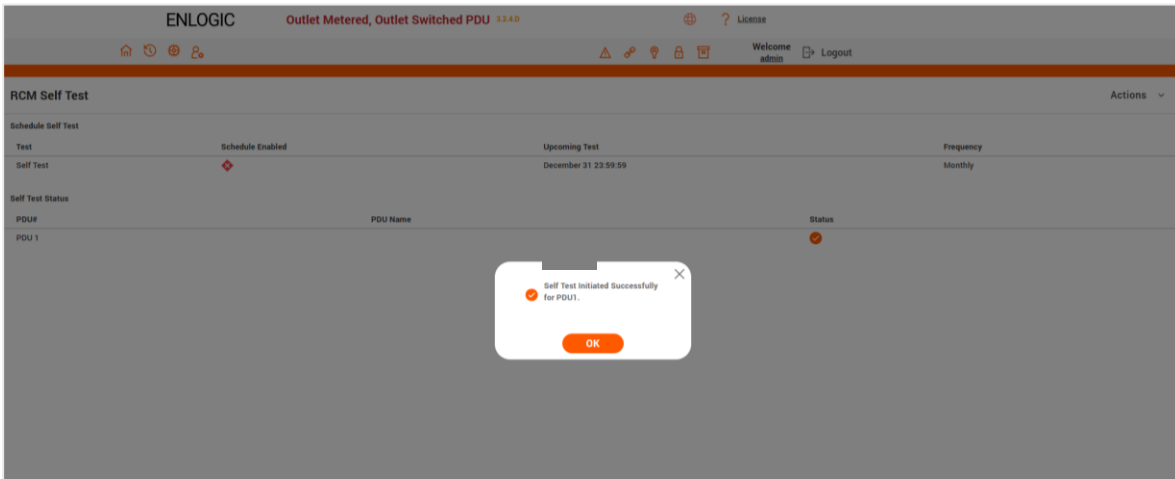
3. Select "On Demand Test" from the drop-down menu.



4. Schedule a On Demand Self Test for a selected PDU from the list.

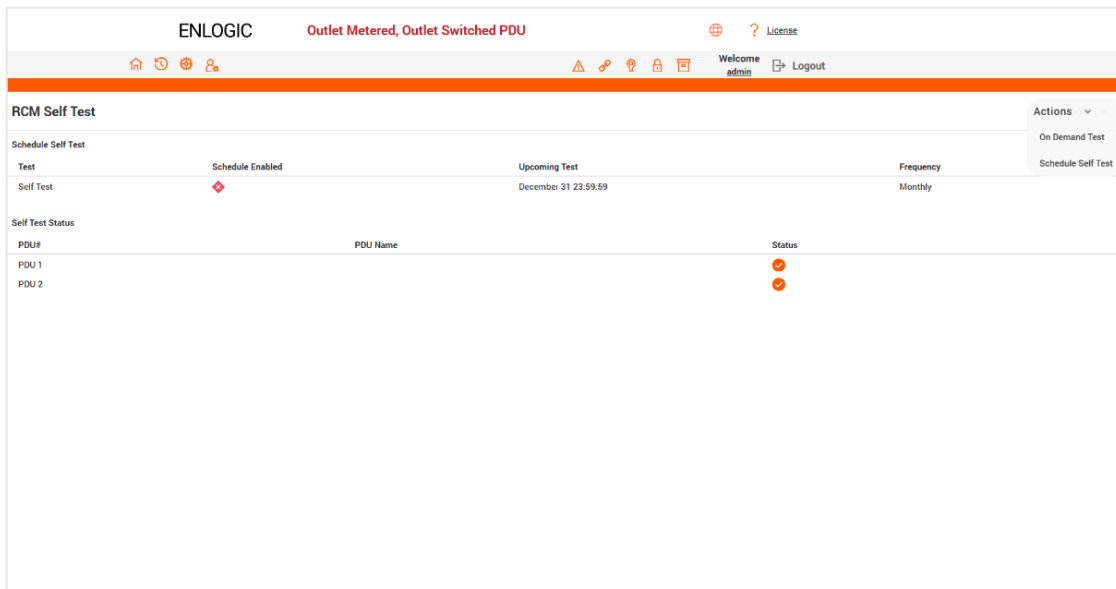
5. Please click on "Start test" to begin on-demand self test.





Schedule Self Test

- From the drop-down menu, select "Schedule Self Test" to schedule a predefined testing cycle.



7. On the scheduling screen,

Select

- Frequency [Daily/ Weekly/ Monthly/ Yearly]
Based on this selection custom options can be selected.
- Month
- Date
- Time
- Enable the schedule test. Toggle On.

Schedule Self Test

Frequency: Daily

23:59:59

Enable Schedule Test:

Set test

Schedule Self Test

Frequency: Weekly

Wednesday

23:59:59

Enable Schedule Test:

Set test

Schedule Self Test

Frequency: Monthly

December

31

23:59:59

Enable Schedule Test:

Set test

Schedule Self Test

Frequency: Yearly

December

31

23:59:59

Enable Schedule Test:

Set test

8. Click on "Set test" to save the settings.

9. The Scheduled Test has been successfully configured.

ENLOGIC Outlet Metered, Outlet Switched PDU

Welcome admin Logout

RCM Self Test

Test	Schedule Enabled	Upcoming Test	Frequency
Self Test	<input checked="" type="checkbox"/>	December 29 23:59:59	Monthly

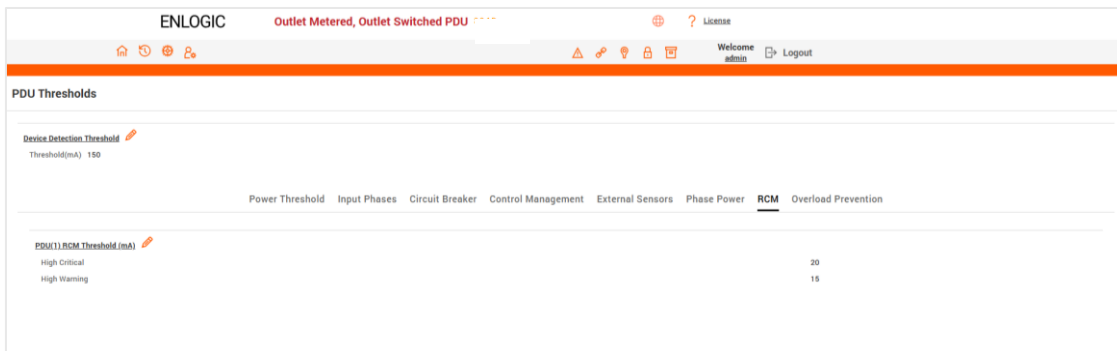
Self Test Status		Status
PDU#	PDU Name	
PDU 1		<input checked="" type="checkbox"/>
PDU 2		<input checked="" type="checkbox"/>


Scheduled Test set successfully

OK

RCM THRESHOLDS

In the Thresholds page, under the RCM tab, the threshold can be set for the selected PDUs.



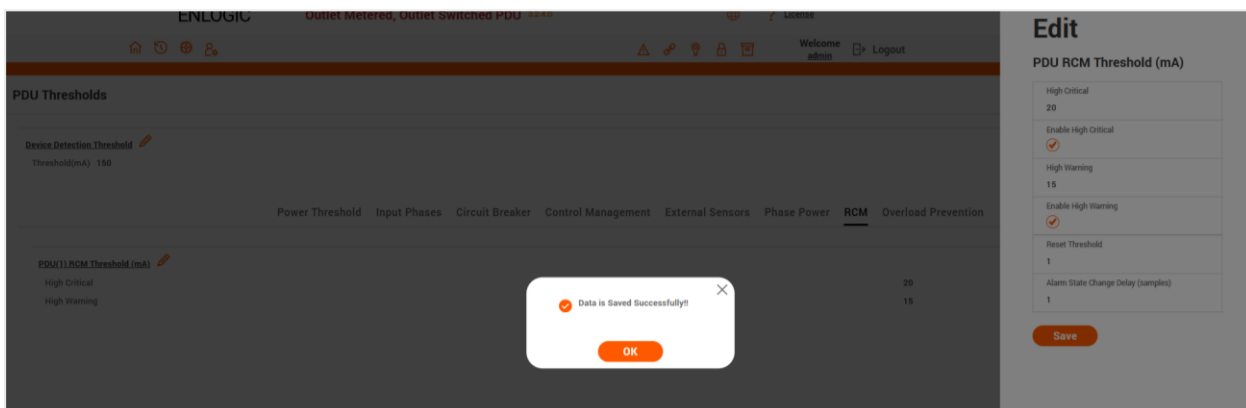
5. In the RCM tab, click on the  edit icon to make changes to the threshold parameters.

- High Critical (W)
- Enable High Critical (W)
- High Warning (W)
- Enable High Warning (W)
- Reset Threshold (W)
- Alarm State Change Delay (samples)

6. Click **Save** button to complete the setting.
7. Repeat the steps for all PDUs. The data is saved successfully.

PDU RCM Threshold (mA)	
High Critical	20
Enable High Critical	<input checked="" type="checkbox"/>
High Warning	15
Enable High Warning	<input checked="" type="checkbox"/>
Reset Threshold	1
Alarm State Change Delay (samples)	1

Save



RCM EVENTS AND ALARMS

In the Event Notifications page, RCM Self Test emails, SNMP Trap and Syslog can be selected to be displayed for PDUs.

The screenshot shows the ENLOGIC interface for 'Outlet Metered, Outlet Switched PDU'. The 'Event Notifications' section contains a table with the following columns: Events, Email, SNMP Trap, and Syslog. Each event has a corresponding checkbox in each column, all of which are checked.

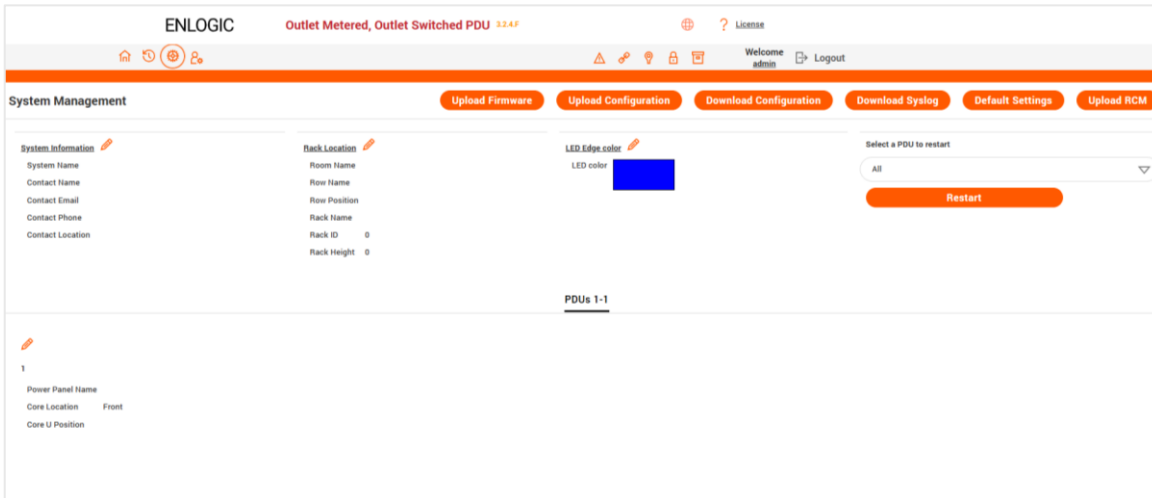
Events	Email	SNMP Trap	Syslog
Critical Alarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Warning Alarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Circuit Breaker Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Outlet Power Control Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
External Sensor Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PDU Configuration File Imported/Exported	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Firmware Update	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Network Card Reset/Start	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Communication Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Daisy Chain Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enter Bootloader Mode	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Activity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Password/Settings Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Role Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LDAP/Radius Error	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Smart Rack Access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power Sharing Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Configuration Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
RCM Self Test	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Outlet Group Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Overload Prevention	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

In the Alarms section, RCM Self Test alarms are displayed for PDUs.

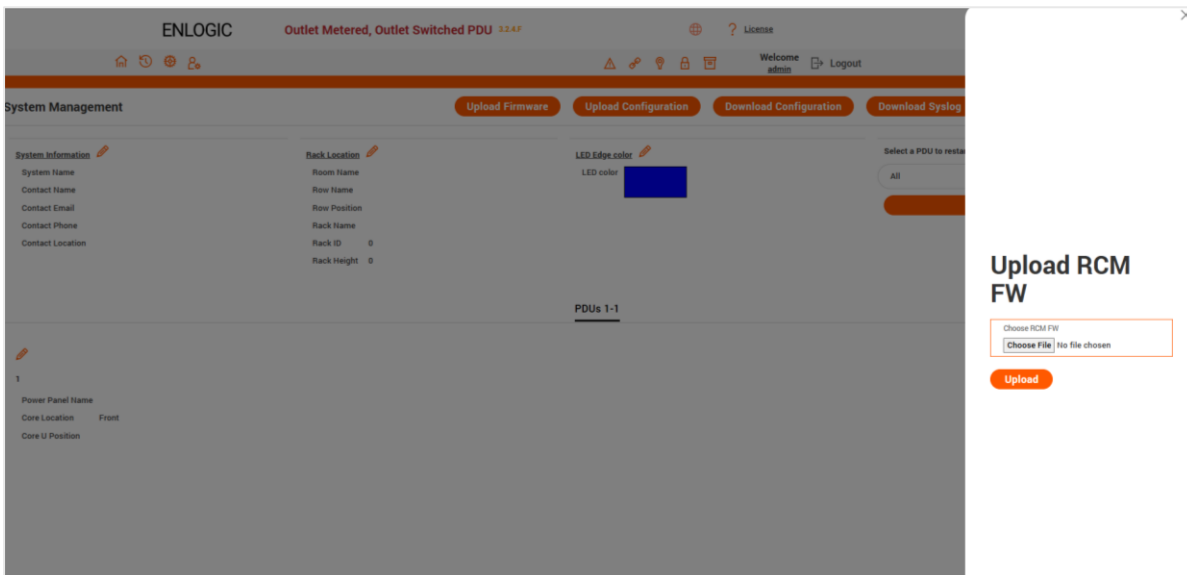
Type	Severity	Description	Date	Time
		Residual Current of PDU(1) is above upper critical	2024/11/14	08:57:25
Type	Severity	Description	Date	Time
		Residual Current of PDU(1) is above upper warning	2024/11/14	09:28:00

RCM FIRMWARE UPDATE

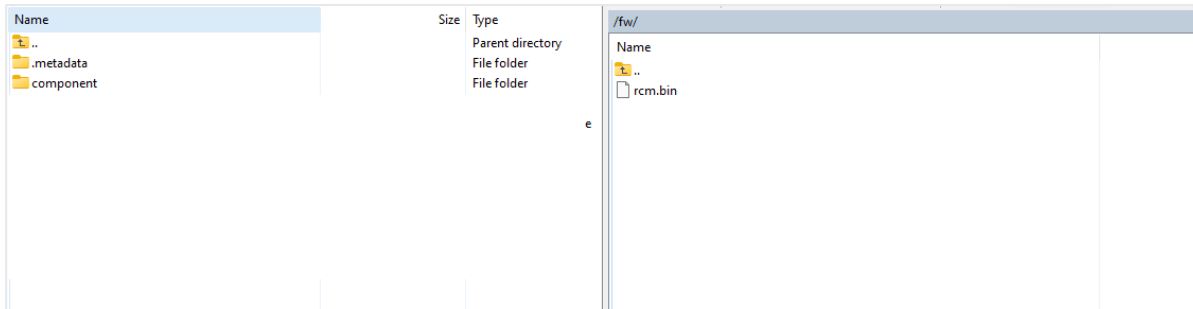
1. Click on the **Settings** icon to dropdown the Settings menu.
2. Select the **System Management** to view the information.



3. Go to System management page and select the Upload Firmware option.



4. Select the PDU you want to upload firmware and upload the rcm.bin file.
Note: PDU will reboot, and Firmware upgrade will complete.
 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 rcm.bin 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 updatercm rcm" 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.

USER SETTINGS

The Advantage Secure PDU includes a standard Administrator profile and a standard User profile. The Administrator profile is typically assigned to the system administrator and possesses the "Admin Role" with full operational permissions. The default User profile encompasses the default "User Role" permissions, with the Administrator required to assign any additional user privileges. Users are identified by their unique login credentials and their assigned user role.

Prior to setting up user profiles, it is essential to determine the necessary roles. Each user must be assigned a role, which defines their granted permissions.

1. To access the User Settings menu, click on the User Settings icon to display the dropdown menu.

The screenshot displays the 'User Settings' page in the ENLOGIC interface. At the top, the system status is 'Outlet Metered, Outlet Switched PDU' and the user is logged in as 'admin'. The 'User Settings' menu is active, showing 'Add Role' and 'Add User' buttons. The page is organized into four main configuration areas:

- Users:** A table listing users with columns for Username, Unit, Role, and Action.

Username	Unit	Role	Action
admin	* F	admin	[Edit]
user	* F	user	[Edit] [Delete]
manager	* F	manager	[Edit] [Delete]
- LDAP Configuration:** Settings for LDAP integration, including Enable (disabled), LDAP Server, Security (none), Port (389), Type (OpenLDAP), Base DN, Bind Password (****), Search User DN, Login Name Attribute, and User Entry Object Class.
- Radius Configuration:** Settings for Radius authentication, including Enable, Server, Port, and Secret.
- Roles:** A table listing roles with columns for Role, Description, and Action.

Role	Description	Action
admin	admin operation	
user	user operation	
manager	redfish user	
- Session Management:** Settings for user sessions, including Sign-in retries allowed (checked), Number of Retries Allowed (3), Session Timeout Value (10 [Minutes of Inactivity]), and Lockout Time (3 [Minutes]).
- Password Policy:** Settings for password requirements, including Password Aging Interval (60d), Minimum Password Length (8), Maximum Password Length (32), and enforcement of password complexity rules (lower case, upper case, numeric, and special characters).

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.



The screenshot shows the ENLOGIC User Settings page. At the top, it says "ENLOGIC Outlet Metered, Outlet Switched PDU". There are navigation icons and a "Welcome admin Logout" message. Below the header, there are "Add Role" and "Add User" buttons. The main content is divided into several sections:

- Users:** A table with columns: Username, Unit, Role, Action. It lists three users: admin (Unit: *F, Role: admin), user (Unit: *F, Role: user), and manager (Unit: *F, Role: manager). Each row has edit and delete icons.
- LDAP Configuration:** A list of settings with checkboxes and values: Enable (checked), LDAP Server, Security (none), Port (389), Type (OpenLDAP), Base DN, Bind Password (****), Search User DN, Login Name Attribute, and User Entry Object Class.
- Radius Configuration:** A table with columns: Enable, Server, Port, Secret, Action. It lists two entries with Server: 1812 and Secret: *****.
- Roles:** A table with columns: Role, Description, Action. It lists three roles: admin (Description: admin operation), user (Description: user operation), and manager (Description: redfish user).
- Session Management:** A list of settings: Sign-In retries allowed (checked), Number of Retries Allowed (3), Session Timeout Value (10 [Minutes of Inactivity]), and Lockout Time (3 [Minutes]).
- Password Policy:** A list of settings: Password Aging Interval (60d), Minimum Password Length (8), Maximum Password Length (32), Enforce at least one lower case character (unchecked), Enforce at least one upper case character (unchecked), Enforce at least one numeric character (checked), and Enforce at least one special character (unchecked).

ADD USERS

To create a new role with custom configurations, where an administrator can assign specific roles to a User.

1. Click on the **User Settings**, the user settings page opens.
2. Click on **Add User** 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.

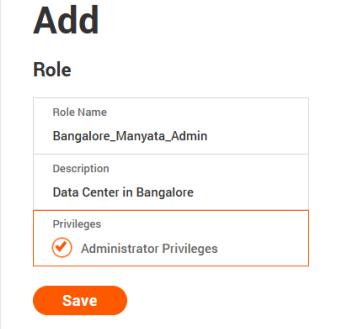
The "Add" form contains the following fields and options:

- User:**
 - Username: Admin_Bangalore
 - Password: [masked]
 - Confirm Password: [masked]
- Role:**
 - admin
 - user
 - manager
 - Manager
- Force Password Change:**
- Save** button

ADD USERS

To create a new user role:

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



Add	
Role	
Role Name	Bangalore_Manyata_Admin
Description	Data Center in Bangalore
Privileges	<input checked="" type="checkbox"/> Administrator Privileges
Save	

Access Control List, allows the administrator to create new roles with custom configuration. This customization includes configuring all/selective outlets/outlet groups control. Roles created with this custom configuration may be assigned to users as per the requirement. These users (with special access permission) shall be able to control assigned outlets/groups.

To create a new user profile with custom configurations, where an administrator can assign specific outlets and outlet groups the user can control :

9. Click on the User Settings, the user settings page opens.
10. Click on the **Add Role** icon, to create a new user role profile.
11. The add user window opens, for a user with Administrator Privileges enter the information:
12. Role Name
13. Description
14. Do not select Leave the Administrator Privileges unchecked to customize outlets/outlet groups for this new role.
15. Scroll Down to set Outlet Privileges, to select the required outlets to be assigned to this role from the list.
16. Choose the Outlet Groups Privileges that have been preassigned to this user during the Add User process.
17. Likewise, select the required outlet groups if any to be assigned to this role.

Note: If there are no outlet groups present in the setup, Outlet Group Privileges sub-section shows No Outlet Groups. To create a new outlet group, go to Control and Manage Page and click on Add Outlet Group button.

18. Select Click on Save button to save the new user role profile. The role is created successfully.

Add

Role

Role Name
Manager

Description
Data Center in Bangalore

Privileges
 Administrator Privileges

Outlet Privileges

PDU 1

<input checked="" type="checkbox"/> Outlet 1	<input type="checkbox"/> Outlet 2
<input checked="" type="checkbox"/> Outlet 3	<input type="checkbox"/> Outlet 4
<input checked="" type="checkbox"/> Outlet 5	<input type="checkbox"/> Outlet 6
<input type="checkbox"/> Outlet 7	<input type="checkbox"/> Outlet 8
<input type="checkbox"/> Outlet 9	<input type="checkbox"/> Outlet 10
<input checked="" type="checkbox"/> Outlet 11	<input type="checkbox"/> Outlet 12
<input checked="" type="checkbox"/> Outlet 13	<input type="checkbox"/> Outlet 14
<input type="checkbox"/> Outlet 15	<input type="checkbox"/> Outlet 16
<input type="checkbox"/> Outlet 17	<input type="checkbox"/> Outlet 18
<input type="checkbox"/> Outlet 19	<input type="checkbox"/> Outlet 20
<input type="checkbox"/> Outlet 21	<input type="checkbox"/> Outlet 22
<input type="checkbox"/> Outlet 23	<input type="checkbox"/> Outlet 24
<input type="checkbox"/> Outlet 25	<input type="checkbox"/> Outlet 26
<input type="checkbox"/> Outlet 27	<input type="checkbox"/> Outlet 28
<input type="checkbox"/> Outlet 29	<input type="checkbox"/> Outlet 30
<input type="checkbox"/> Outlet 31	<input type="checkbox"/> Outlet 32
<input type="checkbox"/> Outlet 33	<input type="checkbox"/> Outlet 34
<input type="checkbox"/> Outlet 35	<input type="checkbox"/> Outlet 36

PDU 2

<input checked="" type="checkbox"/> Outlet 1	<input type="checkbox"/> Outlet 2
<input type="checkbox"/> Outlet 3	<input type="checkbox"/> Outlet 4
<input checked="" type="checkbox"/> Outlet 5	<input type="checkbox"/> Outlet 6
<input checked="" type="checkbox"/> Outlet 7	<input type="checkbox"/> Outlet 8
<input checked="" type="checkbox"/> Outlet 9	<input type="checkbox"/> Outlet 10
<input type="checkbox"/> Outlet 11	<input type="checkbox"/> Outlet 12
<input type="checkbox"/> Outlet 13	<input type="checkbox"/> Outlet 14
<input type="checkbox"/> Outlet 15	<input type="checkbox"/> Outlet 16
<input type="checkbox"/> Outlet 17	<input type="checkbox"/> Outlet 18
<input type="checkbox"/> Outlet 19	<input type="checkbox"/> Outlet 20
<input type="checkbox"/> Outlet 21	<input type="checkbox"/> Outlet 22
<input type="checkbox"/> Outlet 23	<input type="checkbox"/> Outlet 24
<input type="checkbox"/> Outlet 25	<input type="checkbox"/> Outlet 26
<input type="checkbox"/> Outlet 27	<input type="checkbox"/> Outlet 28
<input type="checkbox"/> Outlet 29	<input type="checkbox"/> Outlet 30
<input type="checkbox"/> Outlet 31	<input type="checkbox"/> Outlet 32
<input checked="" type="checkbox"/> Outlet 19	<input type="checkbox"/> Outlet 20
<input type="checkbox"/> Outlet 21	<input type="checkbox"/> Outlet 22

PDU 2

<input checked="" type="checkbox"/> Outlet 1	<input type="checkbox"/> Outlet 2
<input type="checkbox"/> Outlet 3	<input type="checkbox"/> Outlet 4
<input checked="" type="checkbox"/> Outlet 5	<input type="checkbox"/> Outlet 6
<input type="checkbox"/> Outlet 7	<input type="checkbox"/> Outlet 8
<input checked="" type="checkbox"/> Outlet 9	<input type="checkbox"/> Outlet 10
<input type="checkbox"/> Outlet 11	<input type="checkbox"/> Outlet 12
<input type="checkbox"/> Outlet 13	<input type="checkbox"/> Outlet 14
<input type="checkbox"/> Outlet 15	<input type="checkbox"/> Outlet 16
<input type="checkbox"/> Outlet 17	<input type="checkbox"/> Outlet 18
<input type="checkbox"/> Outlet 19	<input type="checkbox"/> Outlet 20
<input type="checkbox"/> Outlet 21	<input type="checkbox"/> Outlet 22
<input type="checkbox"/> Outlet 23	<input type="checkbox"/> Outlet 24
<input type="checkbox"/> Outlet 25	<input type="checkbox"/> Outlet 26
<input type="checkbox"/> Outlet 27	<input type="checkbox"/> Outlet 28
<input type="checkbox"/> Outlet 29	<input type="checkbox"/> Outlet 30
<input type="checkbox"/> Outlet 31	<input type="checkbox"/> Outlet 32
<input type="checkbox"/> Outlet 33	<input type="checkbox"/> Outlet 34
<input type="checkbox"/> Outlet 35	<input type="checkbox"/> Outlet 36

PDU 3

<input type="checkbox"/> Outlet 1	<input type="checkbox"/> Outlet 2
<input type="checkbox"/> Outlet 3	<input type="checkbox"/> Outlet 4
<input type="checkbox"/> Outlet 5	<input type="checkbox"/> Outlet 6
<input type="checkbox"/> Outlet 7	<input type="checkbox"/> Outlet 8
<input type="checkbox"/> Outlet 9	<input type="checkbox"/> Outlet 10
<input type="checkbox"/> Outlet 11	<input type="checkbox"/> Outlet 12
<input type="checkbox"/> Outlet 13	<input type="checkbox"/> Outlet 14
<input type="checkbox"/> Outlet 15	<input type="checkbox"/> Outlet 16
<input type="checkbox"/> Outlet 17	<input type="checkbox"/> Outlet 18
<input type="checkbox"/> Outlet 19	<input type="checkbox"/> Outlet 20
<input type="checkbox"/> Outlet 21	<input type="checkbox"/> Outlet 22
<input type="checkbox"/> Outlet 23	<input type="checkbox"/> Outlet 24
<input type="checkbox"/> Outlet 25	<input type="checkbox"/> Outlet 26
<input type="checkbox"/> Outlet 27	<input type="checkbox"/> Outlet 28
<input type="checkbox"/> Outlet 29	<input type="checkbox"/> Outlet 30
<input type="checkbox"/> Outlet 31	<input type="checkbox"/> Outlet 32
<input type="checkbox"/> Outlet 33	<input type="checkbox"/> Outlet 34
<input type="checkbox"/> Outlet 35	<input type="checkbox"/> Outlet 36

Outlet Groups Privileges

Goals3

Routers_BNG1

Routers_USTUS2

Routers_STL3

Save

ENLOGIC Outlet Metered, Outlet Switched PDU

Welcome **admin** [Logout](#)

User Settings Add Role Add User

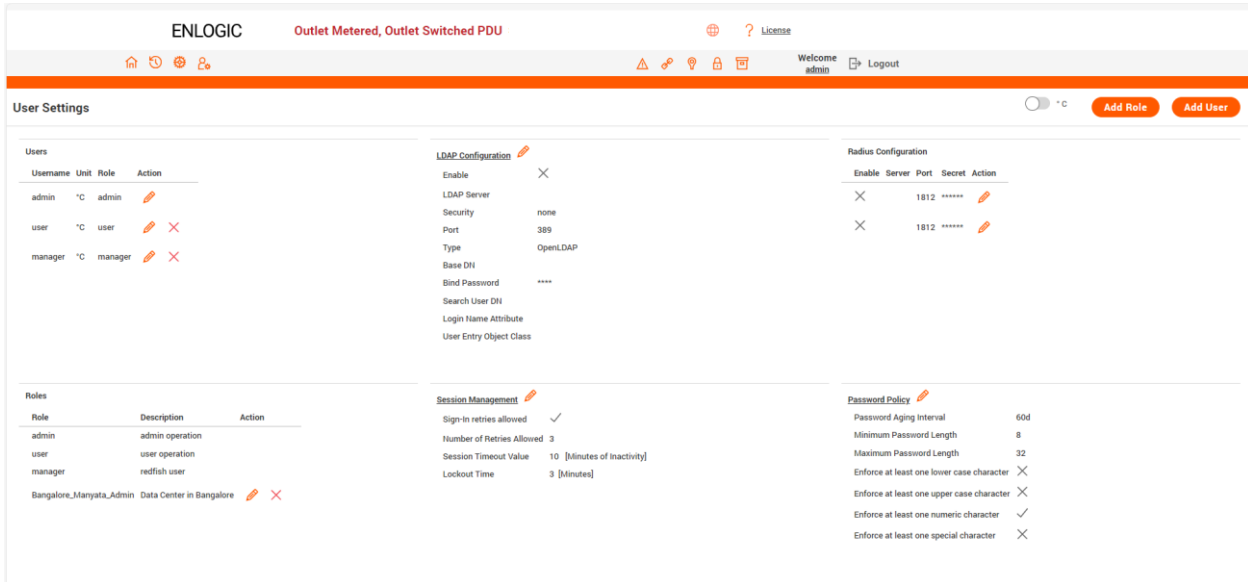
<table border="1" style="width: 100%; border-collapse: collapse; font-size: x-small;"> <thead> <tr><th>Username</th><th>Unit</th><th>Role</th><th>Action</th></tr> </thead> <tbody> <tr><td>admin</td><td>°C</td><td>admin</td><td>✎</td></tr> <tr><td>user</td><td>°C</td><td>user</td><td>✎ ✖</td></tr> <tr><td>manager</td><td>°C</td><td>manager</td><td>✎ ✖</td></tr> </tbody> </table>	Username	Unit	Role	Action	admin	°C	admin	✎	user	°C	user	✎ ✖	manager	°C	manager	✎ ✖	<p>LDAP Configuration</p> <p>Enable <input checked="" type="checkbox"/></p> <p>LDAP Server <input type="checkbox"/></p> <p>Security none</p> <p>Port 389</p> <p>Type OpenLDAP</p> <p>Base DN</p> <p>Bind Password</p> <p>Search User DN</p> <p>Login Name Attribute</p> <p>User Entry Object Class</p>	<p>Radius Configuration</p> <table border="1" style="width: 100%; border-collapse: collapse; font-size: x-small;"> <thead> <tr><th>Enable</th><th>Server</th><th>Port</th><th>Secret</th><th>Action</th></tr> </thead> <tbody> <tr><td><input checked="" type="checkbox"/></td><td>1812</td><td>*****</td><td>✎</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>1812</td><td>*****</td><td>✎</td></tr> </tbody> </table>	Enable	Server	Port	Secret	Action	<input checked="" type="checkbox"/>	1812	*****	✎	<input checked="" type="checkbox"/>	1812	*****	✎
Username	Unit	Role	Action																												
admin	°C	admin	✎																												
user	°C	user	✎ ✖																												
manager	°C	manager	✎ ✖																												
Enable	Server	Port	Secret	Action																											
<input checked="" type="checkbox"/>	1812	*****	✎																												
<input checked="" type="checkbox"/>	1812	*****	✎																												
<table border="1" style="width: 100%; border-collapse: collapse; font-size: x-small;"> <thead> <tr><th>Role</th><th>Description</th><th>Action</th></tr> </thead> <tbody> <tr><td>admin</td><td>admin operation</td><td>✎</td></tr> <tr><td>user</td><td>user operation</td><td>✎</td></tr> <tr><td>manager</td><td>refresh user</td><td>✎</td></tr> <tr><td>Bangalore_Manyata_Admin</td><td>Data Center in Bangalore</td><td>✎ ✖</td></tr> </tbody> </table>	Role	Description	Action	admin	admin operation	✎	user	user operation	✎	manager	refresh user	✎	Bangalore_Manyata_Admin	Data Center in Bangalore	✎ ✖	<p>Session Management</p> <p>Sign-in retries allowed <input checked="" type="checkbox"/></p> <p>Number of Retries Allowed 3</p> <p>Session Timeout Value 10 [minutes of inactivity]</p> <p>Lockout Time 3 [minutes]</p>	<p>Password Policy</p> <p>Password Aging Interval 60d</p> <p>Minimum Password Length 8</p> <p>Maximum Password Length 32</p> <p>Enforce at least one lower case character <input checked="" type="checkbox"/></p> <p>Enforce at least one upper case character <input checked="" type="checkbox"/></p> <p>Enforce at least one numeric character <input checked="" type="checkbox"/></p> <p>Enforce at least one special character <input checked="" type="checkbox"/></p>														
Role	Description	Action																													
admin	admin operation	✎																													
user	user operation	✎																													
manager	refresh user	✎																													
Bangalore_Manyata_Admin	Data Center in Bangalore	✎ ✖																													

Role added Successfully!

OK

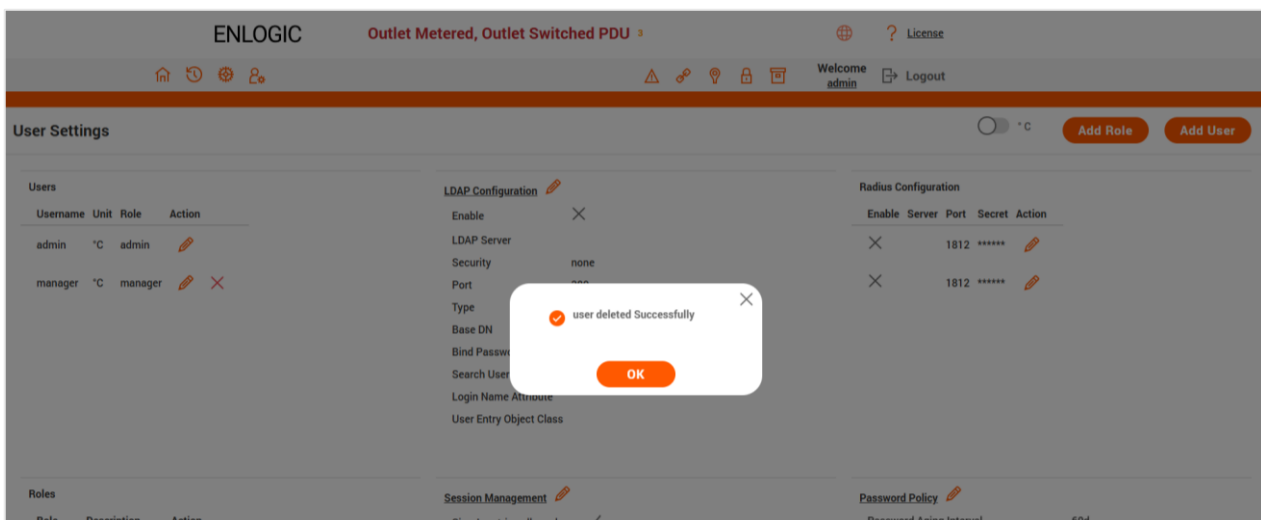
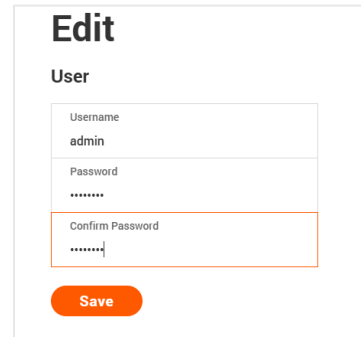
To modify a role profile:

1. Select the role. Click on the edit icon.
2. Edit the Role Name and Privileges as needed.
3. Select **Save** to modify the user profile.



To delete a user profile:

4. Select the role. Click on the **X** icon
5. Click the Delete button. User is deleted successfully.



LDAP/LDAPS SERVER SETTINGS

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

The screenshot shows the ENLOGIC web interface with the following sections:

- Users Table:**

Username	Unit	Role	Action
admin	°C	admin	[Edit]
Admin_Bangalore	°C	admin	[Edit] [X]
manager	°C	manager	[Edit] [X]
- LDAP Configuration:**
 - Enable:
 - LDAP Server: [X]
 - Security: none
 - Port: 389
 - Type: OpenLDAP
 - Base DN: [X]
 - Bind Password: ****
 - Search User DN: [X]
 - Login Name Attribute: [X]
 - User Entry Object Class: [X]
- Radius Configuration:**

Enable	Server	Port	Secret	Action
<input checked="" type="checkbox"/>	[X]	1812	*****	[Edit]
<input checked="" type="checkbox"/>	[X]	1812	*****	[Edit]
- Roles Table:**

Role	Description	Action
admin	admin operation	[Edit]
user	user operation	[Edit]
manager	redfish user	[Edit]
Manager	Data Center in Bangalore	[Edit] [X]
- 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:
 - Enforce at least one numeric character:
 - Enforce at least one special character:

1. In User Setting, go to LDAP Configuration.
2. Select the LDAP Enable.
3. LDAP Server (Type IP Address)
4. Type Port number. Note: For Microsoft, this is typically 389.
5. From the Type (Type of LDAP Server) drop down menu, select Open LDAP.
6. Specify LDAP Type.
7. In the Base DN field, type in the account.
8. Example - CN=myuser, CN=Users, DC=EMEA, DC=mydomain, DC=com
9. Type Password in the Bind Password box
10. Search User DN.
11. Type SAMAccountName (typically) in the Login Name Attribute field.
12. Type Person Name in the User Entry Object Class field.
13. With these LDAP settings configured, the Bind is complete.

The 'Edit LDAP Configuration' form contains the following fields:

- Enable:
- LDAP Server: 10.10.115.86
- Port: 389
- Type: OpenLDAP
- LDAP Type: none
- Base DN: [X]
- Bind Password:
- Search User DN: [X]
- Login Name Attribute: admin
- User Entry Object Class: [X]

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).

In the Edit dialog box, click the Enable button to enable LDAP.

14. Select the LDAP Enable
15. Type the Port number in the Port field.
16. LDAP Server (Type IP Address)
17. Type Port number. Note: For Microsoft, this is typically 389.
18. Click in the Type (for Type of LDAP Server) field, select Open LDAP from the dropdown menu.
19. Click in the LDAP Type field, select TLS from the dropdown menu.
TLS provides additional layer of security making LDAP to secure LDAP.
20. In the Base DN field, type in the account. Example: CN+=myuser, CN=Users, DC=EMEA, DC=mydomain, DC=com
21. In the Bind Password field, type in the password. Type the password again in the Confirm Password box when it opens, to complete the step.
22. Search User DN. Type in your DN.
23. Type SAMAccountName (typically) in the Login Name Attribute field.
24. Type Person Name in the User Entry Object Class field.
25. Click the Save button.

For Testing LDAP Configuration

26. Once LDAP authentication is ready to use.
27. To test this, click **save**, then click "**LDAP Configuration**" again and type **Active Directory username/password** into the test box.
28. Click Test LDAP Configuration.
29. If a box pops up with all green "SUCCEEDED" (no X's), the LDAP is successfully configured.

Edit

LDAP Configuration

Enable	<input checked="" type="checkbox"/>
LDAP Server	10.10.115.86
Port	389
Type	OpenLDAP
LDAP Type	none
Base DN	
Bind Password
Search User DN	
Login Name Attribute	admin
User Entry Object Class	

Test LDAP Configuration

Test Name	Admin_Bangalore
Test Password

RADIUS CONFIGURATION

1. In the **User Settings** go to **Radius Configuration** and click the Edit icon.

The screenshot shows the ENLOGIC User Settings interface. The top navigation bar includes 'ENLOGIC', 'Outlet Metered, Outlet Switched PDU', and a 'License' link. Below the navigation bar, there are icons for home, refresh, settings, and user management. The main content area is titled 'User Settings' and contains several sections:

- Users:** A table with columns 'Username', 'Unit', 'Role', and 'Action'. It lists users: 'admin' (Unit: ^C, Role: admin), 'Admin_Bangalore' (Unit: ^C, Role: admin), and 'manager' (Unit: ^C, Role: manager).
- LDAP Configuration:** A form with fields: 'Enable' (checked), 'LDAP Server', 'Security' (none), 'Port' (389), 'Type' (OpenLDAP), 'Base DN', 'Bind Password' (****), 'Search User DN', 'Login Name Attribute', and 'User Entry Object Class'.
- Radius Configuration:** A table with columns 'Enable', 'Server', 'Port', 'Secret', and 'Action'. It shows two configurations: one with Server '10.10.102.113', Port '1812', and Secret '*****'; another with Port '1812' and Secret '*****'.
- Roles:** A table with columns 'Role', 'Description', and 'Action'. It lists roles: 'admin' (admin operation), 'user' (user operation), 'manager' (redfish user), and 'Manager' (Data Center in Bangalore).
- Session Management:** A form with fields: 'Sign-In retries allowed' (checked), 'Number of Retries Allowed' (3), 'Session Timeout Value' (10 [Minutes of Inactivity]), and 'Lockout Time' (3 [Minutes]).
- Password Policy:** A form with fields: 'Password Aging Interval' (60d), 'Minimum Password Length' (8), 'Maximum Password Length' (32), and four checkboxes for enforcing password complexity rules.

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. The user can add up to two radius server configurations.

The 'Edit Radius Configuration' dialog box is shown. It has a title 'Edit Radius Configuration' and an 'Enable' toggle switch which is currently turned on. Below the toggle are input fields for 'Server' (10.10.102.113), 'Port' (1812), and 'Secret' (*****). A 'Save' button is located at the bottom of the dialog.

This screenshot shows the ENLOGIC User Settings page after the Radius Configuration has been saved. The 'Radius Configuration' table now shows the configuration with the 'Enable' checkbox checked. The 'Secret' field is now visible as '*****'.

RADIUS CONFIGURATION

To allow users to login as the admin Enlogic-User-Role. This example demonstrates how to configure freeradius with users that can login as the admin Enlogic-User-Role. It assumes a clean installation of freeradius on Ubuntu or an equivalent installation.

1. Install **freeradius** or start with a pre-existing installation.
2. Create authorized client configuration statements in `/etc/freeradius/3.0/clients.conf` that are configured for your security requirements.
3. Create a dictionary at `/usr/share/freeradius/dictionary.Enlogic` containing:

```
# -*- text -*-  
VENDOR Enlogic 38446  
BEGIN-VENDOR Enlogic  
ATTRIBUTE Enlogic-User-Role 1 integer  
VALUE Enlogic-User-Role User 1  
VALUE Enlogic-User-Role Admin 2  
END-VENDOR Enlogic  
Load dictionary.
```
4. Enlogic by appending the following line to
`/etc/freeradius/3.0/dictionary:`

```
$INCLUDE /usr/share/freeradius/dictionary.Enlogic
```
5. Add authorized users to `/etc/freeradius/3.0/mods-config/files/authorize` with the desired role. (Note: the 'users' file location may vary based on unique customizations or different package managers.)
6. When specified, the Enlogic-User-Role MUST be the first attribute of the user. Use passwords that are configured for your security requirements.
7. **Enlogic-User-Role** is not specified: (This user logs in as the default "user" Role)

```
radiusdefault Cleartext-Password := "12345678"  
Service-Type = 1
```
8. **Enlogic-User-Role** is set to Admin: (This user logs in as the "admin" Role)

```
radiusadmin Cleartext-Password := "87654321"
```
9. **Enlogic-User-Role** = Admin,

```
Service-Type = 1
```
10. **Enlogic-User-Role** is set to User: (This user logs in as the "user" Role)

```
radiususer Cleartext-Password := "55555555"
```
11. **Enlogic-User-Role** = User,

```
Service-Type = 1
```
12. If you started with a clean install of freeradius, you may need to configure these options to enable authentication in `/etc/freeradius/3.0/radiusd.conf`: (make sure they are configured for your security requirements)

```
auth_badpass = yes  
auth_goodpass = yes  
auth = yes
```

13. Restart the RADIUS server for the configuration changes to take effect.

```
systemctl stop freeradius
```

```
systemctl start freeradius
```

14. Verify the server is able to perform authentication and returns the configured

15. Enlogic-User-Role. Note: You may need to change this example based on any client restrictions that are enforced.

16. Usage: radtest [OPTS] user passwd radius-server[:port] nas-port-number secret

```
# radtest 'radiusadmin' '87654321' 192.0.2.1 0 'Enlogic#1' "
```

17. Sending Access-Request of id 212 to 192.0.2.1 port 1812

```
User-Name = "radiusadmin"
```

```
User-Password = "87654321"
```

```
NAS-IP-Address = 127.0.1.1
```

```
NAS-Port = 0
```

```
Message-Authenticator = 0x00000000000000000000000000000000
```

```
rad_recv: Access-Accept packet from host 192.0.2.1 port 1812, id=212, length=38
```

```
Enlogic-User-Role = Admin
```

```
Service-Type = Framed-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.

The screenshot shows the ENLOGIC User Settings interface. At the top, there's a navigation bar with 'ENLOGIC', 'Outlet Metered, Outlet Switched PDU', and 'License' information. Below that, a 'User Settings' section contains several panels:

- Users:** A table with columns 'Username', 'Unit', 'Role', and 'Action'. It lists 'admin', 'Admin_Bangalore', and 'manager'.
- LDAP Configuration:** A form with fields for 'Enable', 'LDAP Server', 'Security', 'Port', 'Type', 'Base DN', 'Bind Password', 'Search User DN', 'Login Name Attribute', and 'User Entry Object Class'.
- Radius Configuration:** A table with columns 'Enable', 'Server', 'Port', 'Secret', and 'Action'. It shows two entries for RADIUS servers.
- Roles:** A table with columns 'Role', 'Description', and 'Action'. It lists 'admin', 'user', 'manager', and 'Manager'.
- Session Management:** A form with fields for 'Sign-In retries allowed', 'Number of Retries Allowed', 'Session Timeout Value', and 'Lockout Time'.
- Password Policy:** A form with fields for 'Password Aging Interval', 'Minimum Password Length', 'Maximum Password Length', and several enforcement checkboxes for password complexity.

2. Add the required data and click on **Save** button to update the new settings.

The 'Edit Session Management' dialog box is shown, containing the following fields:

- Sign-In retries allowed:
- Number of Retries Allowed: 3
- Session Timeout Value: 10 Minutes
- Lockout Time: 3 Minutes

A 'Save' button is located at the bottom of the dialog.

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**.

The screenshot shows the ENLOGIC User Settings interface. The 'Password Policy' section is highlighted, showing the following configuration:

Enable	Server	Port	Secret	Action
<input checked="" type="checkbox"/>	10.10.102.113	1812	*****	
<input type="checkbox"/>		1812	*****	

Enable	Server	Port	Secret	Action
<input checked="" type="checkbox"/>	10.10.102.113	1812	*****	
<input type="checkbox"/>		1812	*****	

Role	Description	Action
admin	admin operation	
user	user operation	
manager	refresh user	
Manager	Data Center in Bangalore	

Session Management	Action
Sign-In retries allowed	<input checked="" type="checkbox"/>
Number of Retries Allowed	3
Session Timeout Value	10 [Minutes of inactivity]
Lockout Time	3 [Minutes]

Password Policy	Action
Password Aging Interval	60d
Minimum Password Length	8
Maximum Password Length	32
Enforce at least one lower case character	<input checked="" type="checkbox"/>
Enforce at least one upper case character	<input checked="" type="checkbox"/>
Enforce at least one numeric character	<input checked="" type="checkbox"/>
Enforce at least one special character	<input checked="" type="checkbox"/>

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.
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.

The screenshot shows the 'Edit Password Policy' form with the following fields and values:

- 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:

A **Save** button is located at the bottom of the form.

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.

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

The screenshot shows the ENLOGIC web interface for an 'Outlet Metered, Outlet Switched PDU'. The 'SNMP Management' section is active, with a 'Download MIB' button. The 'SNMP General' section shows 'Enable' checked and 'SNMP Version' set to 'V1/2c&V3'. The 'SNMP Port' section shows 'SNMP Port' as 161 and 'SNMP Trap Port' as 162. Below are two tables: 'SNMP V1/2c Manager' and 'SNMP V3 Manager'.

IP Address	Read Community	Write Community	Enable
0.0.0.0	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	✗

Username	Security Level	Authentication Password	Authentication Algorithm	Privacy Key	Privacy Algorithm	Enable
	NoAuthNoPriv	*****	MD5	*****	AES256	✗
	NoAuthNoPriv	*****	MD5	*****	AES256	✗

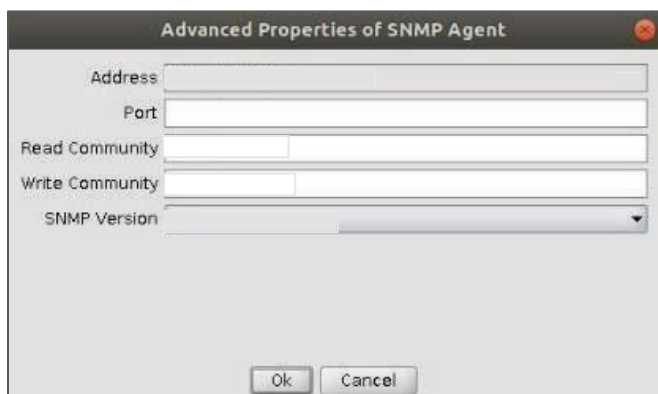
WORKING WITH MIB BROWSER

Download the MIB browser and install it.

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



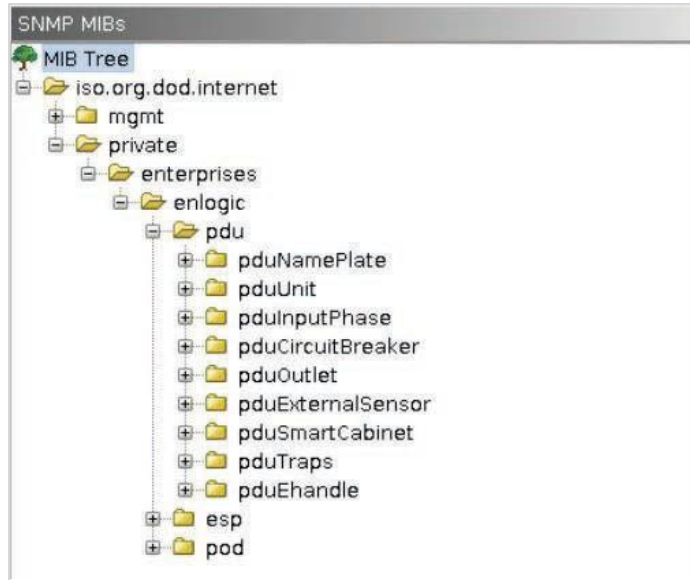
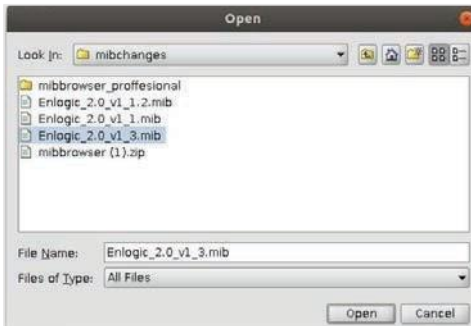
2. Click the Advanced button, in the **Advanced Properties of SNMP Agent** window , enter the respective Port, Read Community and Write Community information.
3. Select the SNMP manager version – **1 / 2 / 3**.



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

DMTF's Redfish[®] is a standard designed to deliver simple and secure management for converged, hybrid IT and the Software Defined Data Center (SDDC). Both human readable and machine capable, Redfish leverages common Internet and web services standards to expose information directly to the modern tool chain.

Enlogic firmware utilizes Redfish, a web-based API, which means that resources are accessed via client-supplied URLs. URLs are necessary for identifying Redfish resources. The Redfish API has a basic URL hierarchy that follows the `/redfish/v1/` pattern for all its resources.

Data center and IT teams want to be able to automate important operations and remotely control hardware, performing services such as:

- Monitor device health and receive automatic notifications on potential concerns.
- Configuring BIOS
- Controlling device power
- Automatically update firmware
- Authorizing and managing users
- Logging events and much more

REDFISH CONFIGURATION

Redfish is a standard that uses RESTful interface semantics to access a schema based data model to conduct management operations. It is suitable for a wide range of devices, from stand-alone servers to composable infrastructures, and to large-scale cloud environments.

REDFISH SCHEMA

Redfish resource schemas are developed using OData Schema, which may be simply converted to JSON Schema. It is a defined directory structure that is accessible using the standard HTTP/HTTPS GET/POST/PUT/DELETE (etc.) methods to perform some action on the application in question.

The REST API lets you select the kind of request. It follows the CRUD standard format (Create, Retrieve, Update, and Delete). The data is created by visiting URIs that are accessible via the following HTTP methods:

Options include GET, HEAD, POST, PUT, PATCH, and DELETE.

REDFISH AUTHENTICATION AND AUTHORIZATION

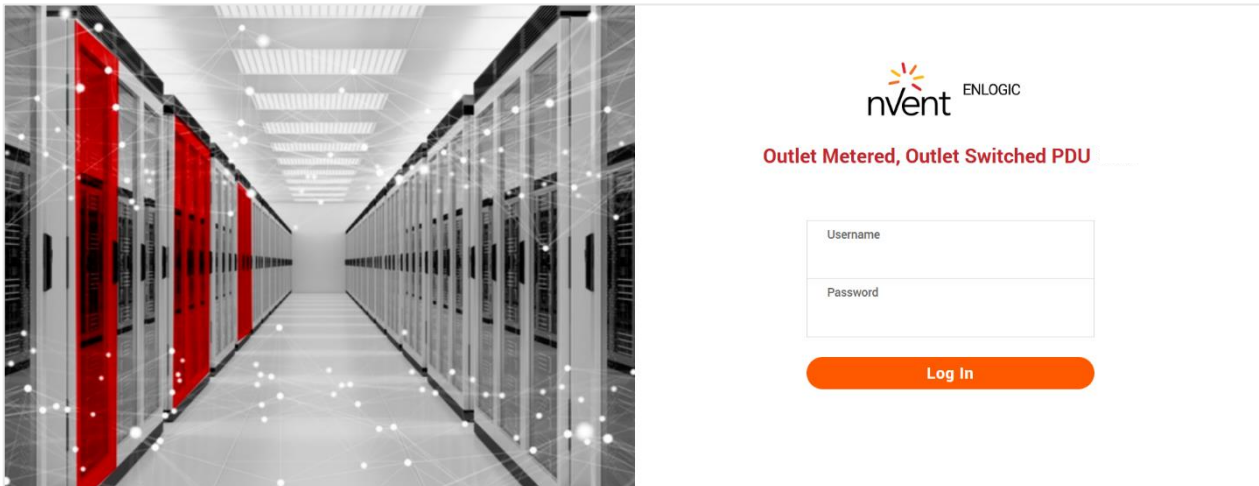
Redfish uses the controlled system for necessary credentials and supported authentication methods. Enlogic Network Controller Management modules uses both local and remote authentication methods, including Active Directory and LDAP. Authorization involves both user privilege and licensing authorization. The user can disable and enable Redfish services using multiple interfaces like CLI/SSH, WEB UI.

The Redfish service provides access to Redfish URLs by using the following methods:

- Basic authentication: In this method, user name and password are provided for each Redfish API request.
- Session-based authentication: This method is used while issuing multiple Redfish operation requests.
- Session login is initiated by accessing the Create session URI. The response for this request includes an X-Auth-Token header with a session token. Authentication for subsequent requests is made using the X-Auth-Token header.
- Session logout is performed by issuing a DELETE of the Session resource provided by the Login operation including the X-Auth-Token header.

LOGIN TO REDFISH USING WEB UI

1. Login to the WEB UI with valid credentials provided. Change the default password.



2. In the main menu, mouse over to Setting and select Network Settings.

3. Select the Web/RESTapi configuration and click on the pen icon to edit the settings.

The screenshot shows the ENLOGIC configuration interface. At the top, there's a header with 'ENLOGIC', 'Outlet Metered, Outlet Switched PDU', and a 'License' link. Below the header is a navigation bar with 'Welcome admin' and 'Logout'. The main content area is titled 'Network Settings' and contains several configuration panels:

- Ethernet-0 IP Configuration:** Network Mode (IPv4/IPv6), Boot Mode IPv4 (DHCP), Boot Mode IPv6 (Autoconfig), IP v4 Address (10.20.15.58), Network Mask (255.255.255.128), Default Gateway (10.20.15.1), IPv6 Link Local Address (fe80::490c:6292::220c:423c), IPv6 Global Configured Address (2001:1111:1111:1121:3b4f:d015:4f3f:d3b0), LLDP (disabled), Authentication (NO Authentication).
- Ethernet-1 IP Configuration:** Network Mode (IPv4/IPv6), Boot Mode IPv4 (DHCP), Boot Mode IPv6 (Autoconfig), IP v4 Address (0.0.0.0), Network Mask (0.0.0.0), Default Gateway (0.0.0.0), IPv6 Link Local Address, IPv6 Global Configured Address, LLDP (disabled), Authentication (NO Authentication).
- Domain Name System:** Manually Override Servers (0.0.0.0), Primary DNS Server (0.0.0.0), Secondary DNS Server (0.0.0.0), Edit Hostname/Domain (disabled), Host Name, Domain Name(IPv4/IPv6).
- Web/RESTapi Access Configuration:** Web Access (http&https), Web Port (80/443), Redirection (checked), RESTapi Access (disabled), Certificate (View Certificate button).
- SSH/FTPs Configuration:** SSH Access (checked), SSH Port (22), FTPs Access (checked), FTPs Port (21), Telnet Access (disabled), Telnet Port (23).
- Network Time Protocol(NTP):** Enable (disabled), Primary NTP Server (0.0.0.0), Secondary NTP Server (0.0.0.0).
- Date/Time Settings:** Date (2024/12/17), Time (12:01:42), Date Format (YYYY/MM/DD).
- Daylight Saving Time:** Enable (disabled), Start Month (HH|H|0), End Month (HH|H|0).

4. In the Edit screen, provide all the details and Enable the RESTapi Access. Click Save.

The screenshot shows the 'Edit Web/RESTapi Access Configuration' dialog box. It contains the following fields and options:

- Web Access:** Htt & Https
- HTTP Port:** Default 80 for Http, 80
- HTTPS Port:** Default 443 for Https, 443
- Redirection:**
- RESTapi Access:** Disable (selected), Enable (highlighted in blue)
- SSL Certificate:** Choose File No file chosen
- SSL Certificate Key:** Choose File No file chosen
- Save:** Save button

REDFISH URLS SUPPORTED WITH GET METHOD

Listed URLs with their Syntax

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}
5	/redfish/v1/EventService

Managers

S.No	URL
1	/redfish/v1/Managers
2	/redfish/v1/Managers/manager
3	/redfish/v1/Managers/1/Actions/Manager.DownloadConfiguration
4	/redfish/v1//Managers/manager/NetworkProtocol
5	/redfish/v1//Managers/1/LogServices
6	/redfish/v1//Managers/1/LogServices/Log
7	/redfish/v1//Managers/1/LogServices/Log/Entries
8	/redfish/v1/Managers/manager/EthernetInterfaces
9	/redfish/v1/Managers/manager/EthernetInterfaces/eth0
10	/redfish/v1/Managers/manager/EthernetInterfaces/eth1
11	/redfish/v1/Managers/LogServices/SyslogEntries
12	/redfish/v1/Managers/1/LogServices/Log/Entries

Account Service

S.No	URL
1	/redfish/v1/AccountService
2	/redfish/v1/AccountService/Accounts
3	/redfish/v1/AccountService/Accounts/{user/admin}
4	/redfish/v1/AccountService/Roles
5	/redfish/v1/AccountService/Roles/{Administrator/ ReadOnly / Operator/ Manager}
6	/redfish/v1/AccountService/Accounts/1
7	/redfish/v1/AccountService/Accounts/10

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}
4	/redfish/v1/PowerEquipment/PDUs/1/Actions/PowerShare
5	/redfish/v1/PowerEquipment/PDUs/1/PhaseData
6	/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/TotalEnergy

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

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

Chassis

S.No	URL
1	/redfish/v1/Chassis/1/Power/OutletGroups
2	/redfish/v1/Chassis/1/Sensors/DeviceDetectionThreshold

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}

NEW REDFISH URLS SUPPORTED WITH POST METHOD

Thresholds

S.No	URL
1	/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/PDUTemp
2	/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/PDUHumidity
3	/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/PowerThreshold
4	/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/VoltageThreshold
5	/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/CurrentThreshold
6	/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/CBThreshold
7	/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/OutletThreshold

Other Features

S.No	URL
1	/redfish/v1/Managers/SysInfo
2	/redfish/v1/Chassis/1/Oem/nVentChassis/v1_0_0/LEDColor
3	/redfish/v1/EventService/Subscriptions/Syslog
4	/redfish/v1/Actions/Control.ResetToDefaults

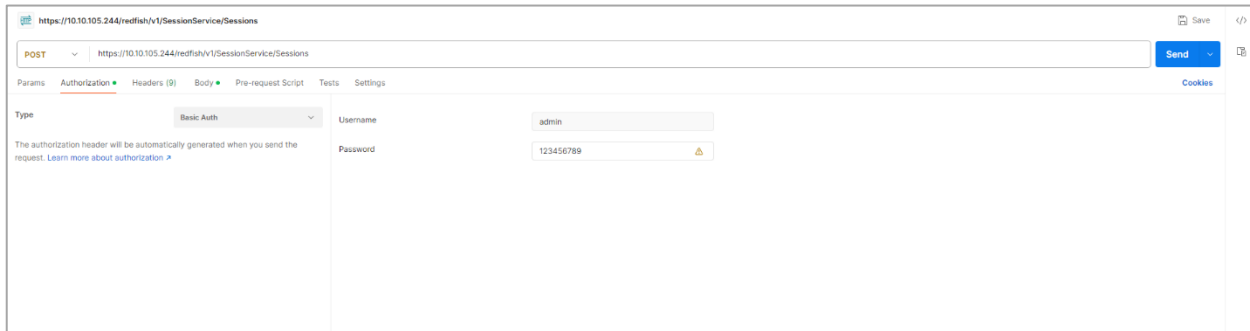
GETTING STARTED WITH REDFISH

Using Redfish Post method, the user can create accounts and their privileges. Let us understand the steps to create them.

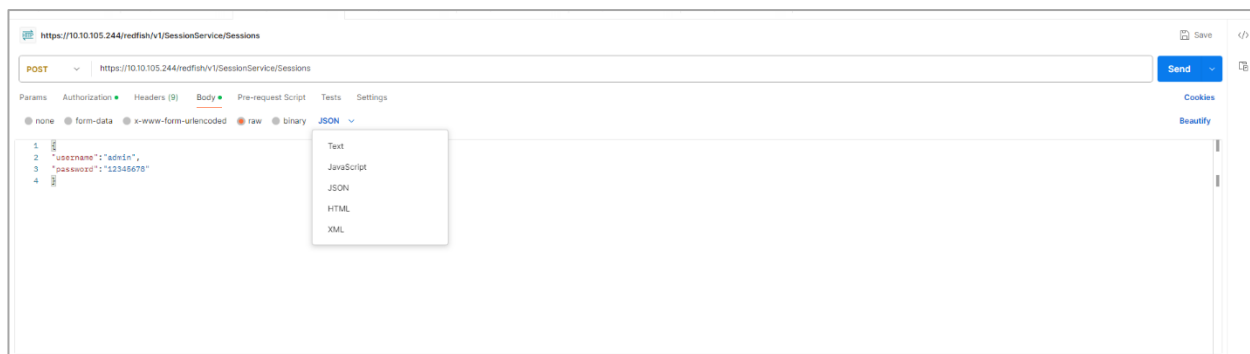
1. Creating A Session

METHOD: POST

1. Download Install the Postman API from <https://www.postman.com/downloads/>



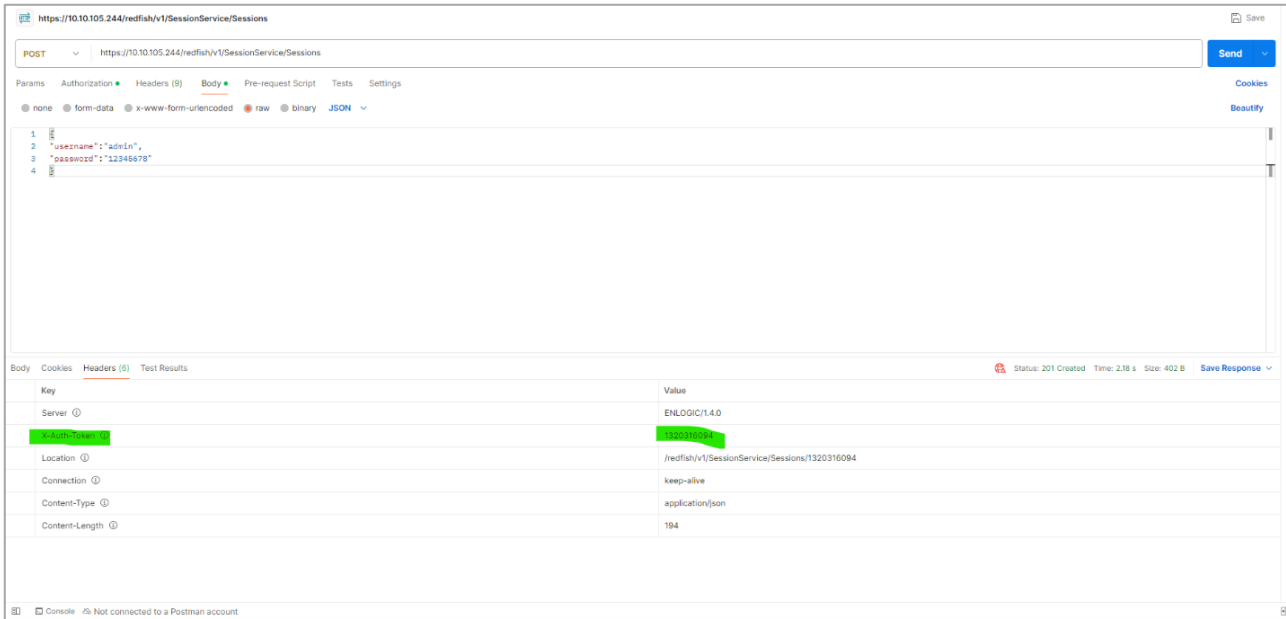
2. On the header, click on the **Body** tab, select **raw**, and under the JSON tab select **Payload**



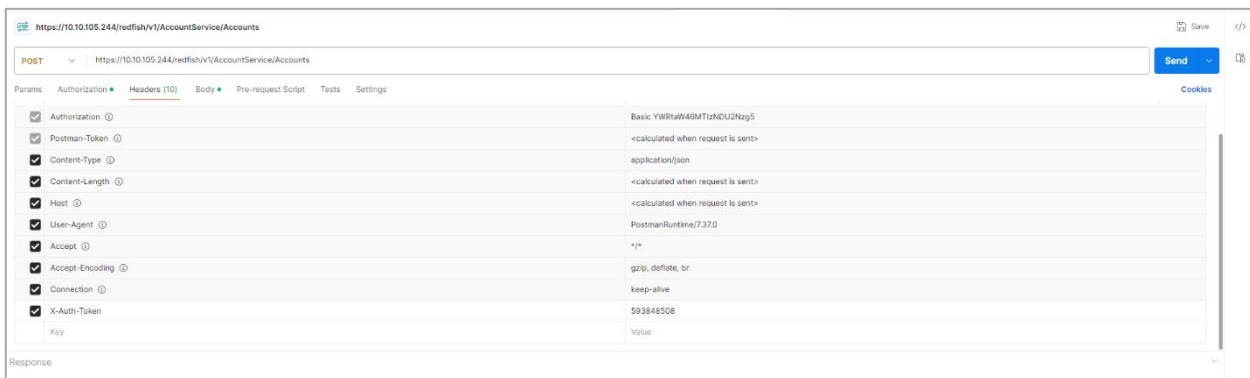
3. Add the **Payload** script and **Send** the request.

Payload:

```
{  
  "username": "admin",  
  "password": "12345678"  
}
```



- Copy the X-Auth-Token values displayed in the above screen and add them under the X-Auth-Token Header. Next use the POST, PATCH, DELETE as shown in the next sections.



Note – Authorization should be containing BASE64 encoded credentials.

2. Add New User

METHOD: POST

URL – <https://{pdu-ip}/redfish/v1/AccountService/Accounts>

Payload:

```
{
  "UserName": "admin16",
  "Password": "123456789",
  "RoleId": "admin"
}
```

Success response:

```
{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "ManagerAccount",
      "Message": "Successfully Completed Request",
      "Severity": "OK",
      "MessageSeverity": "OK",
      "Resolution": "NONE"
    }
  ]
}
```

Curl Command

```
curl -location 'https://{pdu-ip}/redfish/v1/AccountService/Accounts' \
--header 'X-Auth-Token: 593848508' \
--header 'Content-Type: application/json' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg=' \
--data '{
  "UserName": "admin17",
  "Password": "123456789",
  "RoleId": "admin"
}'
```

The screenshot shows a REST client interface with the following details:

- URL:** `https://10.10.105.244/redfish/v1/AccountService/Accounts`
- Method:** `POST`
- Body (Request):**

```

1  {
2  ... "UserName": "admin16",
3  ... "Password": "123456789",
4  ... "RoleId": "admin"
5  }

```
- Response:**
 - Status:** 201 Created
 - Time:** 452 ms
 - Size:** 399 B
- Body (Response):**

```

1  {
2  "code": "Success",
3  "message": "Successfully Completed Request",
4  "@Message.ExtendedInfo": [
5  {
6  "@odata.type": "Message.v1_2_0.Message",
7  "MessageId": "ManagerAccount",
8  "Message": "Successfully Completed Request",
9  "Severity": "OK",
10 "MessageSeverity": "OK",
11 "Resolution": "NONE"
12 }
13 ]
14 }

```

Parameter Errors and Resolution Messages

User Privilege Error:

```

{
"code": "JSON data Error", "message": "Privilege Error", "@Message.ExtendedInfo": [
{
"@odata.type": "Message.v1_2_0.Message", "MessageId": "ManagerAccount", "Message":
"Privilege Error",
"Severity": "Warning", "MessageSeverity": "Warning",
"Resolution": "User Don't have valid Privilege to configure the system"
}
]
}

```

```
}  
]  
}
```

b. Existing User Error:

```
{  
  "code": "User Privilege Error", "message": "Failed to add user", "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "ManagerAccount", "Message": "Failed to add  
      user",  
      "Severity": "Warning", "MessageSeverity": "Warning", "Resolution": "User is already existed"  
    }  
  ]  
}
```

c. JSON Packet Error:

```
{  
  "code": "URL Error",  
  "message": "Failed to parse the packet", "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "ManagerAccount", "Message":  
      "Failed to parse the packet", "Severity": "Warning",  
      "MessageSeverity": "Warning",  
      "Resolution": "JSON unpack error, Enter the valid JSON packet"  
    }  
  ]  
}
```

d. Missing User Name Or Role ID In Payload Or Both:

```
{  
  "UserName": "", "Password": "123456789", "RoleId": ""  
}
```

Response-body:

```
{  
  "code": "Invalid Information", "message": "Bad request", "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "ManagerAccount", "Message": "Bad  
      request",  
      "Severity": "Warning", "MessageSeverity": "Warning",  
      "Resolution": "Incomplete information provided, Enter the full and valid data"  
    }  
  ]  
}
```

```
}  
]  
}
```

e. Invalid User RoleID In Payload:

```
{  
  "code": "Invalid Information", "message": "Bad request", "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "ManagerAccount", "Message": "Bad request",  
      "Severity": "Warning", "MessageSeverity": "Warning", "Resolution": "Enter the valid Roletype"  
    }  
  ]  
}
```

f. Data Error:

```
{  
  "code": "Data Error",  
  "message": "User information not found", "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "ManagerAccount", "Message": "User  
information not found", "Severity": "Warning",  
      "MessageSeverity": "Warning",  
      "Resolution": "User not found, Enter valid user"  
    }  
  ]  
}
```

g. User Privilege Error:

```
{  
  "code": "User Privilege Error", "message": "Privilege Error", "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "ManagerAccount", "Message": "Privilege Error",  
      "Severity": "Warning", "MessageSeverity": "Warning", "Resolution": "Token not authorized"  
    }  
  ]  
}
```


3. User Delete:

METHOD: DELETE

URL – <https://{pdu->

[ip}/redfish/v1/AccountService/Accounts/{user_name}](https://{pdu-ip}/redfish/v1/AccountService/Accounts/{user_name}) Note –

In the last Parameter specify the Username to be deleted.

Payload: NA

Success response:

```
{
  "code": "Success",
  "message": "Successfully Completed Request", "@ Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "ManagerAccount",
      "Message": "Successfully Completed Request", "Severity": "OK", "MessageSeverity": "OK",
      "Resolution": "User deleted successfully"
    }
  ]
}
```

Curl Command

```
curl -location --request DELETE
'https://{pdu-ip}/redfish/v1/AccountService/Accounts/admin16' \
--header 'X-Auth-Token: 786707833'

curl -location 'https://{pdu-ip}/redfish/v1/AccountService/Roles'
\--header 'X-Auth-Token: 786707833' \
--header 'Content-Type: application/json' \
--data '{
  "Id": "Administrator", "Description": "nmc user", "Name": "NMC"
}'
```

https://10.10.105.244/redfish/v1/AccountService/Accounts/admin16 Save

DELETE | https://10.10.105.244/redfish/v1/AccountService/Accounts/admin16 Send

Params Authorization Headers (7) **Body** Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary

This request does not have a body

Body Cookies Headers (4) Test Results 200 OK 2.32 s 414 B Save Response

Pretty Raw Preview Visualize JSON 🔍

```
1  |
2  |   "code": "Success",
3  |   "message": "Successfully Completed Request",
4  |   "@Message.ExtendedInfo": [
5  |     {
6  |       "@odata.type": "Message.v1_2_0.Message",
7  |       "MessageId": "ManagerAccount",
8  |       "Message": "Successfully Completed Request",
9  |       "Severity": "OK",
10 |       "MessageSeverity": "OK",
11 |       "Resolution": "User deleted sucesfully"
12 |     }
13 |   ]
14 |
```

4. Add User Roles:

METHOD: POST

URL – <https://{pdu-ip}/redfish/v1/AccountService/Roles>

Payload:

```
{  
  "Id": "Administrator", "Description": "LDAPs user", "Name": "LDAP Admin"  
}
```

Note – “Id” defines the privileges of the role, here there are two types of Administrator for Admin and Read Only for “user”.

Success response:

```
{  
  "code": "Success",  
  "message": "Successfully Completed Request", "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "User Role",  
      "Message": "Successfully Completed Request", "Severity": "OK",  
      "MessageSeverity": "OK", "Resolution": "NONE"  
    }  
  ]  
}
```

Curl Command

```
curl -location 'https://{pdu-ip}/redfish/v1/AccountService/Roles' \  
-header 'X-Auth-Token: 786707833' \  
-header 'Content-Type: application/json' \  
-data '{  
  "Id": "Administrator", "Description": "nmc user", "Name": "NMC"  
}'
```

https://10.10.105.22/redfish/v1/AccountService/Roles Save

POST Send https://10.10.105.22/redfish/v1/AccountService/Roles

Params Authorization Headers (9) **Body** Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary **JSON** Beautifuly

```
1 {
2   "Id": "Administrator",
3   "Description": "LDAPs user",
4   "Name": "Ldap Admin"
5 }
6
7
```

Body Cookies Headers (4) Test Results Status: 201 Created Time: 17.28 s Size: 394 B Save Response

Pretty Raw Preview Visualize **JSON** Search

```
1 {
2   "code": "Success",
3   "message": "Successfully Completed Request",
4   "@Message.ExtendedInfo": [
5     {
6       "@odata.type": "Message.v1_2_0.Message",
7       "MessageId": "User Role",
8       "Message": "Successfully Completed Request",
9       "Severity": "OK",
10      "MessageSeverity": "OK",
11      "Resolution": "NONE"
12    }
13  ]
14 }
```

Parameter Errors and Resolution Messages

a. Json Payload Error:

URL – <https://{pdu-ip}/redfish/v1/AccountService/Roles>

Payload:

```
{
  "Id": "ReadOnly", "Description": "LDAPs user", "Name": "LDAP User"
}
```

Success response:

```
{
  "code": "JSON data Error",
  "message": "Failed to load JSON database", "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "User Role",
      "Message": "Failed to load JSON database", "Severity": "Warning",
      "MessageSeverity": "Warning",
      "Resolution": "JSON unpack error, Enter the valid JSON packet"
    }
  ]
}
```

b. User Privilege Error:

```
{
  "code": "User Privilege Error", "message": "Privilege Error", "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "User Role", "Message":
      "Privilege Error", "Severity": "Warning", "MessageSeverity": "Warning", "Resolution": "User
      Don't have valid Privilege to configure the system"
    }
  ]
}
```

5. Edit Roles:

URL – <https://{pdu-ip}/redfish/v1/AccountService/Roles>

POST METHOD

Payload:

```
{  
  "Id": "Administrator", "Description": "LDAPs user", "Name": "LDAP Admin"  
}
```

Success response:

```
{  
  "code": "Success",  
  "message": "Successfully Completed Request", "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "User Role",  
      "Message": "Successfully Completed Request", "Severity": "OK",  
      "MessageSeverity": "OK", "Resolution": "NONE"  
    }  
  ]  
}
```

Curl Command:

```
curl -location --request PATCH  
'https://{pdu-ip}/redfish/v1/AccountService/Roles' \  
-header 'X-Auth-Token: 786707833' \  
-header 'Content-Type: application/json' \  
-data '{ "Id": "Administrator",  
  "Description": "nmc use", "Name": "NMC"  
}'
```

Parameter Errors and Resolution Messages

User Role Does Not Exist:

```
{  
  "code": "Data Error",  
  "message": " User information not found", "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "User Role",  
      "Message": " User information not found", "Severity": "Warning",  
      "MessageSeverity": "Warning", "Resolution": "UserRole not existed"  
    }  
  ]  
}
```

HTTP <https://10.10.105.244/redfish/v1/AccountService/Roles> Save

PATCH <https://10.10.105.244/redfish/v1/AccountService/Roles> Send

Params Authorization Headers (9) **Body** Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary **JSON** Beautify

```
1 {
2   "Id": "Administrator",
3   "Description": "nmc-use",
4   "Name": "NMC"
5 }
```

Body Cookies Headers (4) Test Results 201 Created 2.19 s 394 B Save Response

Pretty Raw Preview Visualize **JSON** 🔍

```
1 {
2   "code": "Success",
3   "message": "Successfully Completed Request",
4   "@Message.ExtendedInfo": [
5     {
6       "@odata.type": "Message.v1_2_0.Message",
7       "MessageId": "User Role",
8       "Message": "Successfully Completed Request",
9       "Severity": "OK",
10      "MessageSeverity": "OK",
11      "Resolution": "NONE"
12     }
13   ]
14 }
```

6. Delete User:

METHOD : DELETE

URL – <https://{pdu-ip}/redfish/v1/AccountService/Roles>

Payload:

```
{  
  "Name": "LDAP Admin"  
}
```

Success response:

```
{  
  "code": "Success",  
  "message": "Successfully Completed Request", "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "User Role",  
      "Message": "Successfully Completed Request", "Severity": "OK",  
      "MessageSeverity": "OK", "Resolution": "NONE"  
    }  
  ]  
}
```

Curl Command:

```
curl -location --request DELETE  
'https://{pdu-ip}/redfish/v1/AccountService/Roles' \  
-header 'X-Auth-Token: 786707833' \  
-header 'Content-Type: application/json' \  
-data  
{  
  "Name": "NMC"  
}
```


HTTP <https://10.10.105.244/redfish/v1/AccountService/Roles> Save

DELETE ▼ | <https://10.10.105.244/redfish/v1/AccountService/Roles> Send ▼

Params Authorization Headers (9) **Body** ● Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary **JSON** ▼ Beautify

```
1
2  ... "Name": "NMC"
3
```

Body Cookies Headers (4) Test Results 200 OK 2.00 s 389 B Save Response ▼

Pretty Raw Preview Visualize **JSON** ▼ 🔍

```
1
2  "code": "Success",
3  "message": "Successfully Completed Request",
4  "@Message.ExtendedInfo": [
5    {
6      "@odata.type": "Message.v1_2_0.Message",
7      "MessageId": "User Role",
8      "Message": "Successfully Completed Request",
9      "Severity": "OK",
10     "MessageSeverity": "OK",
11     "Resolution": "NONE"
12   }
13 ]
14
```

Parameter Errors and Resolution Messages

d. User Role Does Not Exist:

```
{
  "code": "Data Error",
  "message": "User information not found", "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "User Role",
      "Message": "User information not found", "Severity": "Warning",
      "MessageSeverity": "Warning", "Resolution": "UserRole is not existed"
    }
  ]
}
```

7. Outlet Control:

METHOD: POST

URL – <https://{pdu-ip}/redfish/v1/PowerEquipment/RackPDUs/{pdu-id}/Outlets/OUTLET{outlet-number}/Action/Outlet.PowerControl>

Payload:

```
{
  "PowerState": "Off"
}
```

Other values can be specified : PoweringOff ,PoweringOn
,PowerCycle ,RebootDelay

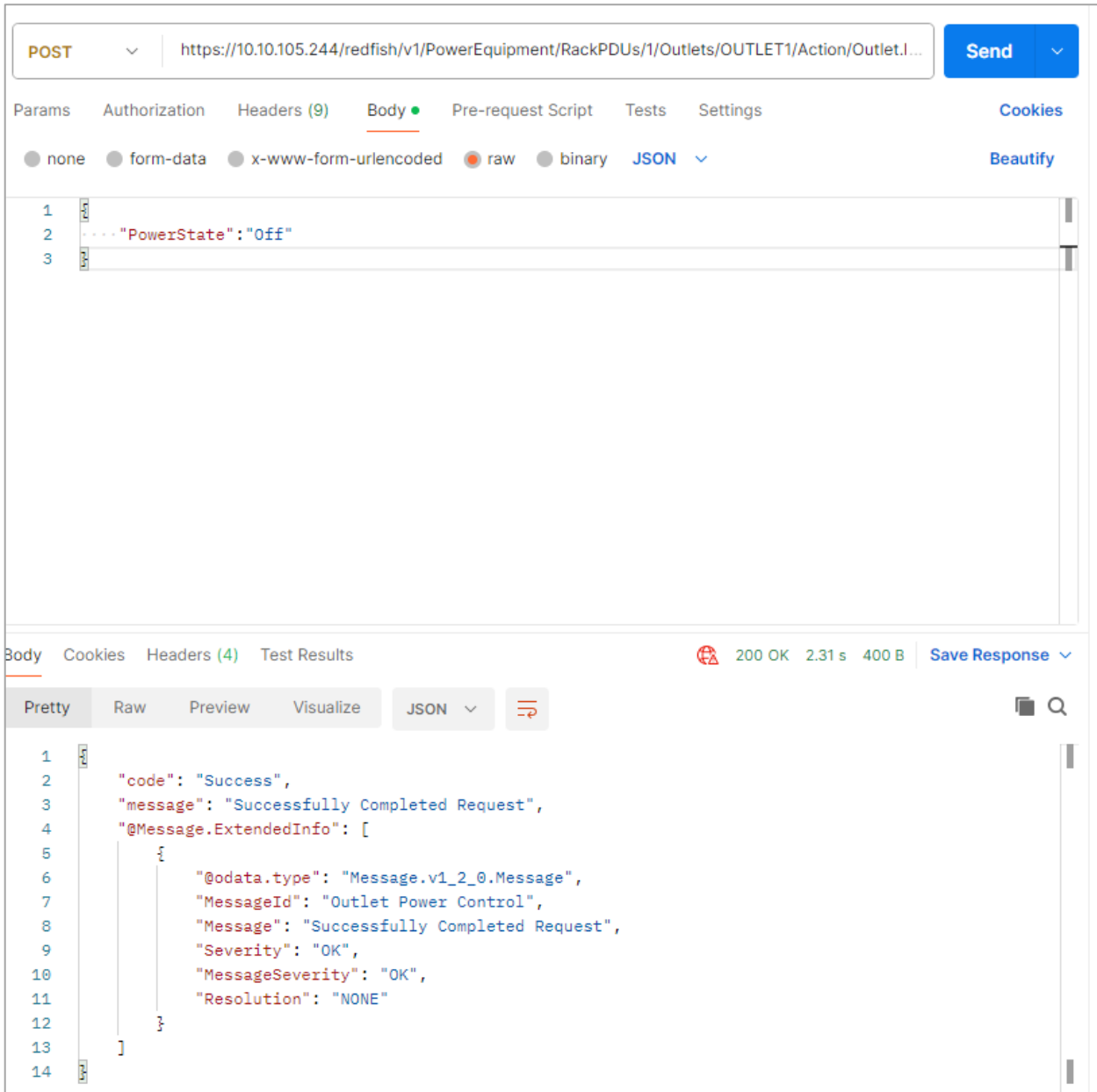
Success Response:

```
{
  "code": "Success",
  "message": "Successfully Completed Request", "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "Outlet Power Control", "Message":
      "Successfully Completed Request", "Severity": "OK",
      "MessageSeverity": "OK", "Resolution": "NONE"
    }
  ]
}
```

Curl Command:

```
curl -location
```

```
'https://{pdu-ip}/redfish/v1/PowerEquipment/RackPDUs/1/ Outlets/OUTLET1/Action/Outlet.PowerControl' \
--header 'X-Auth-Token: 786707833' \
--header 'Content-Type: application/json' \
--data '{ "PowerState": "Off"
}
```



Parameter Errors and Resolution Messages

a. If Outlet Control is disabled:

```
{
"code": "ManagerAccount", "message": "Method Not Allowed", "@Message.ExtendedInfo":
[
{
```

```

"@odata.type": "Message.v1_2_0.Message", "MessageId": "Outlet Power Control",
"Message": "Method Not Allowed", "Severity": "Warning", "MessageSeverity": "Warning",
"Resolution": "Outlet control flag is disabled"
}
]
}

```

b. Wrong Outlet Number:

```

{
"code": "URL Error", "message": "Invalid URL", "@Message.ExtendedInfo": [
{
"@odata.type": "Message.v1_2_0.Message", "MessageId": "Outlet Power Control", "Message": "Invalid
URL",
"Severity": "Warning", "MessageSeverity": "Warning",
"Resolution": "Query with valid URL, Invalid Outlet ID"
}
]
}

```

8. Configure an Outlet:

METHOD: PATCH

URL - <https://{pdu-ip}/redfish/v1/PowerEquipment/RackPDUs/{pdu-id}/Outlets/OUTLET{outlet-number}/Action/Outlet.ResetMetrics>

Payload:

```

{
  "PowerOnDelaySeconds":11,
  "PowerOffDelaySeconds":22,
  "PowerRestoreDelaySeconds":33,
  "PowerState": "LastState",
  "Name": "ira1"
}

```

Value Range

On Delay(0-7200s), Off Delay(0-7200s), Reboot Duration(0-60s)
 PowerState=on,off,lastknown

Success Response:

```

{
"code": "Success",
"message": "Successfully Completed Request",
"@Message.ExtendedInfo": [
{
"@odata.type": "Message.v1_2_0.Message",
"MessageId": "Outlet Reset Metrics",
"Message": "PowerOnDelaySeconds information Updated",

```

```

    "Severity": "None",
    "MessageSeverity": "None",
    "Resolution": ""
  },
  {
    "@odata.type": "Message.v1_2_0.Message",
    "MessageId": "Outlet Reset Metrics",
    "Message": "PowerOffDelaySeconds information Updated",
    "Severity": "None",
    "MessageSeverity": "None",
    "Resolution": ""
  },
  {
    "@odata.type": "Message.v1_2_0.Message",
    "MessageId": "Outlet Reset Metrics",
    "Message": "PowerRestoreDelaySeconds information Updated",
    "Severity": "None",
    "MessageSeverity": "None",
    "Resolution": ""
  },
  {
    "@odata.type": "Message.v1_2_0.Message",
    "MessageId": "Outlet Reset Metrics",
    "Message": "PowerState information Updated",
    "Severity": "None",
    "MessageSeverity": "None",
    "Resolution": ""
  },
  {
    "@odata.type": "#Outlet.v1_4_1.Outlet",
    "MessageId": "Outlet Reset Metrics",
    "Message": "Outlet name information Updated",
    "Severity": "None",
    "MessageSeverity": "None",
    "Resolution": ""
  },
  {
    "@odata.type": "#Outlet.v1_4_1.Outlet",
    "MessageId": "Outlet Reset Metrics",
    "Message": "Successfully Completed Request",
    "Severity": "OK",
    "MessageSeverity": "OK",
    "Resolution": ""
  }
]
}

```

Curl Command:

```
curl -location --request PATCH 'https:// {pdu-
ip}/redfish/v1/PowerEquipment/RackPDUs/1/Outlets/OUTLET1/Action/Outlet.ResetMetrics' \
```

```

--header 'X-Auth-Token: 786707833' \
--header 'Content-Type: application/json' \
--data '{
  "PowerOnDelaySeconds":11,
  "PowerOffDelaySeconds":22,
  "PowerRestoreDelaySeconds":33,
  "PowerState": "LastState",
  "Name": "ira1"
}'

```

The screenshot shows a REST client interface with the following details:

- URL:** `https://10.10.106.37/redfish/v1/PowerEquipment/RackPDUs/1/Outlets/OUTLET1/Action/Outlet.ResetMetrics`
- Method:** PATCH
- Request Body (JSON):**

```

{
  "PowerOnDelaySeconds":11,
  "PowerOffDelaySeconds":22,
  "PowerRestoreDelaySeconds":33,
  "PowerState": "LastState",
  "Name": "ira1"
}

```
- Response Status:** 200 OK, 2.92 s, 1.35 KB
- Response Body (JSON):**

```

{
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Outlet Reset Metrics",
      "Message": "PowerOnDelaySeconds information Updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": ""
    },
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Outlet Reset Metrics",
      "Message": "PowerOffDelaySeconds information Updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": ""
    },
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Outlet Reset Metrics",
      "Message": "PowerRestoreDelaySeconds information Updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": ""
    }
  ]
}

```

Parameter Errors and Resolution Messages

- a. Wrong PDU ID In URL:

```
{  
"code": "URL Error", "message": "Invalid URL", "@Message.ExtendedInfo": [  
{  
"@odata.type": "Message.v1_2_0.Message", "MessageId": "Outlet Reset Metrics", "Message":  
"Invalid URL",  
"Severity": "Warning", "MessageSeverity": "Warning",  
"Resolution": "Query with valid URL, Invalid PDU Number"  
}  
]
```

- b. Wrong PDU Outlet ID In URL:

```
{  
"code": "URL Error",  
"message": "Invalid URL",  
"@Message.ExtendedInfo": [  
{  
"@odata.type": "Message.v1_2_0.Message",  
"MessageId": "Outlet Reset Metrics",  
"Message": "Invalid URL",  
"Severity": "Warning",  
"MessageSeverity": "Warning",  
"Resolution": "Query with valid URL, Invalid Outlet ID"  
}  
]  
}
```

9. Reset a PDU:

METHOD: POST

URL – <https://{pdu-ip}/redfish/v1/Managers/1/Actions/Manager.Reset>

Payload:

```
{  
  "ResetType": "ForceRestart"  
}
```

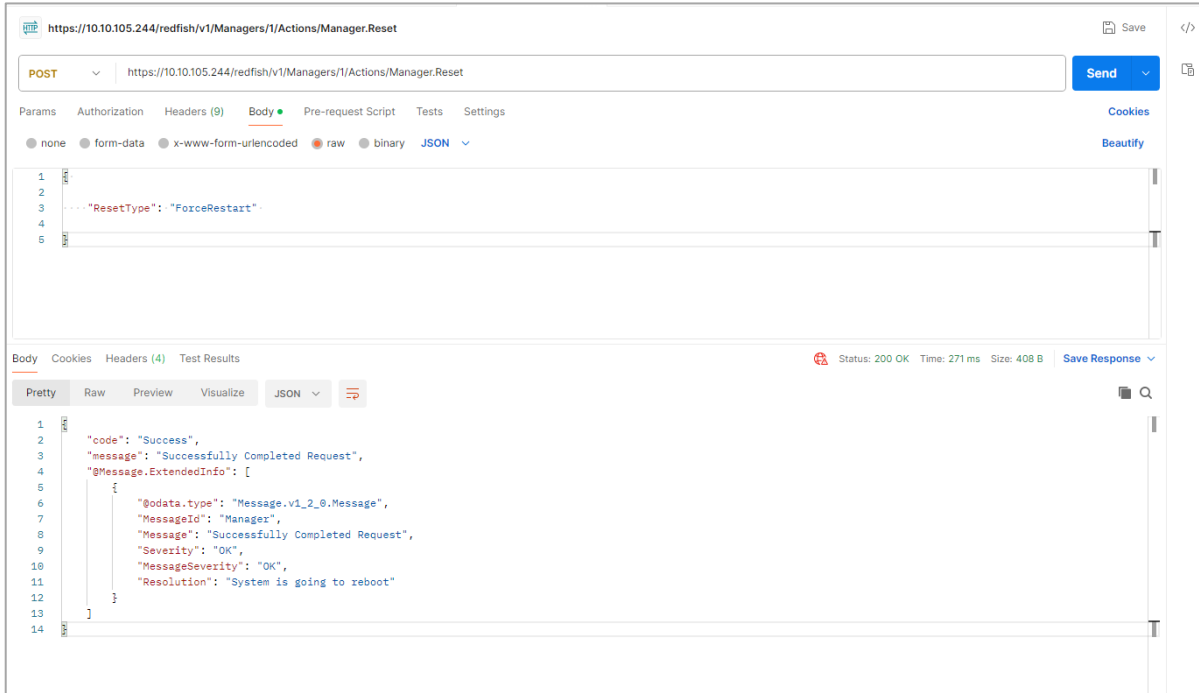
Curl Command:

```
curl --location  
'https://{pdu-ip}/redfish/v1/Managers/1/Actions/Manager.Reset' \  
-header 'X-Auth-Token: 821985700' \  
-header 'Content-Type: application/json' \  
-data '{  
  "ResetType": "ForceRestart"  
}'
```

Success Response:

```
{  
  "code": "Success",  
  "message": "Successfully Completed Request", "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message", "MessageId": "Manager",  
      "Message": "Successfully Completed Request", "Severity": "OK",  
      "MessageSeverity": "OK",  
      "Resolution": "System is going to reboot"  
    }  
  ]  
}
```


}



Parameter Errors and Resolution Messages

a. Authorization Error:

```
{
  "code": "User Privilege Error",
  "message": "Privilege Error",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Manager",
      "Message": "Privilege Error",
      "Severity": "Warning",
      "MessageSeverity": "Warning",
      "Resolution": "Token not authorized"
    }
  ]
}
```

b. Wrong Payload:

```
{
  "code": "JSON data Error",
  "message": "Failed to load JSON database",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Manager",
      "Message": "Failed to load JSON database",

```

```
"Severity": "Warning",
"MessageSeverity": "Warning",
"Resolution": "JSON unpack error, Enter the valid JSON packet"
}
]
}
```

10.

11. Static IPv4 Configuration:

METHOD: PATCH

URL – <https://{pdu-ip}/redfish/v1/Managers/1/EthernetInterfaces>

Payload: for eth0

```
{
  "IPv4StaticAddresses": [
    {
      "Address": "10.10.106.107",
      "SubnetMask": "255.255.252.0",
      "Gateway": "10.10.104.254"
    }
  ]
}
```

Success Response:

```
{
  "code": "Success",
  "message": "Ethernet configuration is updated, System is going to reboot",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "IPv4 Configuration",
      "Message": "Static IPv4 Port 1 Configuration updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": ""
    },
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Ethernet Interface configuration",
      "Message": "Ethernet configuration is updated, System is going to reboot",
      "Severity": "OK",
      "MessageSeverity": "OK",
      "Resolution": ""
    }
  ]
}
```

Curl Command:

```
curl -location --request PATCH 'https://{pdu-ip}/redfish/v1/Managers/1/EthernetInterfaces' \  
--header 'X-Auth-Token: 100603786' \  
--header 'Content-Type: application/json' \  
--data '{  
  "IPv4StaticAddresses": [  
    {  
      "Address": "10.10.105.244",  
      "SubnetMask": "255.255.252.0",  
      "Gateway": "10.10.104.254"  
    }  
  ]  
}'
```

The screenshot shows a REST client interface with the following details:

- URL:** `https://10.10.105.244/redfish/v1/Managers/1/EthernetInterfaces`
- Method:** PATCH
- Request Body (JSON):**

```
{  
  "IPv4StaticAddresses": [  
    {  
      "Address": "10.10.105.244",  
      "SubnetMask": "255.255.252.0",  
      "Gateway": "10.10.104.254"  
    }  
  ]  
}
```
- Status:** 200 OK, Time: 123 ms, Size: 666 B
- Response Body (JSON):**

```
{  
  "code": "Success",  
  "message": "Ethernet configuration is updated, System is going to reboot",  
  "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message",  
      "MessageId": "IPv4 Configuration",  
      "Message": "Static IPv4 Port 1 Configuration updated",  
      "Severity": "None",  
      "MessageSeverity": "None",  
      "Resolution": ""  
    },  
    {  
      "@odata.type": "Message.v1_2_0.Message",  
      "MessageId": "Ethernet Interface configuration",  
      "Message": "Ethernet configuration is updated, System is going to reboot",  
      "Severity": "OK",  
      "MessageSeverity": "OK",  
      "Resolution": ""  
    }  
  ]  
}
```

Payload: for eth0 and eth1

```
{
  "IPv4StaticAddresses": [
    {
      "Address": "10.10.106.107",
      "SubnetMask": "255.255.252.0",
      "Gateway": "10.10.104.254"
    },
    {
      "Address": "0.0.0.0",
      "SubnetMask": "255.255.252.0",
      "Gateway": "10.10.104.254"
    }
  ]
}
```

Success Response:

```
{
  "code": "Success",
  "message": "Ethernet configuration is updated, System is going to reboot",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "IPv4 Configuration",
      "Message": "Static IPv4 Port 1 Configuration updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": ""
    },
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "IPv4 Configuration",
      "Message": "Static IPv4 Port 2 Configuration updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": ""
    },
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Ethernet Interface configuration",
      "Message": "Ethernet configuration is updated, System is going to reboot",
      "Severity": "OK",
      "MessageSeverity": "OK",
      "Resolution": ""
    }
  ]
}
```

Curl Command:

```
curl -location --request PATCH 'https://{pdu-ip}/redfish/v1/Managers/1/EthernetInterfaces' \  
--header 'X-Auth-Token: 100603786' \  
--header 'Content-Type: application/json' \  
--data '{  
  "IPv4StaticAddresses": [  
    {  
      "Address": "10.10.105.244",  
      "SubnetMask": "255.255.252.0",  
      "Gateway": "10.10.104.254"  
    },  
    {  
      "Address": "0.0.0.0",  
      "SubnetMask": "255.255.252.0",  
      "Gateway": "10.10.104.254"  
    }  
  ]  
}'
```

The screenshot shows a Postman interface for a PATCH request to the endpoint `https://10.10.105.244/redfish/v1/Managers/1/EthernetInterfaces`. The request body is a JSON array of IPv4 static addresses. The response status is 200 OK, and the response body is a JSON object with a success code and two messages indicating that the configuration was updated and the system is going to reboot.

```
1  PATCH https://10.10.105.244/redfish/v1/Managers/1/EthernetInterfaces  
2  {  
3    "IPv4StaticAddresses": [  
4      {  
5        "Address": "10.10.105.244",  
6        "SubnetMask": "255.255.252.0",  
7        "Gateway": "10.10.104.254"  
8      },  
9      {  
10       "Address": "0.0.0.0",  
11       "SubnetMask": "255.255.252.0",  
12       "Gateway": "10.10.104.254"  
13     }  
14   ]  
15 }  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000
```

Parameter Errors and Resolution Messages

a. Wrong URL:

```
{
  "code": "Failed",
  "message": "Invalid URL",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Ethernet Interface configuration",
      "Message": "Invalid URL",
      "Severity": "Warning",
      "MessageSeverity": "Warning",
      "Resolution": "Query with valid URL"
    }
  ]
}
```

12. Static IPv6 Configuration:

METHOD: PATCH

URL – <https://{pdu-ip}/redfish/v1/Managers/1/EthernetInterfaces>

Payload: for eth0 and eth1

```
{
  "IPv6StaticAddresses": [
    {
      "Address": "2001:c0a8:aa01:0:b96a:7e59:c9ac:aac4",
      "PrefixLength": 64
    },
    {
      "Address": "2001:c0a8:aa01::855",
      "PrefixLength": 64
    }
  ],
  "IPv6StaticDefaultGateways": [
    {
      "Address": "fe80::1ab1:69ff:fed3:abbc",
      "PrefixLength": 64
    },
    {
      "Address": "fe80::1ab1:69ff:fed3:abbc",
      "PrefixLength": 64
    }
  ]
}
```

Success Response:

```
{
  "code": "Success",
  "message": "Ethernet configuration is updated, System is going to reboot",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "IPv6 Configuration",
      "Message": "Static IPv6 Port 1 Configuration updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": ""
    },
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "IPv6 Configuration",
      "Message": "Static IPv6 Port 2 Configuration updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": ""
    },
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Ethernet Interface configuration",
      "Message": "Ethernet configuration is updated, System is going to reboot",
      "Severity": "OK",
      "MessageSeverity": "OK",
      "Resolution": ""
    }
  ]
}
```

Curl Command:

```
curl -location --request PATCH 'https://{pdu-ip}/redfish/v1/Managers/1/EthernetInterfaces' \
--header 'X-Auth-Token: 364319529' \
--header 'Content-Type: application/json' \
--data '{
  "IPv6StaticAddresses": [
    {
      "Address": "2001:c0a8:aa01::1c1",
      "PrefixLength": 64
    },
    {
      "Address": "2001:c0a8:aa01::855",
      "PrefixLength": 64
    }
  ],
  "IPv6StaticDefaultGateways": [
    {
      "Address": "fe80::1ab1:69ff:fed3:abbc",
      "PrefixLength": 64
    },
    {
```

```
}
  "Address": "fe80::1ab1:69ff:fed3:abbc",
  "PrefixLength": 64
}
]
```

The screenshot displays a REST client interface for a PATCH request to `https://10.10.105.244/redfish/v1/Managers/1/EthernetInterfaces`. The request body is a JSON array of IPv6 static addresses. The response is a JSON object indicating success and providing detailed messages for each configuration update.

Request Body (JSON):

```
1  [
2    {
3      "Address": "2001:c0a8:aa01::1c1",
4      "PrefixLength": 64
5    },
6    {
7      "Address": "2001:c0a8:aa01::855",
8      "PrefixLength": 64
9    }
10 ]
11
12 "IPv6StaticDefaultGateways": [
13   {
14     "Address": "fe80::1ab1:69ff:fed3:abbc",
15     "PrefixLength": 64
16   }
17 ]
```

Response Body (JSON):

```
1  {
2    "code": "Success",
3    "message": "Ethernet configuration is updated, System is going to reboot",
4    "@Message.ExtendedInfo": [
5      {
6        "@odata.type": "Message.v1_2_0.Message",
7        "MessageId": "IPv6 Configuration",
8        "Message": "Static IPv6 Port 1 Configuration updated",
9        "Severity": "None",
10       "MessageSeverity": "None",
11       "Resolution": ""
12     },
13     {
14       "@odata.type": "Message.v1_2_0.Message",
15       "MessageId": "IPv6 Configuration",
16       "Message": "Static IPv6 Port 2 Configuration updated",
17       "Severity": "None",
18       "MessageSeverity": "None",
19       "Resolution": ""
20     }
21   ]
22 }
```

Status: 200 OK Time: 2.59 s Size: 864 B

13. NTP Configuration:

METHOD: PATCH

URL – <https://{pdu-ip}/redfish/v1/Managers/1/NetworkProtocol>

Payload:

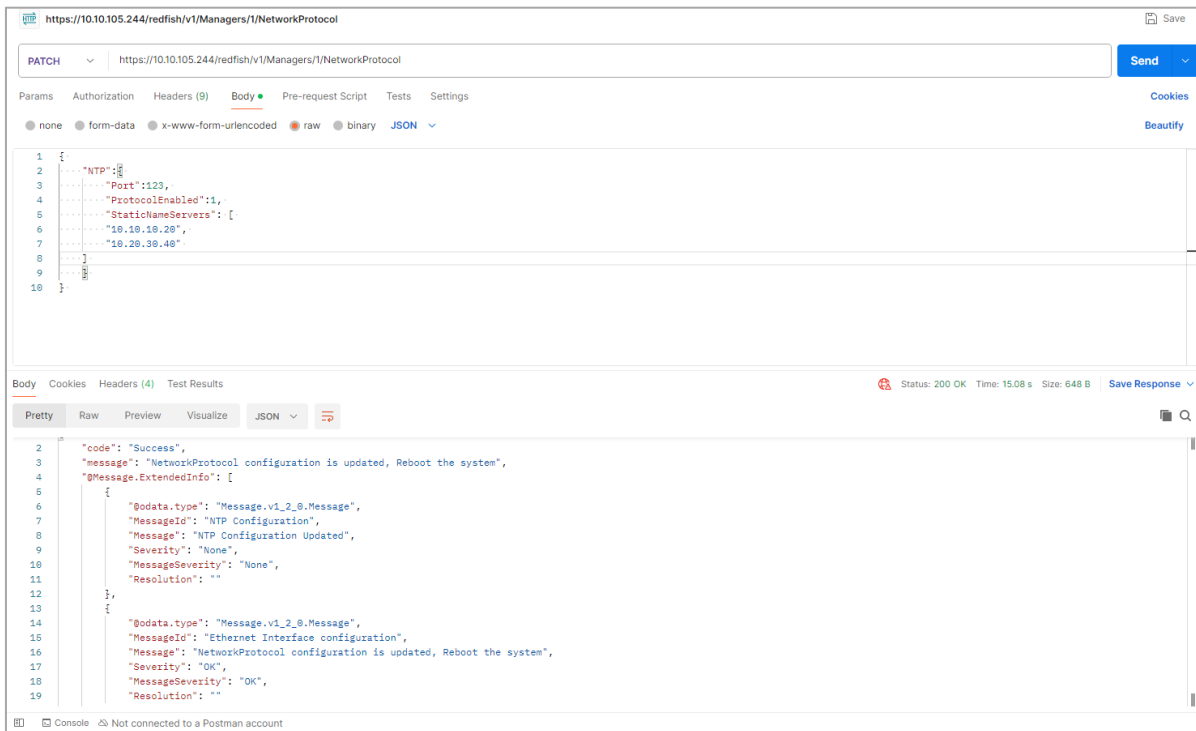
```
{
  "NTP":{
    "Port":123,
    "ProtocolEnabled":1,
    "StaticNameServers": [
      "10.10.10.20",
      "10.20.30.40"
    ]
  }
}
```

Success Response:

```
{
  "code": "Success",
  "message": "Ethernet configuration is updated, System is going to reboot",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "NTP Configuration",
      "Message": "NTP Configuration Updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": ""
    },
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Ethernet Interface configuration",
      "Message": "Ethernet configuration is updated, System is going to reboot",
      "Severity": "OK",
      "MessageSeverity": "OK",
      "Resolution": ""
    }
  ]
}
```

Curl Command:

```
curl --location --request PATCH 'https://{pdu-ip}/redfish/v1/Managers/1/NetworkProtocol' \  
--header 'X-Auth-Token: 364319529' \  
--header 'Content-Type: application/json' \  
--data '{  
  "NTP":{  
    "Port":123,  
    "ProtocolEnabled":1,  
    "StaticNameServers": [  
      "10.10.10.20",  
      "10.20.30.40"  
    ]  
  }  
}'
```



14. SNMP V3 Users Configuration:

METHOD: PATCH/POST

URL – <https://{pdu-ip}/redfish/v1/AccountService/Accounts>

Note: To add the user for the first time, use the post request. After adding, use the patch request to amend.

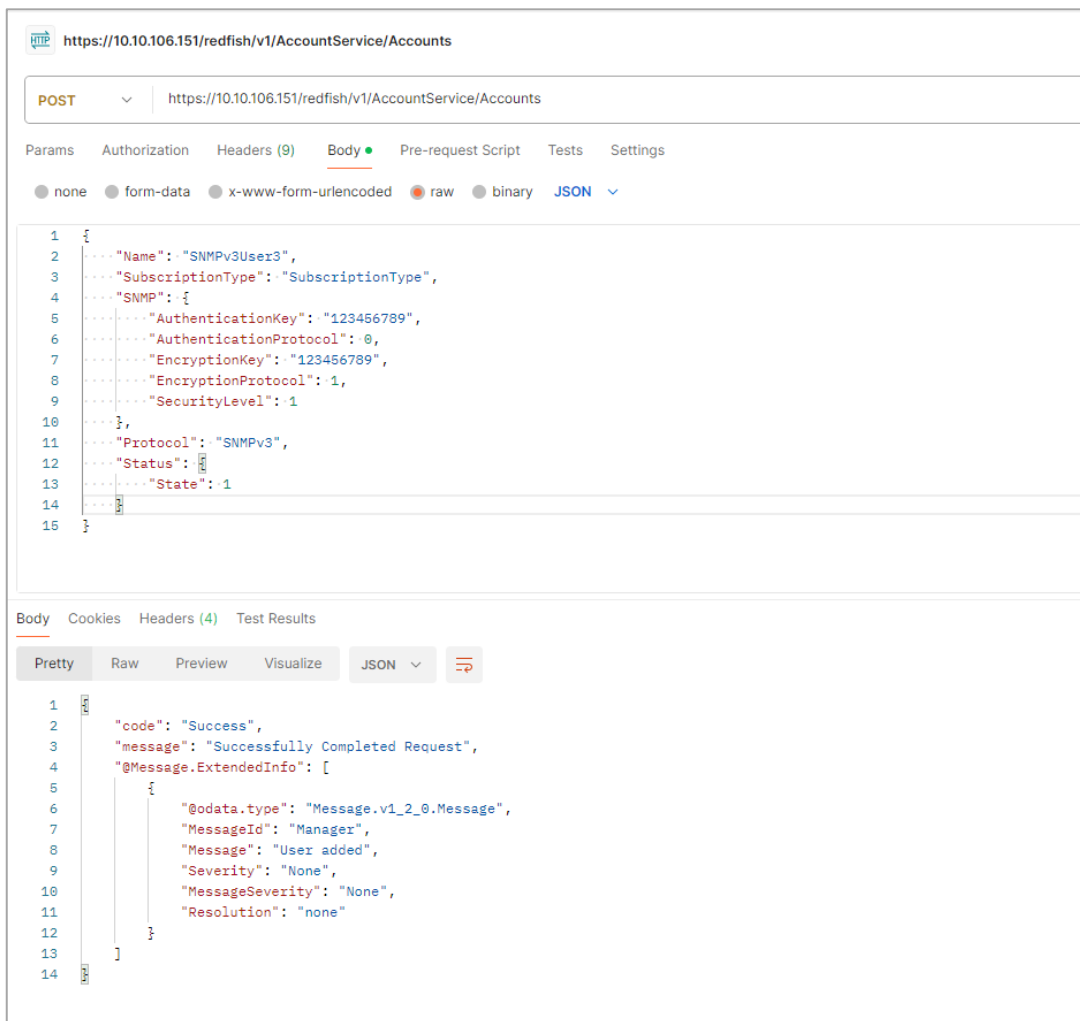
Payload is same for editing

Payload:

```
{
  "Name": "SNMPv3User3",
  "SubscriptionType": "SubscriptionType",
  "SNMP": {
    "AuthenticationKey": "123456789",
    "AuthenticationProtocol": 0,
    "EncryptionKey": "123456789",
    "EncryptionProtocol": 1,
    "SecurityLevel": 1
  },
  "Protocol": "SNMPv3",
  "Status": {
    "State": 0
  }
}
```

Success Response body Post:

```
{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Manager",
      "Message": "User added",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": "none"
    }
  ]
}
```



Curl Command:

```

curl -location 'https://{pdu-ip}/redfish/v1/AccountService/Accounts' \
--header 'X-Auth-Token: 1681692777' \
--header 'Content-Type: application/json' \
--data '{
  "Name": "SNMPv3User3",
  "SubscriptionType": "SubscriptionType",
  "SNMP": {
    "AuthenticationKey": "123456789",
    "AuthenticationProtocol": 0,
    "EncryptionKey": "123456789",
    "EncryptionProtocol": 1,
    "SecurityLevel": 1
  },
  "Protocol": "SNMPv3",
  "Status": {
    "State": 1
  }
}'

```

Success Response for Patch:

```
{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Manager",
      "Message": "User information updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": "none"
    }
  ]
}
```

Curl Command:

```
curl -location --request PATCH 'https://{pdu-ip}///redfish/v1/AccountService/Accounts' \
--header 'X-Auth-Token: 1681692777' \
--header 'Content-Type: application/json' \
--data '{
  "Name": "SNMPv3User3",
  "SubscriptionType": "SubscriptionType",
  "SNMP": {
    "AuthenticationKey": "123456789",
    "AuthenticationProtocol": 0,
    "EncryptionKey": "123456789",
    "EncryptionProtocol": 1,
    "SecurityLevel": 1
  },
  "Protocol": "SNMPv3",
  "Status": {
    "State": 0
  }
}'
```

Payload For Delete:

```
{
  "Name": "SNMPv3User3",
  "Protocol": "SNMPv3"
}
```

Success Response for Delete:

```
{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
```

```

{
  "@odata.type": "Message.v1_2_0.Message",
  "MessageId": "Manager",
  "Message": "User Deleted",
  "Severity": "None",
  "MessageSeverity": "None",
  "Resolution": "none"
}
]
}

```

Curl Command:

```

curl -location --request DELETE 'https://{pdu-ip}/redfish/v1/AccountService/Accounts' \
--header 'X-Auth-Token: 1794027639' \
--header 'Content-Type: application/json' \
--data '{
  "Name": "snmpv3user3",
  "Protocol": "SNMPv3"
}'

```

The screenshot displays a REST client interface for the endpoint `https://10.10.105.244/redfish/v1/AccountService/Accounts`. The request method is `DELETE` and the body is set to `JSON`. The request body contains the following JSON:

```

{
  "Name": "snmpv3user3",
  "Protocol": "SNMPv3"
}

```

The response status is `200 OK` with a time of `1338 ms` and a size of `373 B`. The response body is shown in `JSON` format and contains the following JSON:

```

{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Manager",
      "Message": "User Deleted",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": "none"
    }
  ]
}

```

15. SNMP V1/2 Users Configuration:

METHOD: PATCH/POST

URL – <https://{pdu-ip}/redfish/v1/Managers/1>

Payload:

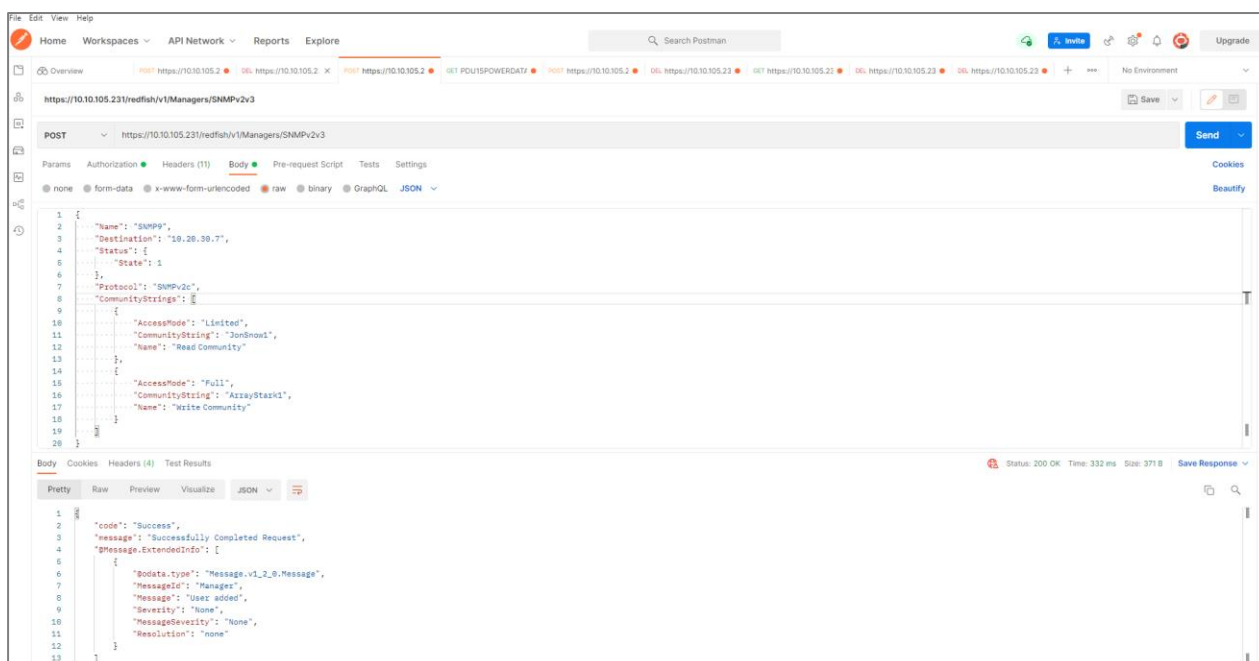
```
{
  "Name": "SNMP9",
  "Destination": "10.20.30.7",
  "Status": {
    "State": 1
  },
  "Protocol": "SNMPv2c",
  "CommunityStrings": [
    {
      "AccessMode": "Limited",
      "CommunityString": "JonSnow1",
      "Name": "Read Community"
    },
    {
      "AccessMode": "Full",
      "CommunityString": "ArrayStark1",
      "Name": "Write Community"
    }
  ]
}
```

Success Response for Post:

```
{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Manager",
      "Message": "User added",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": "none"
    }
  ]
}
```

Curl Command:

```
curl -location --request POST 'https://{pdu-ip}/redfish/v1/Managers/SNMPv2v3' \  
--header 'X-Auth-Token: 1804289383' \  
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
  "Name": "SNMP9",  
  "Destination": "10.20.30.7",  
  "Status": {  
    "State": 1  
  },  
  "Protocol": "SNMPv2c",  
  "CommunityStrings": [  
    {  
      "AccessMode": "Limited",  
      "CommunityString": "JonSnow1",  
      "Name": "Read Community"  
    },  
    {  
      "AccessMode": "Full",  
      "CommunityString": "ArrayStark1",  
      "Name": "Write Community"  
    }  
  ]  
}'
```



Success Response for Patch:

```
{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Manager",
      "Message": "User information Updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": "none"
    }
  ]
}
```

Curl Command:

```
curl -location --request PATCH 'https://{pdu-ip}/redfish/v1/Managers/SNMPv2v3'\
--header 'X-Auth-Token: 1659861792' \
--header 'Content-Type: application/json' \
--data '{"Name":"snmp9","Destination":"10.20.30.8","Status":{"State":0},"Protocol":"SNMPv2c",
"CommunityStrings":[{"
  "AccessMode":"Limited",
  "CommunityString":"Jonsnow1",
  "Name":"Read Community"
}],
{
  "AccessMode":"Full",
  "CommunityString":"ArrayStark1",
  "Name":"Write Community"
}
]}'
```

Payload For Delete:

```
{
  "Name":"SNMP9",
  "Protocol":"SNMPv2c"
}
```

Success Response for Delete:

```
{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
```

```
    "MessageId": "Manager",
    "Message": "User Deleted",
    "Severity": "None",
    "MessageSeverity": "None",
    "Resolution": "none"
  }
]
```

Curl Command:

```
curl --location --request DELETE 'https://{pdu-ip}/redfish/v1/Managers/SNMPv2v3' \
--header 'X-Auth-Token: 1804289383' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \
--header 'Content-Type: application/json' \
--data-raw '{
  "Name": "SNMP9",
  "Protocol": "SNMPv2c"
}'
```

The screenshot shows a REST client interface for a DELETE request to `https://10.10.105.231/redfish/v1/Managers/SNMPv2v3`. The request body is a JSON object: `{ "Name": "SNMP9", "Protocol": "SNMPv2c" }`. The response status is 200 OK, and the response body is a JSON object: `{ "code": "Success", "message": "Successfully Completed Request", "messageExtendedInfo": [{ "odata.type": "Message-v1_2_0.Message", "messageId": "Manager", "message": "User Deleted", "severity": "None", "messageSeverity": "None", "resolution": "none" }] }`.

16. SNMP Trap Configuration:

METHOD: PATCH/POST

URL – <https://{pdu-ip}/redfish/v1/EventService/Subscriptions>

17. SNMP Trap V1/2 Trap Configuration Payload :

```
{
  "Name": "SNMP3",
  "Destination": "192.168.1.49",
  "SubscriptionType": "SNMPTrap",
  "SNMP": {
    "TrapCommunity": "hello"
  },
  "Status": {
    "State": 1
  },
  "Context": "WebUser2",
  "Protocol": "SNMPv2c"
}
```

Success Response Body For Post :

```
{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Manager",
      "Message": "User added",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": "none"
    }
  ]
}
```

Curl Command:

```
curl -location 'https://{pdu-ip}/redfish/v1/EventService/Subscriptions' \
--header 'X-Auth-Token: 1790411260' \
--header 'Content-Type: application/json' \
--data '{"Name": "SNMP3", "Destination": "192.168.1.49", "SubscriptionType": "SNMPTrap",
"SNMP": {"TrapCommunity": "hello"},
"Status": {"State": 1},
"Context": "WebUser2",
"Protocol": "SNMPv2c"
}'
```

https://10.10.105.244/redfish/v1/EventService/Subscriptions Save

POST ▼ | https://10.10.105.244/redfish/v1/EventService/Subscriptions Send ▼

Params Authorization Headers (9) **Body** ● Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary **JSON** ▼ Beautify

```
1 [{"Name": "SNMP3", "Destination": "192.168.1.49", "SubscriptionType": "SNMPTrap",
2   "SNMP": {"TrapCommunity": "hello"},
3   "Status": {"State": 1},
4   "Context": "WebUser2",
5   "Protocol": "SNMPv2c"}
6 ]
```

Body Cookies Headers (4) Test Results 200 OK 2.51 s 371 B Save Response ▼

Pretty Raw Preview Visualize **JSON** ▼ 🔍

```
1 [{"code": "Success",
2   "message": "Successfully Completed Request",
3   "@Message.ExtendedInfo": [
4     {
5       "@odata.type": "Message.v1_2_0.Message",
6       "MessageId": "Manager",
7       "Message": "User added",
8       "Severity": "None",
9       "MessageSeverity": "None",
10      "Resolution": "none"
11     }
12   ]
13 }
14 ]
```

Success Response Body Patch:

```
{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Manager",
      "Message": "User information updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": "none"
    }
  ]
}
```

Curl Command:

```
curl -location --request PATCH 'https://{pdu-ip}/redfish/v1/EventService/Subscriptions' \
--header 'X-Auth-Token: 1790411260' \
--header 'Content-Type: application/json' \
--data '{"Name":"SNMP3","Destination":"192.168.1.4","SubscriptionType":"SNMPTrap",
"SNMP":{"TrapCommunity":"hello"},
"Status":{"State":1},
"Context":"WebUser2",
"Protocol":"SNMPv2c"}'
```

The screenshot displays a REST client interface for the URL `https://10.10.105.244/redfish/v1/EventService/Subscriptions`. The request method is `PATCH` and the body is in `JSON` format. The request body is:

```
1 {"Name":"SNMP3","Destination":"192.168.1.4","SubscriptionType":"SNMPTrap",
2  "SNMP":{"TrapCommunity":"hello"},
3  "Status":{"State":1},
4  "Context":"WebUser2",
5  "Protocol":"SNMPv2c"}
6
```

The response status is `200 OK` with a time of `3.28 s` and a size of `385 B`. The response body is shown in `JSON` format:

```
1 {
2   "code": "Success",
3   "message": "Successfully Completed Request",
4   "@Message.ExtendedInfo": [
5     {
6       "@odata.type": "Message.v1_2_0.Message",
7       "MessageId": "Manager",
8       "Message": "User information updated",
9       "Severity": "None",
10      "MessageSeverity": "None",
11      "Resolution": "none"
12     }
13   ]
14 }
```

Payload For Delete:

```
{  
  "Name": "SNMP3",  
  "Protocol": "SNMPv2c"  
}
```

Success Response Body Delete:

```
{  
  "code": "Success",  
  "message": "Successfully Completed Request",  
  "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message",  
      "MessageId": "Manager",  
      "Message": "User Deleted",  
      "Severity": "None",  
      "MessageSeverity": "None",  
      "Resolution": "none"  
    }  
  ]  
}
```

Curl Command:

```
curl -location --request DELETE 'https://{pdu-ip}/redfish/v1/EventService/Subscriptions' \  
--header 'X-Auth-Token: 1790411260' \  
--header 'Content-Type: application/json' \  
--data '{"Name": "SNMP3",  
"Protocol": "SNMPv2c"  
}'
```

HTTP <https://10.10.105.244/redfish/v1/EventService/Subscriptions> Save

DELETE <https://10.10.105.244/redfish/v1/EventService/Subscriptions> Send

Params Authorization Headers (9) **Body** Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary JSON Beautify

```
1 {"Name": "SNMP3",
2  "Protocol": "SNMPv2c"
3 }
```

Body Cookies Headers (4) Test Results 200 OK 3.28 s 373 B Save Response

Pretty Raw Preview Visualize JSON 🔍

```
1 {"code": "Success",
2  "message": "Successfully Completed Request",
3  "@Message.ExtendedInfo": [
4    {
5      "@odata.type": "Message.v1_2_0.Message",
6      "MessageId": "Manager",
7      "Message": "User Deleted",
8      "Severity": "None",
9      "MessageSeverity": "None",
10     "Resolution": "none"
11   }
12 ]
13 }
14 }
```

18. SNMP Trap V3 Trap Configuration

Payload For Patch And Post :

```
{
  "Name": "Name4",
  "Destination": "40.40.40.40",
  "SubscriptionType": "SubscriptionType",
  "SNMP": {
    "AuthenticationKey": "123456789",
    "AuthenticationProtocol": 1,
    "EncryptionKey": "123456789",
    "EncryptionProtocol": 2,
    "SecurityLevel":1
  },
  "Status": {
    "State":1
  },
  "Context": "Context",
  "Protocol": "SNMPv3"
}
```

Note- The user should use the values shown below for changing or altering the following fields.

Parameters & Values
SecurityLevel: NoAuthNoPriv=0 , AuthNoPriv=1, AuthPriv=2
Privacy algorithm: EncryptionProtocol: DES=0,AES128=1, AES192=2, AES256=3
Authentication Algorithm: AuthenticationProtocol: SHA=1,MD5=0

Success Response For Post:

```
{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Manager",
      "Message": "User added",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": "none"
    }
  ]
}
```


Curl Command:

```
curl -location 'https://{pdu-ip}/redfish/v1/EventService/Subscriptions' \  
-header 'X-Auth-Token: 775191544' \  
-header 'Content-Type: application/json' \  
-data '{"Name":"SNMP3","Destination":"192.168.1.49","SubscriptionType":"SNMPTrap",  
"SNMP":{"TrapCommunity":"hello"},  
"Status":{"State":1},  
"Context":"WebUser2",  
"Protocol":"SNMPv2c"  
'
```

The screenshot displays a REST client interface for a POST request to `https://10.10.105.244/redfish/v1/EventService/Subscriptions`. The request body is a JSON object with the following structure:

```
1 {"Name": "SNMP3", "Destination": "192.168.1.49", "SubscriptionType": "SNMPTrap",  
2  "SNMP": {"TrapCommunity": "hello"},  
3  "Status": {"State": 1},  
4  "Context": "WebUser2",  
5  "Protocol": "SNMPv2c"  
6 }
```

The response is a 200 OK status with a response time of 1565 ms and a size of 371 B. The response body is shown in a pretty-printed JSON format:

```
1 {"code": "Success",  
2  "message": "Successfully Completed Request",  
3  "@Message.ExtendedInfo": [  
4    {  
5      "@odata.type": "Message.v1_2_0.Message",  
6      "MessageId": "Manager",  
7      "Message": "User added",  
8      "Severity": "None",  
9      "MessageSeverity": "None",  
10     "Resolution": "none"  
11   }  
12 ]  
13 ]  
14 }
```

Success Response For Patch:

```
{
  "code": "Success",
  "message": "Successfully Completed Request",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "Message.v1_2_0.Message",
      "MessageId": "Manager",
      "Message": "User information updated",
      "Severity": "None",
      "MessageSeverity": "None",
      "Resolution": "none"
    }
  ]
}
```

Curl Command:

```
curl --location --request PATCH 'https://{pdu-ip}/redfish/v1/EventService/Subscriptions' \
--header 'X-Auth-Token: 775191544' \
--header 'Content-Type: application/json' \
--data '{"Name":"SNMP3","Destination":"192.168.1.4","SubscriptionType":"SNMPTrap",
"SNMP":{"TrapCommunity":"hello"},
"Status":{"State":1},
"Context":"WebUser2",
"Protocol":"SNMPv2c"}'
```

The screenshot displays a REST client interface for a PATCH request to `https://10.10.105.244/redfish/v1/EventService/Subscriptions`. The request body is a JSON object with the following structure:

```
1 {"Name":"SNMP3","Destination":"192.168.1.4","SubscriptionType":"SNMPTrap",
2  "SNMP":{"TrapCommunity":"hello"},
3  "Status":{"State":1},
4  "Context":"WebUser2",
5  "Protocol":"SNMPv2c"}
6
```

The response is a 200 OK status with a response time of 1587 ms and a size of 385 B. The response body is a JSON object with the following structure:

```
1 {
2   "code": "Success",
3   "message": "Successfully Completed Request",
4   "@Message.ExtendedInfo": [
5     {
6       "@odata.type": "Message.v1_2_0.Message",
7       "MessageId": "Manager",
8       "Message": "User information updated",
9       "Severity": "None",
10      "MessageSeverity": "None",
11      "Resolution": "none"
12     }
13   ]
14 }
```

Payload For Delete:

```
{  
  "Name": "Name4",  
  "Protocol": "SNMPv3"  
}
```

Success Response For Delete:

```
{  
  "code": "Success",  
  "message": "Successfully Completed Request",  
  "@Message.ExtendedInfo": [  
    {  
      "@odata.type": "Message.v1_2_0.Message",  
      "MessageId": "Manager",  
      "Message": "User Deleted",  
      "Severity": "None",  
      "MessageSeverity": "None",  
      "Resolution": "none"  
    }  
  ]  
}
```

Curl Command:

```
curl -location --request DELETE 'https://{pdu-ip}/redfish/v1/EventService/Subscriptions' \  
--header 'X-Auth-Token: 775191544' \  
--header 'Content-Type: application/json' \  
--data '{  
  "Name": "Name4",  
  "Protocol": "SNMPv3"  
}'
```

https://10.10.105.244/redfish/v1/EventService/Subscriptions

Save

DELETE https://10.10.105.244/redfish/v1/EventService/Subscriptions

Send

Params Authorization Headers (9) **Body** Pre-request Script Tests Settings

Cookies

none form-data x-www-form-urlencoded **raw** binary JSON

Beautify

```
1 {}
2 "Name": "Name4",
3 "Protocol": "SNMPv3"
4 {}
```

Body Cookies Headers (4) Test Results

200 OK 1333 ms 373 B Save Response

Pretty Raw Preview Visualize JSON

```
1 {}
2 "code": "Success",
3 "message": "Successfully Completed Request",
4 "@Message.ExtendedInfo": [
5   {
6     "@odata.type": "Message.v1_2_0.Message",
7     "MessageId": "Manager",
8     "Message": "User Deleted",
9     "Severity": "None",
10    "MessageSeverity": "None",
11    "Resolution": "none"
12  }
13 ]
14 {}
```


19. Setting Temperature Thresholds

METHOD: POST

URL – <https://{pdu-ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/PDUTemp>

Payload For Post:

```
{
  "PDU_ID": 1,
  "SENSOR_ID": 1,
  "EnableLowCritical": 1,
  "EnableUpWarning": 1,
  "EnableLowWarning": 1,
  "EnableUpCritical": 1,
  "LowCritical": 50,
  "LowWarning": 60,
  "UpWarning": 70,
  "UpCritical": 80,
  "Units": "C"
}
```

Success Response

```
{
  "code": "TEMPERATURE_SENSOR_SET_SUCCESS",
  "message": "Temperature Sensor thresholds set successfully.",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "MessageId": "TEMPERATURE_SENSOR_SET_SUCCESS",
      "RelatedProperties": [],
      "MessageArgs": [
        "Temperature"
      ],
      "Resolution": "Temperature Sensor thresholds set successfully."
    }
  ]
}
```

Curl Command:

```
curl -location --request POST 'https://{pdu-  
ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/PDUTemp' \  
--header 'X-Auth-Token: 1540383426' \  
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
  "PDU_ID": 1, "SENSOR_ID": 1,  
  "EnableLowCritical": 1,  
  "EnableUpWarning": 1,  
  "EnableLowWarning": 1,  
  "EnableUpCritical": 1,  
  "LowCritical": 50,  
  "LowWarning": 60,  
  "UpWarning": 70,  
  "UpCritical": 80,  
  "Units": "C"  
}'
```

The screenshot displays a REST client interface for a POST request to `https://10.10.105.231/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/PDUTemp`. The request body is a JSON object with the following structure:

```
1  {  
2    "PDU_ID": 1,  
3    "SENSOR_ID": 2,  
4    "EnableLowCritical": 1,  
5    "EnableUpWarning": 1,  
6    "EnableLowWarning": 1,  
7    "EnableUpCritical": 1,  
8    "LowCritical": 50,  
9    "LowWarning": 60,  
10   "UpWarning": 70,  
11   "UpCritical": 80,  
12   "Units": "C"  
13 }
```

The response status is 200 OK, with a time of 2.56 s and a size of 463 B. The response body is a JSON object with the following structure:

```
1  {  
2    "code": "TEMPERATURE_SENSOR_SET_SUCCESS",  
3    "message": "Temperature Sensor thresholds set successfully.",  
4    "@Message.ExtendedInfo": [  
5      {  
6        "@odata.type": "#Message.v1_1_1.Message",  
7        "MessageId": "TEMPERATURE_SENSOR_SET_SUCCESS",  
8        "RelatedProperties": [],  
9        "MessageArgs": [  
10         "Temperature"  
11       ]  
12     },  
13     "Resolution": "Temperature Sensor thresholds set successfully."  
14   ]  
15 }
```

20. Setting Humidity Thresholds

METHOD: POST

URL – <https://{pdu-ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/PDUHumidity>

Payload For Post:

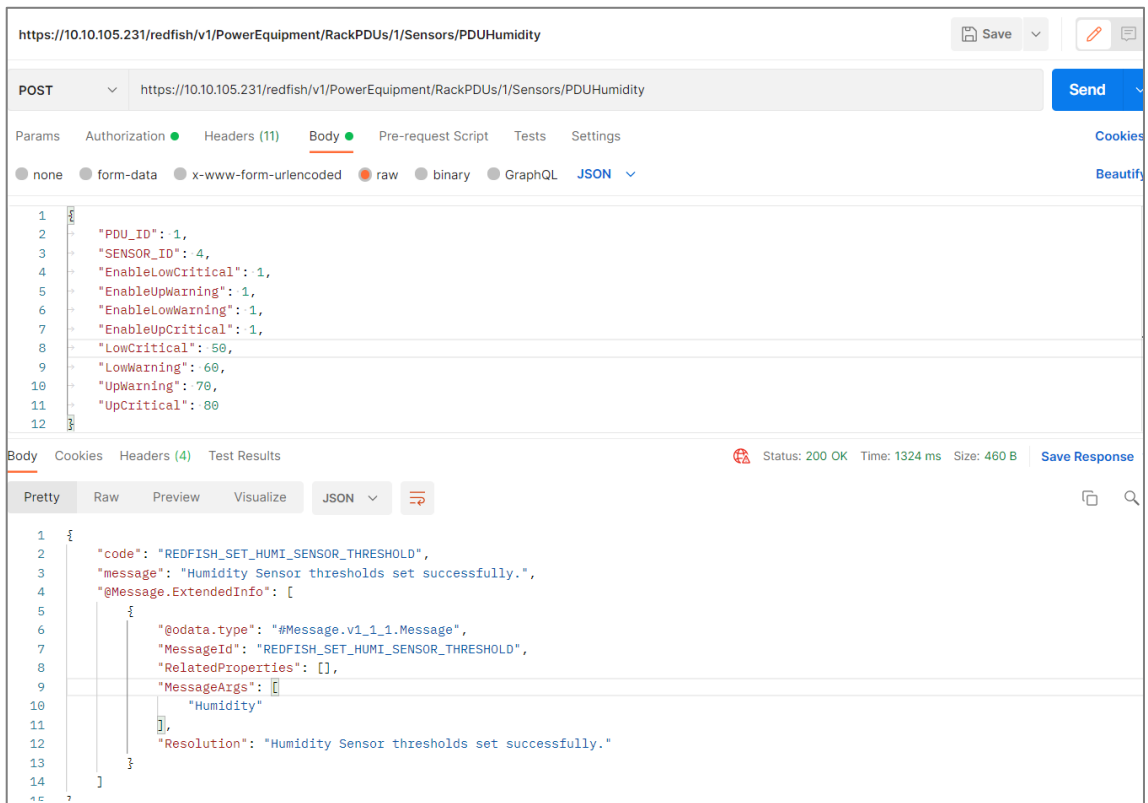
```
{
  "PDU_ID": 1,
  "SENSOR_ID": 4,
  "EnableLowCritical": 1,
  "EnableUpWarning": 1,
  "EnableLowWarning": 1,
  "EnableUpCritical": 1,
  "LowCritical": 50,
  "LowWarning": 60,
  "UpWarning": 70,
  "UpCritical": 80
}
```

Success Response

```
{
  "code": "REDFISH_SET_HUMI_SENSOR_THRESHOLD",
  "message": "Humidity Sensor thresholds set successfully.",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "MessageId": "REDFISH_SET_HUMI_SENSOR_THRESHOLD",
      "RelatedProperties": [],
      "MessageArgs": [
        "Humidity"
      ],
      "Resolution": "Humidity Sensor thresholds set successfully."
    }
  ]
}
```


Curl Command:

```
curl --location --request POST 'https://{pdu-  
ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/PDUHumidity' \  
--header 'X-Auth-Token: 1540383426' \  
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
  "PDU_ID": 1,  
  "SENSOR_ID": 4,  
  "EnableLowCritical": 1,  
  "EnableUpWarning": 1,  
  "EnableLowWarning": 1,  
  "EnableUpCritical": 1,  
  "LowCritical": 50,  
  "LowWarning": 60,  
  "UpWarning": 70,  
  "UpCritical": 80  
}'
```



21. Setting Power Thresholds

METHOD: POST

URL – <https://{pdu-id}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/PowerThreshold>

Payload For Post:

```
{
  "PDU_ID": 1,
  "EnableLowCritical": 1,
  "EnableUpWarning": 1,
  "EnableLowWarning": 1,
  "EnableUpCritical": 1,
  "LowCritical": 50,
  "LowWarning": 60,
  "UpWarning": 70,
  "UpCritical": 80,,
  "ResetThreshold" : 22,
  "Delay":2
}
```

Success Response

```
{
  "code": "#Message.v1_1_1.Message",
  "message": "Power thresholds set successfully.",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "MessageId": "#Message.v1_1_1.Message",
      "RelatedProperties": [],
      "MessageArgs": [
        "Power Threshold"
      ],
      "Resolution": "Power thresholds set successfully."
    }
  ]
}
```

Curl Command:

```
curl --location --request POST https://{pdu-  
ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/PowerThreshold' \  
--header 'X-Auth-Token: 1804289383' \  
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
  "PDU_ID": 1,  
  "EnableLowCritical": 1,  
  "EnableUpWarning": 1,  
  "EnableLowWarning": 1,  
  "EnableUpCritical": 1,  
  "LowCritical": 50,  
  "LowWarning": 60,  
  "UpWarning": 70,  
  "UpCritical": 80,  
  "ResetThreshold": 22,  
  "Delay": 2  
}'
```

The screenshot displays a REST client interface for a POST request to the endpoint `https://10.10.105.231/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/PowerThreshold`. The request body is a JSON object with the following fields: `"PDU_ID": 1`, `"EnableLowCritical": 1`, `"EnableUpWarning": 1`, `"EnableLowWarning": 1`, `"EnableUpCritical": 1`, `"LowCritical": 50`, `"LowWarning": 60`, `"UpWarning": 70`, `"UpCritical": 80`, `"ResetThreshold": 22`, and `"Delay": 2`. The response is a JSON object with a status code of 200 OK, a time of 456 ms, and a size of 427 B. The response body is a JSON object with the following fields: `"code": "#Message.v1_1_1.Message"`, `"message": "Power thresholds set successfully."`, `"@Message.ExtendedInfo": [{"@odata.type": "#Message.v1_1_1.Message", "MessageId": "#Message.v1_1_1.Message", "RelatedProperties": [], "MessageArgs": [{"Power Threshold"}]}, {"Resolution": "Power thresholds set successfully."}]`.

22. Setting Voltage Thresholds

METHOD: POST

URL – <https://{pdu-id}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/VoltageThreshold>

Payload For Post:

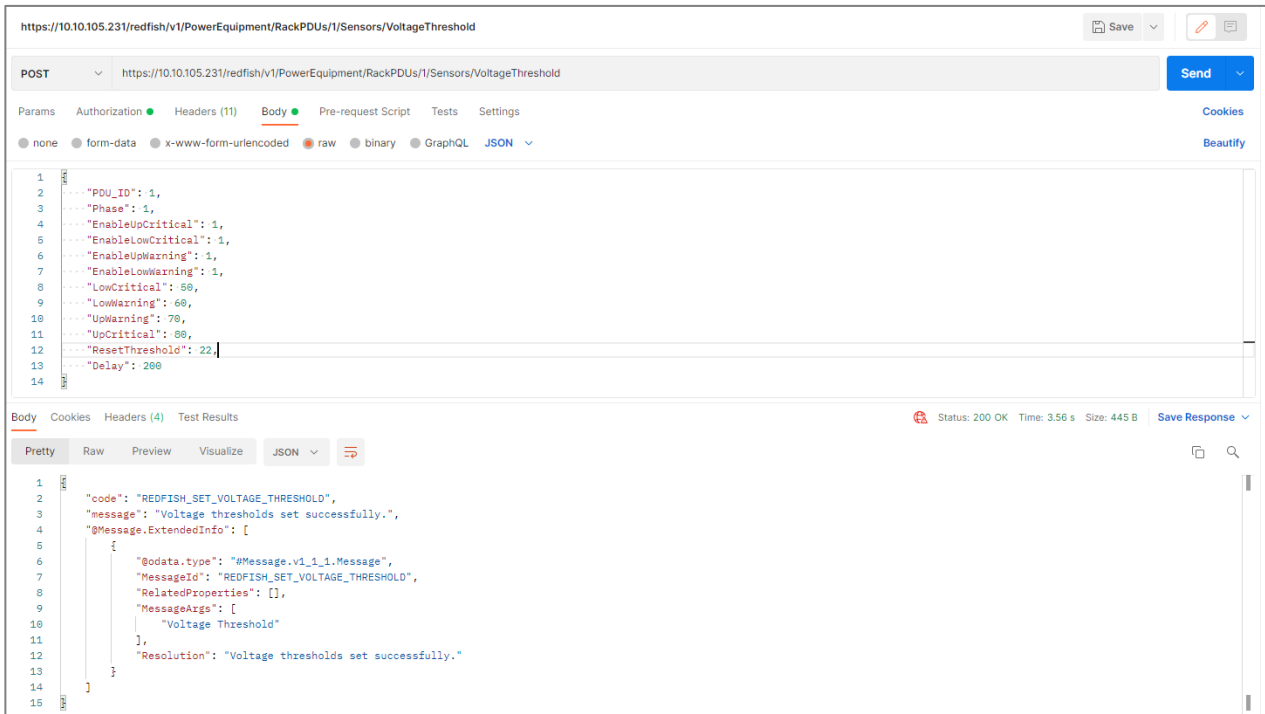
```
{
  "PDU_ID": 1,
  "Phase": 1,
  "EnableUpCritical": 1,
  "EnableLowCritical": 1,
  "EnableUpWarning": 1,
  "EnableLowWarning": 1,
  "LowCritical": 50,
  "LowWarning": 60,
  "UpWarning": 70,
  "UpCritical": 80,
  "ResetThreshold": 22,
  "Delay": 200
}
```

Success Response

```
{
  "code": "REDFISH_SET_VOLTAGE_THRESHOLD",
  "message": "Voltage thresholds set successfully.",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "MessageId": "REDFISH_SET_VOLTAGE_THRESHOLD",
      "RelatedProperties": [],
      "MessageArgs": [
        "Voltage Threshold"
      ],
      "Resolution": "Voltage thresholds set successfully."
    }
  ]
}
```

Curl Command:

```
curl --location --request POST 'https://{pdu-  
ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/VoltageThreshold'  
--header 'X-Auth-Token: 1804289383' \  
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
  "PDU_ID": 1,  
  "Phase": 1,  
  "EnableUpCritical": 1,  
  "EnableLowCritical": 1,  
  "EnableUpWarning": 1,  
  "EnableLowWarning": 1,  
  "LowCritical": 50,  
  "LowWarning": 60,  
  "UpWarning": 70,  
  "UpCritical": 80,  
  "ResetThreshold": 22,  
  "Delay": 200  
'
```



23. Setting Current Thresholds

METHOD: POST

URL – <https://{pdu-id}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/CurrentThreshold>

Payload For Post:

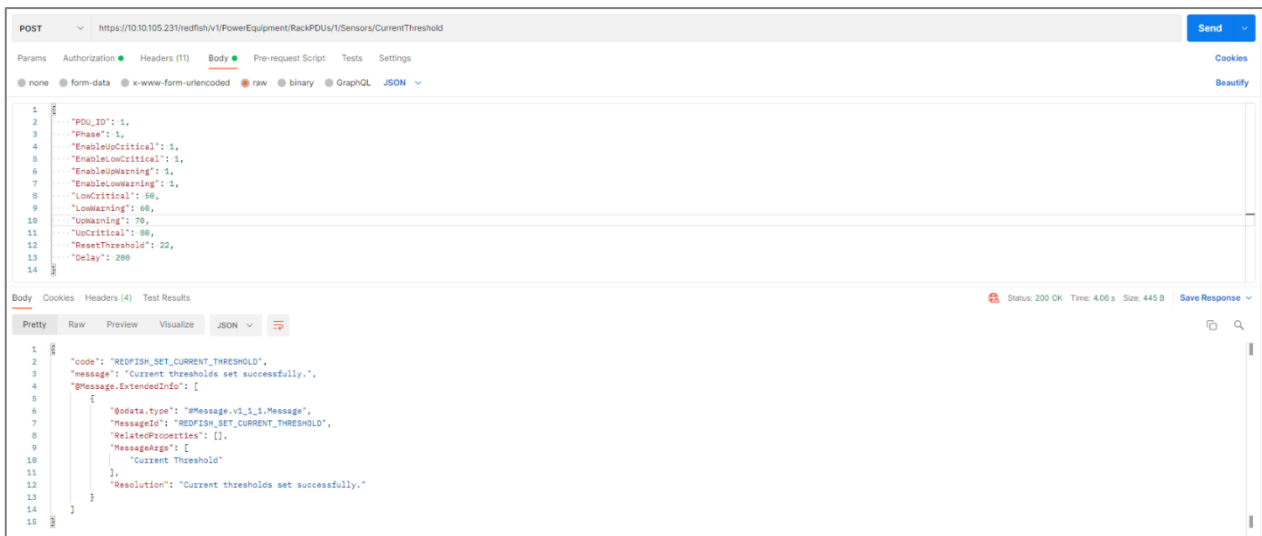
```
{
  "PDU_ID": 1,
  "Phase": 1,
  "EnableUpCritical": 1,
  "EnableLowCritical": 1,
  "EnableUpWarning": 1,
  "EnableLowWarning": 1,
  "LowCritical": 50,
  "LowWarning": 60,
  "UpWarning": 70,
  "UpCritical": 80,
  "ResetThreshold": 22,
  "Delay": 200
}
```

Success Response

```
{
  "code": "REDFISH_SET_CURRENT_THRESHOLD",
  "message": "Current thresholds set successfully.",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "MessageId": "REDFISH_SET_CURRENT_THRESHOLD",
      "RelatedProperties": [],
      "MessageArgs": [
        "Current Threshold"
      ],
      "Resolution": "Current thresholds set successfully."
    }
  ]
}
```

Curl Command:

```
curl --location --request POST 'https://{pdu-  
ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/CurrentThreshold'  
--header 'X-Auth-Token: 1804289383' \  
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
  "PDU_ID": 1,  
  "Phase": 1,  
  "EnableUpCritical": 1,  
  "EnableLowCritical": 1,  
  "EnableUpWarning": 1,  
  "EnableLowWarning": 1,  
  "LowCritical": 50,  
  "LowWarning": 60,  
  "UpWarning": 70,  
  "UpCritical": 80,  
  "ResetThreshold": 22,  
  "Delay": 200  
}'
```



24. Setting CB Thresholds

METHOD: POST

URL – <https://{pdu-ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/CBThreshold>

Payload For Post:

```
{
  "PDU_ID": 1,
  "CB_ID": 1,
  "EnableUpCritical": 1,
  "EnableLowCritical": 1,
  "EnableUpWarning": 1,
  "EnableLowWarning": 1,
  "LowCritical": 50,
  "LowWarning": 60,
  "UpWarning": 70,
  "UpCritical": 80,
  "ResetThreshold": 22,
  "Delay": 200
}
```

Success Response

```
{
  "code": "REDFISH_SET_CB_THRESHOLD",
  "message": "CB thresholds set successfully.",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "MessageId": "REDFISH_SET_CB_THRESHOLD",
      "RelatedProperties": [],
      "MessageArgs": [
        "CB Threshold"
      ],
      "Resolution": "CB thresholds set successfully."
    }
  ]
}
```

Curl Command:

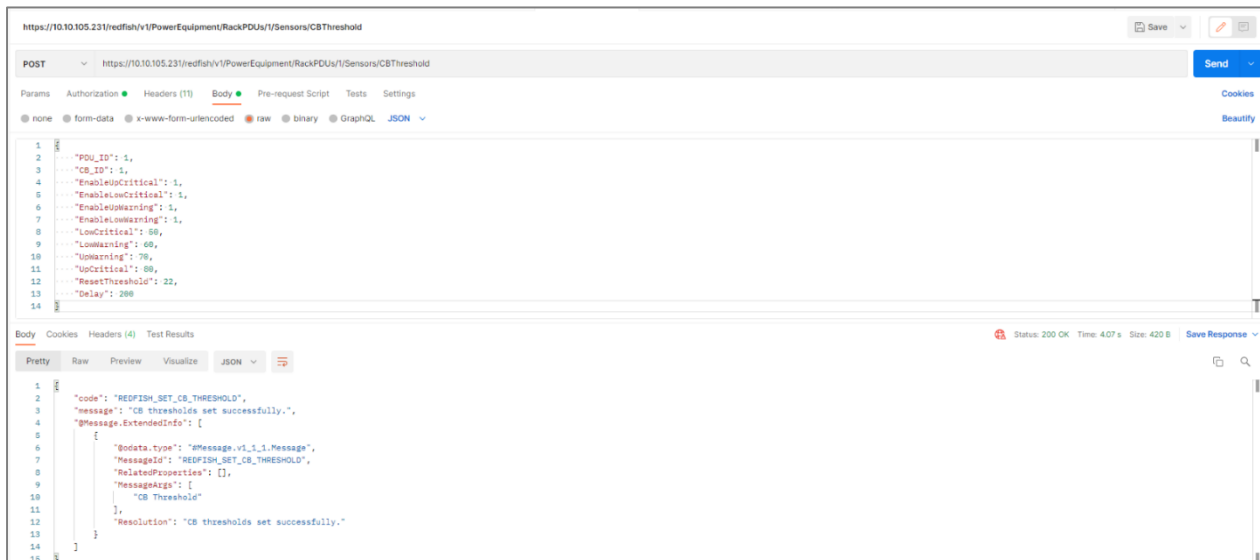
```
curl -location -request POST 'https://{pdu-
ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/CBThreshold'
\
-header 'X-Auth-Token: 1804289383' \
-header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \
-header 'Content-Type: application/json' \
--data-raw '{
  "PDU_ID": 1,
  "CB_ID": 1,
  "EnableUpCritical": 1,
  "EnableLowCritical": 1,
  "EnableUpWarning": 1,
  "EnableLowWarning": 1,
  "LowCritical": 50,
  "LowWarning": 60,
```



```

"UpWarning": 70,
"UpCritical": 80,
"ResetThreshold": 22,
"Delay": 200
}

```



25. Setting Outlet Thresholds

METHOD: POST

URL – <https://{pdu-ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/OutletThreshold>

Payload For Post:

```

{
  "PDU_ID": 1,
  "OutletNumber": 1,
  "EnableUpCritical": 1,
  "EnableLowCritical": 1,
  "EnableUpWarning": 1,
  "EnableLowWarning": 1,
  "LowCritical": 50,
  "LowWarning": 60,
  "UpWarning": 70,
  "UpCritical": 80,
  "ResetThreshold": 22,
  "Delay": 200
}

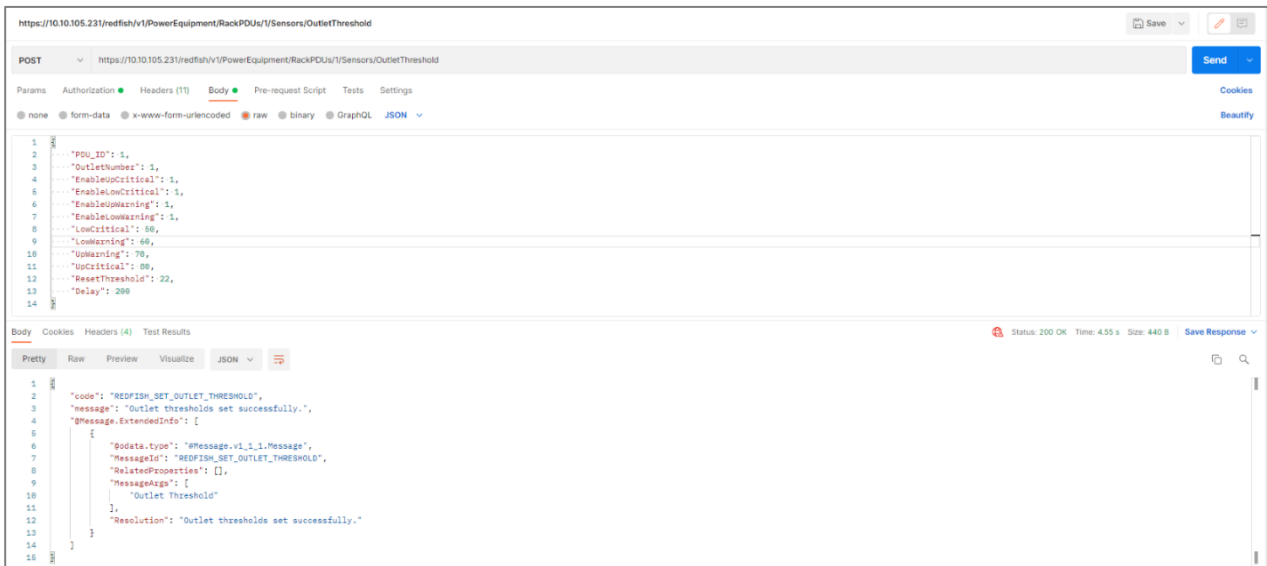
```

Success Response

```
{
  "code": "REDFISH_SET_OUTLET_THRESHOLD",
  "message": "Outlet thresholds set successfully.",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "MessageId": "REDFISH_SET_OUTLET_THRESHOLD",
      "RelatedProperties": [],
      "MessageArgs": [
        "Outlet Threshold"
      ],
      "Resolution": "Outlet thresholds set successfully."
    }
  ]
}
```

Curl Command:

```
curl --location --request POST 'https://{pdu-
ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/OutletThreshold'
--header 'X-Auth-Token: 1804289383' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \
--header 'Content-Type: application/json' \
--data-raw '{
  "PDU_ID": 1,
  "OutletNumber": 1,
  "EnableUpCritical": 1,
  "EnableLowCritical": 1,
  "EnableUpWarning": 1,
  "EnableLowWarning": 1,
  "LowCritical": 50,
  "LowWarning": 60,
  "UpWarning": 70,
  "UpCritical": 80,
  "ResetThreshold": 22,
  "Delay": 200
}'
```



26. Setting LED Colour

METHOD: POST

URL – https://{pdu-ip}/redfish/v1/Chassis/1/Oem/nVentChassis/v1_0_0/LEDColor

Payload For Post:

```

{
  "PanelLEDColor": "Red",
  "Pdu_Id": 1
}

```

Success Response

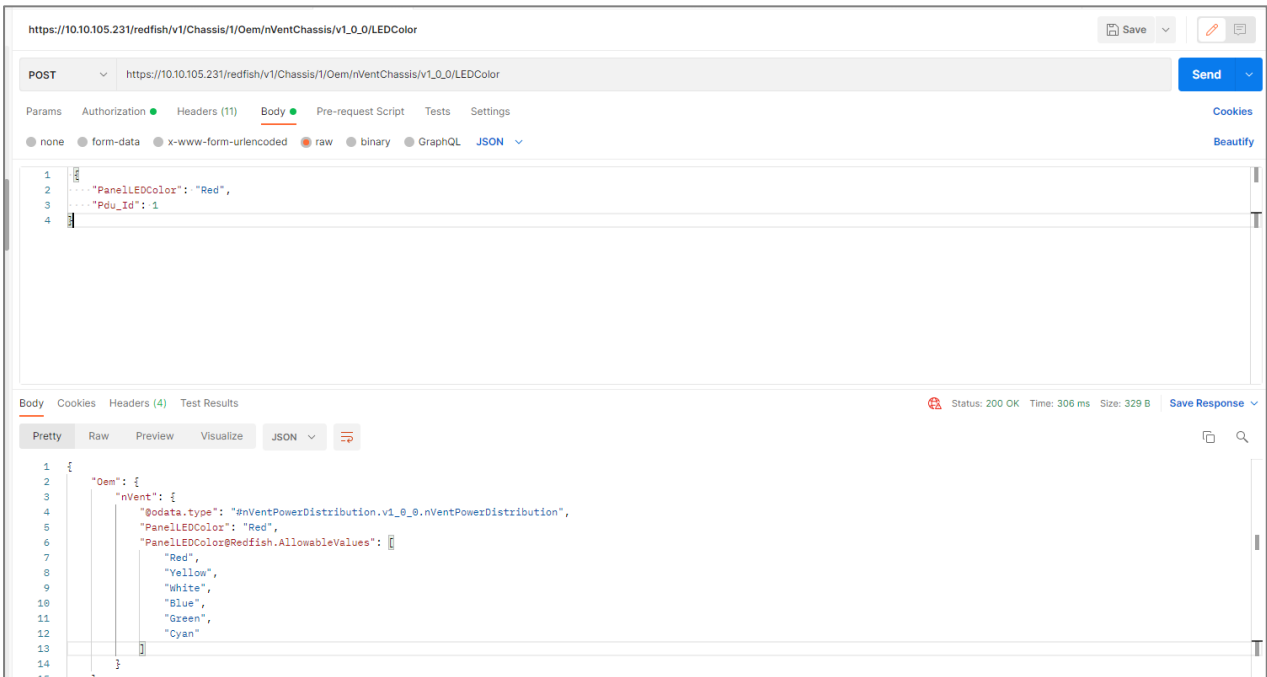
```

{
  "Oem": {
    "nVent": {
      "@odata.type": "#nVentPowerDistribution.v1_0_0.nVentPowerDistribution",
      "PanelLEDColor": "Red",
      "PanelLEDColor@Redfish.AllowableValues": [
        "Red",
        "Yellow",
        "White",
        "Blue",
        "Green",
        "Cyan"
      ]
    }
  }
}

```

Curl Command:

```
curl --location --request POST 'https://{pdu-ip}/redfish/v1/Chassis/1/Oem/nVentChassis/v1_0_0/LEDColor' \  
--header 'X-Auth-Token: 521595368' \  
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
  "PanelLEDColor": "Red",  
  "Pdu_Id": 1  
}'
```



27. Syslog Settings

METHOD: POST

URL – <https://{pdu-ip}/redfish/v1/EventService/Subscriptions/Syslog>

Payload For Post:

```
"SyslogEnabled": 1,
"SyslogAddress": "dummy_syslog_host",
"SyslogPort": 5678,
"SyslogProtocol": 0
}
```

Note - Syslog Protocols can be set to 0 if it is UDP, 1 for TCP and 2 TCP+TLS

Success Response

```
{
"code": "#Message.v1_1_1.Message",
"message": "Syslog settings SET successfully.",
"@Message.ExtendedInfo": [
{
"@odata.type": "#Message.v1_1_1.Message",
"MessageId": "#Message.v1_1_1.Message",
"RelatedProperties": [],
"MessageArgs": [
"Syslog_SET"
],
"Resolution": "Syslog settings SET successfully."
}
]
}
```

Curl Command:

```
curl -location --request POST 'https://{pdu-ip}/redfish/v1/EventService/Subscriptions/Syslog' \
--header 'X-Auth-Token: 294702567' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \
--header 'Content-Type: application/json' \
--data-raw '{
"SyslogEnabled": 1,
"SyslogAddress": "dummy_syslog_host",
"SyslogPort": 5678,
"SyslogProtocol": 0
}'
```

28. Setting Default

METHOD: POST

URL – <https://{pdu-ip}/redfish/v1/Actions/Control.ResetToDefaults>

Payload For Post:

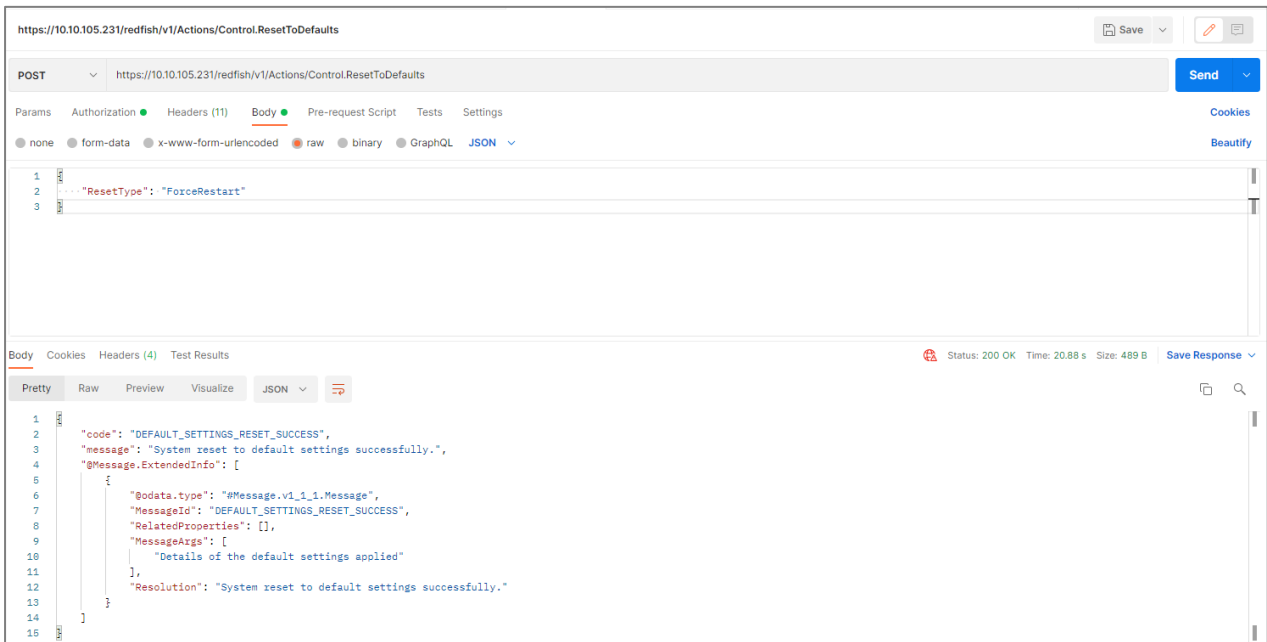
```
{
  "ResetType": "ForceRestart"
}
```

Success Response

```
{
  "code": "DEFAULT_SETTINGS_RESET_SUCCESS",
  "message": "System reset to default settings successfully.",
  "@Message.ExtendedInfo": [
    {
      "@odata.type": "#Message.v1_1_1.Message",
      "MessageId": "DEFAULT_SETTINGS_RESET_SUCCESS",
      "RelatedProperties": [],
      "MessageArgs": [
        "Details of the default settings applied"
      ],
      "Resolution": "System reset to default settings successfully."
    }
  ]
}
```

Curl Command:

```
curl --location --request POST 'https://{pdu-ip}/redfish/v1/Actions/Control.ResetToDefaults' \
--header 'X-Auth-Token: 336465782' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5' \
--header 'Content-Type: application/json' \
--data-raw '{
  "ResetType": "ForceRestart"
}'
```



29. Download Configuration

METHOD: GET

URL – <https://{pdu-ip}/redfish/v1/Managers/1/Actions/Manager.DownloadConfiguration>

Curl Command:

```
curl --location --request GET 'https://redfish/v1/Managers/1/Actions/Manager.DownloadConfiguration' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5'
```

Success Response

```
{
  "@odata.context": "/redfish/v1/$metadata#Manager.Manager",
  "@odata.id": "/redfish/v1/Managers/1/Actions/Manager.DownloadConfiguration",
  "@odata.type": "#Manager.v1_0_0.Manager",
  "Id": "1",
  "Name": "Manager",
  "ConfigurationLink": "/redfish/v1/system/conf/conf.ini"
}
```

https://10.20.15.59/redfish/v1/Managers/1/Actions/Manager.DownloadConfiguration

GET https://10.20.15.59/redfish/v1/Managers/1/Actions/Manager.DownloadConfiguration

Params Authorization Headers (8) Body Pre-request Script Tests Settings Cookies

Query Params

KEY	VALUE	DESCRIPTION	...	Bulk Edit
Key	Value	Description		

Body Cookies Headers (4) Test Results Status: 200 OK Time: 242 ms Size: 384 B Save Response

Pretty Raw Preview Visualize JSON

```

1  {"@odata.context": "/redfish/v1/$metadata#Manager.Manager",
2  "@odata.id": "/redfish/v1/Managers/1/Actions/Manager.DownloadConfiguration",
3  "@odata.type": "#Manager.v1_0_0.Manager",
4  "Id": "1",
5  "Name": "Manager",
6  "ConfigurationLink": "/redfish/v1/system/conf/conf.ini"}
7
8

```

ort < Jntitle: OutletC EN681 GET Outl EN681 OutletC OutletC GET Outl GET http > + No Environment

https://10.20.15.59/redfish/v1/system/conf/conf.ini

GET https://10.20.15.59/redfish/v1/system/conf/conf.ini

admin

123456789

Show Password

Status: 200 OK Time: 178 ms Size: 44.15 KB Save Response

Select path to save file

Downloads

File name: conf.ini

Save as type: All Files (*.*)

Save Cancel

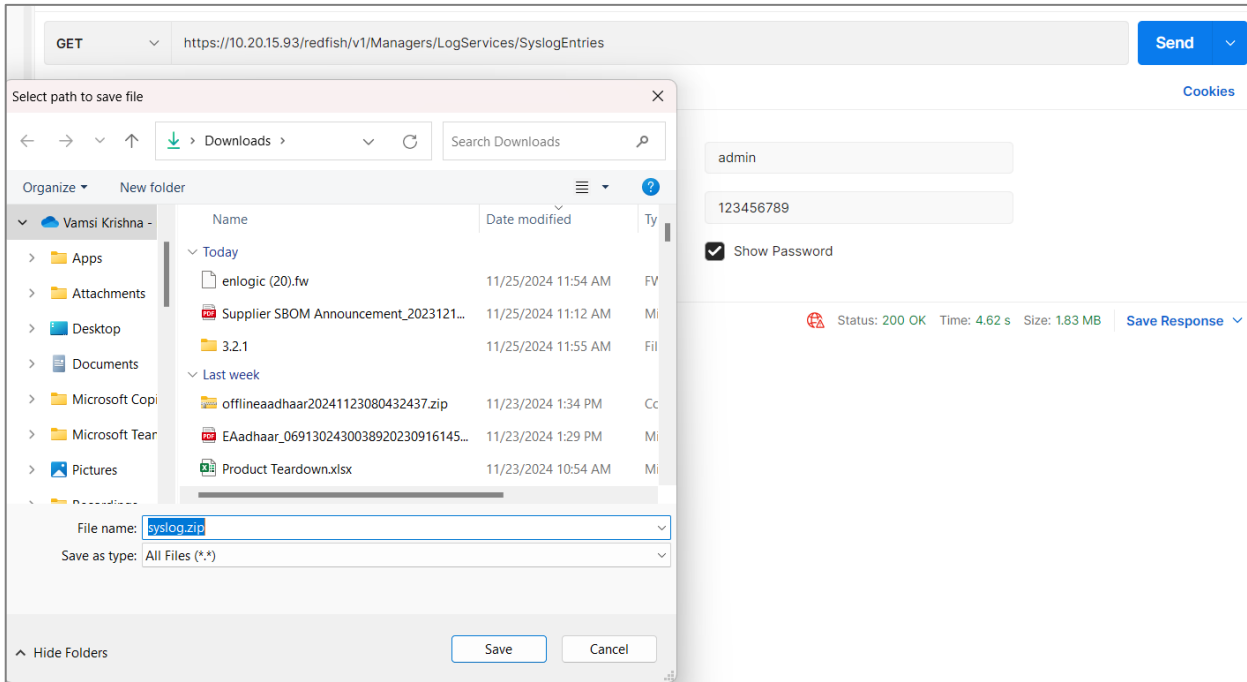
30. Syslog Entries

METHOD: GET

URL – <https://{pdu-ip}/redfish/v1/Managers/LogServices/SyslogEntries>

Curl Command:

```
curl --location --request GET 'https://redfish/v1/Managers/LogServices/SyslogEntries' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5'
```



31. Phase Data

METHOD: GET

URL – <https://{pdu-ip}/redfish/v1/PowerEquipment/PDUs/1/PhaseData>

Payload:

```
[
  {
    "Name": "",
    "PhaseIndex": 1,
    "Current": 0,
    "PowerFactor": 0,
    "Voltage": 0,
    "ApparentPower": 0,
    "Power": 0,
    "Energy": 0
  },
  {
    "Name": "",
    "PhaseIndex": 2,
    "Current": 0,
    "PowerFactor": 0,
    "Voltage": 0,
    "ApparentPower": 0,
    "Power": 0,
    "Energy": 0
  },
  {
    "Name": "",
    "PhaseIndex": 3,
    "Current": 0,
    "PowerFactor": 0,
    "Voltage": 0,
    "ApparentPower": 0,
    "Power": 0,
    "Energy": 0
  }
]
```

Curl Command:

```
curl -location --request GET 'https://redfish/v1/PowerEquipment/PDUs/1/PhaseData' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5'
```

```

GET https://10.20.15.93/redfish/v1/PowerEquipment/PDUs/1/PhaseData
Status: 200 OK Time: 34 ms Size: 522 B
Body
[
  {
    "Name": "Master",
    "PhaseIndex": 1,
    "Current": 0,
    "PowerFactor": 1000,
    "Voltage": 0,
    "ApparentPower": 0,
    "Power": 0,
    "Energy": 0
  },
  {
    "Name": "Master",
    "PhaseIndex": 2,
    "Current": 0,
    "PowerFactor": 1000,
    "Voltage": 200752,
    "ApparentPower": 0,
    "Power": 0,
    "Energy": 0
  },
  {
    "Name": "Master",
    "PhaseIndex": 3,
    "Current": 0,
    "PowerFactor": 1000,
    "Voltage": 200952,
    "ApparentPower": 0,
    "Power": 0,
    "Energy": 0
  }
]

```

32. Outlet Groups

METHOD: GET

URL – <https://{pdu-ip}/redfish/v1/Chassis/1/Power/OutletGroups>

Payload:

```

{
  "cookie": 3869520,
  "groups": [
    {
      "Id": 1,
      "Name": "vamsi",
      "Members": [
        {
          "pdu": 1,
          "outlet": 1,
          "status": "off"
        },
        {
          "pdu": 1,
          "outlet": 2,
          "status": "off"
        },
        {
          "pdu": 1,
          "outlet": 3,

```

```

    "status": "off"
  },
  {
    "pdu": 1,
    "outlet": 14,
    "status": "off"
  },
  {
    "pdu": 1,
    "outlet": 15,
    "status": "off"
  }
],
"PowerWatts": 0.0,
"ApparentPowerWatts": 0.0
},
{
  "Id": 2,
  "Name": "Vamsk",
  "Members": [
    {
      "pdu": 1,
      "outlet": 1,
      "status": "off"
    },
    {
      "pdu": 1,
      "outlet": 4,
      "status": "on"
    },
    {
      "pdu": 1,
      "outlet": 5,
      "status": "on"
    }
  ],
  "PowerWatts": 0.0,
  "ApparentPowerWatts": 0.0
},
{
  "Id": 3,
  "Name": "a",
  "Members": [
    {
      "pdu": 1,
      "outlet": 4,
      "status": "on"
    },
    {
      "pdu": 1,
      "outlet": 30,
      "status": "on"
    }
  ]
}

```

```

    }
  ],
  "PowerWatts": 0.0,
  "ApparentPowerWatts": 0.0
}
]
}

```

Curl Command:

```

curl --location --request GET 'https://redfish/v1/PowerEquipment/RackPDUs/1/OutletGroups' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5'

```

The screenshot shows a REST client interface with the following details:

- Method:** GET
- URL:** https://10.20.15.59/redfish/v1/PowerEquipment/RackPDUs/1/OutletGroups
- Headers:** 8 hidden
- Status:** 200 OK, Time: 282 ms, Size: 9.8 KB
- Body (JSON):**

```

1  {
2    "cookie": 3933240,
3    "groups": [
4      {
5        "Id": 1,
6        "Name": "PDU21@#%$^&*()ALLOUTLETSINDAISYCHAINedpu",
7        "Members": [
8          {
9            "pdu": 2,
10           "outlet": 1,
11           "status": "on"
12         },
13         {
14           "pdu": 2,
15           "outlet": 2,
16           "status": "on"
17         },
18         {
19           "pdu": 2,
20           "outlet": 3,
21           "status": "on"
22         },
23         {
24           "pdu": 2,
25           "outlet": 4

```

33. Total Energy

METHOD: GET

URL – <https://{pdu-ip}/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/TotalEnergy>

Payload:

```
[
  {
    "Total Energy": 0.0,
    "Active Power": 34.0,
    "Apparent Power": 41.0,
    "Resettable Energy": 0.0,
    "Power Factor": 821,
    "Energy Since": "2010/01/04 19:07:24",
    "Maximum Power": 8600.0,
    "Active Power Up Warning": 0.0,
    "Active Power Up Critical": 0.0,
    "Active Power Up Warning Set": false,
    "Active Power Up Critical Set": false,
    "Energy Up Warning": 2147483.0,
    "Energy Up Critical": 2147483.0,
    "Energy Up Warning Set": true,
    "Energy Up Critical Set": true
  }
]
```

Curl Command:

```
curl -location --request GET 'https://redfish/v1/PowerEquipment/RackPDUs/1/Sensors/TotalEnergy' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5'
```

The screenshot displays a REST client interface for a GET request to the URL `https://10.20.15.93/redfish/v1/PowerEquipment/RackPDUs/1/Sensors/TotalEnergy`. The request is configured with Basic Authentication, using the username `admin` and password `123456789`. The response status is `200 OK`. The response body is shown in JSON format:

```
{
  "@odata.id": "/redfish/v1/PowerEquipment/PDUs/1/TotalEnergy",
  "TotalEnergy": 405.0,
  "ResettableEnergy": 0.0,
  "EnergySince": "2024/11/20 15:32:05"
}
```

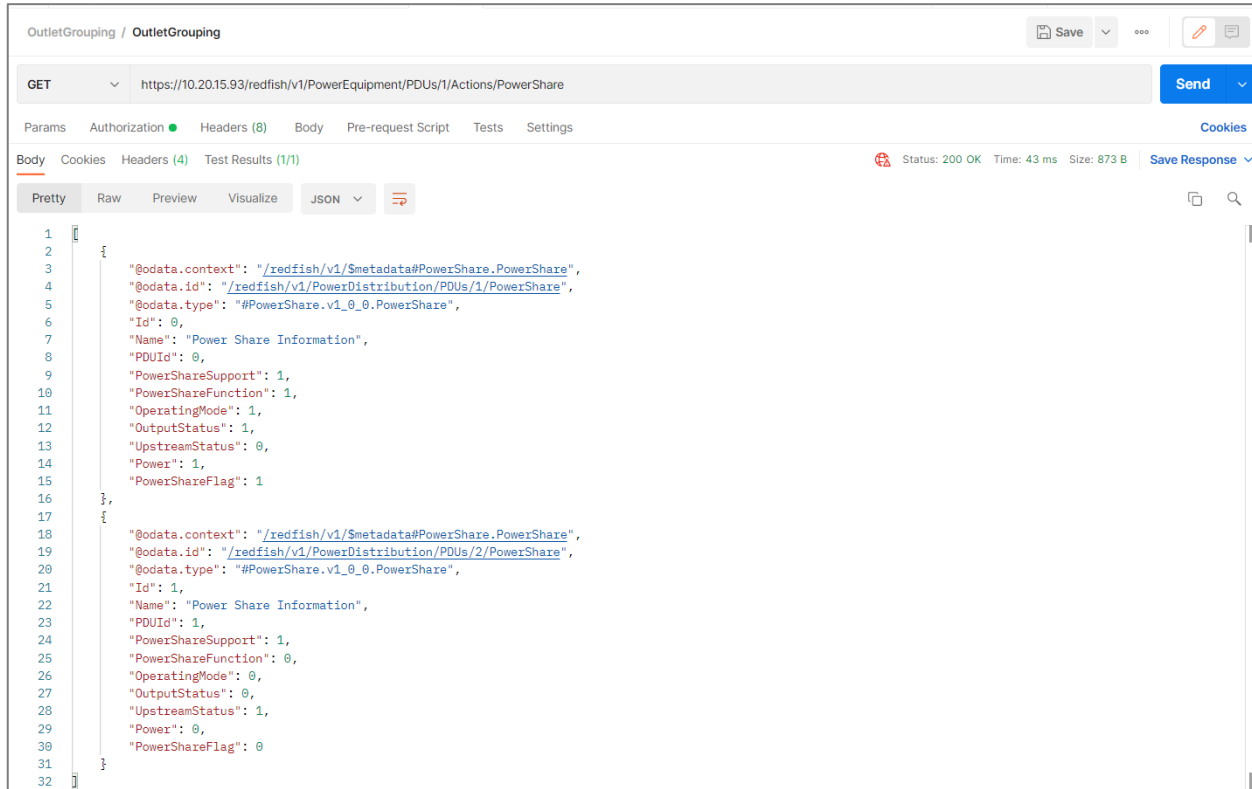
34. Power Share

METHOD: GET

URL – <https://{pdu-ip}/redfish/v1/PowerEquipment/PDUs/1/Actions/PowerShare>

Curl Command:

```
curl --location --request GET 'https://redfish/v1/PowerEquipment/PDUs/1/Actions/PowerShare' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5'
```



OutletGrouping / OutletGrouping

GET <https://10.20.15.93/redfish/v1/PowerEquipment/PDUs/1/Actions/PowerShare> Send

Params Authorization Headers (8) Body Pre-request Script Tests Settings Cookies

Body Cookies Headers (4) Test Results (1/1) Status: 200 OK Time: 43 ms Size: 873 B Save Response

Pretty Raw Preview Visualize JSON

```
1 {
2   {
3     "@odata.context": "/redfish/v1/$metadata#PowerShare.PowerShare",
4     "@odata.id": "/redfish/v1/PowerDistribution/PDUs/1/PowerShare",
5     "@odata.type": "#PowerShare.v1_0_0.PowerShare",
6     "Id": 0,
7     "Name": "Power Share Information",
8     "PDUId": 0,
9     "PowerShareSupport": 1,
10    "PowerShareFunction": 1,
11    "OperatingMode": 1,
12    "OutputStatus": 1,
13    "UpstreamStatus": 0,
14    "Power": 1,
15    "PowerShareFlag": 1
16  },
17  {
18    "@odata.context": "/redfish/v1/$metadata#PowerShare.PowerShare",
19    "@odata.id": "/redfish/v1/PowerDistribution/PDUs/2/PowerShare",
20    "@odata.type": "#PowerShare.v1_0_0.PowerShare",
21    "Id": 1,
22    "Name": "Power Share Information",
23    "PDUId": 1,
24    "PowerShareSupport": 1,
25    "PowerShareFunction": 0,
26    "OperatingMode": 0,
27    "OutputStatus": 0,
28    "UpstreamStatus": 1,
29    "Power": 0,
30    "PowerShareFlag": 0
31  }
32 }
```

35. Device Detection Threshold

METHOD: GET

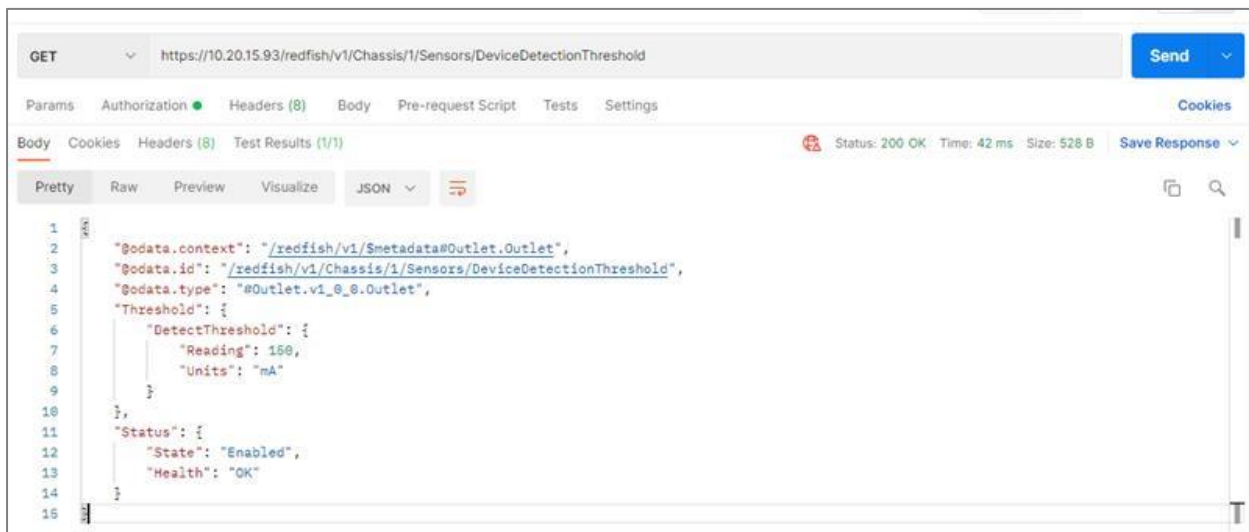
URL – <https://{pdu-ip}/redfish/v1/Chassis/1/Sensors/DeviceDetectionThreshold>

Payload:

```
{
  "@odata.context": "/redfish/v1/$metadata#Outlet.Outlet",
  "@odata.id": "/redfish/v1/Chassis/1/Sensors/DeviceDetectionThreshold",
  "@odata.type": "#Outlet.v1_0_0.Outlet",
  "Threshold": {
    "DetectThreshold": {
      "Reading": 150,
      "Units": "mA"
    }
  },
  "Status": {
    "State": "Enabled",
    "Health": "OK"
  }
}
```

Curl Command:

```
curl --location --request GET 'https://redfish/v1/Chassis/1/Sensors/DeviceDetectionThreshold' \
--header 'Authorization: Basic YWRtaW46MTIzNDU2Nzg5'
```



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
```



RESTAPI URLs AND CURL COMMANDS

1. Session ID: Creating 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:

```
cis@ldap:~$ curl -X POST -H "Content-Type: application/json" -d '{"username":"admin","password":"123456789","cookie":0}' -k https://10.88.0.82/xhrlogin.jsp {"cookie": 953139345, "change_password": false, "is_ldap": false, "role": "admin", "temperature": 0, "pdumode": 0}cis@ldap:~$ █
```

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:

```
cis@ldap:~$ curl -X POST -H "Content-Type: application/json" -d '{"pdu": [{"panel_name": "RACK_ONE_001","core_location": "Front","core_u_position": "4"} ], "cookie":953139345}' -k https://10.88.0.82/sys\_info\_set.jsp
{"uptstatus": 1}cis@ldap:~$
```

Note the response {"uptstatus":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
```

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:

```
cis@ldap:~$ 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
{"uptstatus": 1}cis@ldap:~$
```

Note the response {"uptstatus":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
```

Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
username	string	32
password	text/password	31
temperatureunit	int	0-Celsius, 1-Fahrenheit
chkenable	boolean	True/False
email	string	
active	boolean	True/False
roles	string	"admin", "manager", "user" default user
frpasschk	boolean	True/False

4. Edit USER & PASSWORD:

Curl commands to edit the User and Manager User Password

ADMIN USER:

CURL Command:

```
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:

```
cis@ldap:~$ 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  
{ "upstatus": 1 } cis@ldap:~$
```

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
```

Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
username	string	32
password	text/password	31
temperatureunit	int	0-Celsius, 1-Fahrenheit
chkenable	boolean	True/False
email	string	
active	boolean	True/False
roles	string	"admin", "manager", "user" default user

5. MANAGER USER:

CURL Command:

```
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
```

Screen Capture From Linux Box:

```
cis@ldap:~$ 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": 1603135659}' -k https://10.88.0.82/xhredituserpost.jsp  
{"uptstatus": 1}cis@ldap:~$
```

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
```

Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
username	string	32
password	text/password	31
temperatureunit	int	0-Celsius, 1-Fahrenheit
chkenable	boolean	True/False
email	string	
active	boolean	True/False
roles	string	"admin", "manager", "user" default user

6. DELETE USER:

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"cookie": 1761158407, "username": "test"}' -k https://10.88.0.82/xhrusersdel.jsp
```

CURL Command Formatted:

```
curl -X POST \  
-H "Content-Type: application/json" \  
-d '  
{  
    "cookie": 1761158407,  
    "username": "test"  
}' \  
-k https://10.88.0.82/xhrusersdel.jsp
```

7. 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/xhrchangeppost.jsp
```

Screen Capture From Linux Box:

```
cis@ldap:~$ curl -X POST -H "Content-Type: application/json" -d '{"oldpassword":"123456789","newpassword":"testing123","cookie":953139345}' -k https://10.88.0.82/xhrchangeppost.jsp  
{"uptstatus": 1}cis@ldap:~$
```

Note the response {"uptstatus":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/xhrchangeppost.jsp
```

8. LDAP

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"ldapuser": "12345678", "ldapbasedn": "test", "ldapdn": "test", "ldapnameattr": "admin", "ldapdomain": "", "ldappass": "12345678", "ldapebst": 32, "ldaphost": "2001:1890:1974:3380::263", "ldapport": 389, "ldapauth": "", "cookie": 1761158407}' -k https://10.88.0.82/xhrlldapset.jsp
```

CURL Command Formatted:

```
curl -X POST \  
-H "Content-Type: application/json" \  
-d '  
{  
  "ldapuser": "12345678",  
  "ldapbasedn": "test",  
  "ldapdn": "test",  
  "ldapnameattr": "admin",  
  "ldapdomain": "",  
  "ldappass": "12345678",  
  "ldapebst": 32,  
  "ldaphost": "2001:1890:1974:3380::263",  
  "ldapport": 389,  
  "ldapauth": "",  
  "cookie": 1761158407  
}' \  
-k https://10.88.0.82/xhrlldapset.jsp
```

Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
ldapuser	string	32
ldapbasedn	string	32
ldapdn	string	32
ldapnameattr	string	32
ldapdomain	string	32
ldappass	password	31
ldapebst		
ldaphost	string	64 (Ipv4/Ipv6/FQDN)
ldapport	int	1-65535
ldapauth	string	32

9. SESSION PREFERNCE

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"chkuserblocking": 1, "maxnumfailedlogins": 6, "blocktimeout": 3, "idletimeout": 1440, "temperature": 0, "ipmode": 3, "cookie": 1761158407}' -k https://10.88.0.82/xhrsetloginset.jsp
```

CURL Command Formatted:

```
curl -X POST \  
-H "Content-Type: application/json" \  
-d '  
{  
"chkuserblocking": 1,  
"maxnumfailedlogins": 6,  
"blocktimeout": 3,  
"idletimeout": 1440,  
"temperature": 0,  
"ipmode": 3,  
"cookie": 1761158407  
}' \  
-k https://10.88.0.82/xhrsetloginset.jsp
```

Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
chkuserblocking	int/Flag	0 or 1
maxnumfailedlogins	int	3 to 10
blocktimeout	int	1 min to infinite (0)
idletimeout	int	1 min to 1440 min (24hrs)
temperature	int	0-Celsius, 1-Fahrenheit
ipmode	int	1- IPV4, 2- IPV6, 3 - Both IPV4 & IPV6

10. PASSWORD POLICY

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{ "pswpolicy": 4, "maxpwdlen": 32, "minpwdlen": 8, "pwdaginginterval": 0, "cookie": 1761158407 }' -k https://10.88.0.82/xhrpwpolicyset.jsp
```

CURL Command Formatted:

```
curl -X POST \  
-H "Content-Type: application/json" \  
-d '  
{  
"pswpolicy": 4,  
"maxpwdlen": 32,  
"minpwdlen": 8,  
"pwdaginginterval": 0,  
"cookie": 1761158407  
}' \  
-k https://10.88.0.82/xhrpwpolicyset.jsp
```

Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
maxpwdlen	int	8 to 32
pswpolicy	int	lower(1), upper(2), One Numeric(4), Special Character(8)
minpwdlen	int	8 to 32
pwdaginginterval	int	7d(10080),14d(20160),30d(43200), 60d(86400),90d(129600),180d(259200), 365d(525600),never expire(0) (Time in minutes)

11. SNMP Version:

Curl commands to set V1/V2

CURL Command:

```
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:

```
cis@ldap:~$ 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 {"uptstatus": 1}cis@ldap:~$
```

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 Commands to set V3 Only

CURL Command:

```
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:

```
cis@ldap:~$ 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 {"uptstatus": 1}cis@ldap:~$
```

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 Commands to set V1/V2 & V3

CURL Command:

```
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:

```
cis@ldap:~$ 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  
{"uptstatus": 1}cis@ldap:~$ █
```

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
```

12. SNMP Community Strings [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":"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/xhrsnmpptest.jsp
```

Screen Capture From Linux Box:

```
cis@ldap:~$ 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"}],"cookie": 1603135659}' -k https://10.88.0.82/xhrsnmpptest.jsp
{"upststatus": 1}cis@ldap:~$
```

Note the response {"upststatus":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"
    }
    ]
}
```

```
"enable":false,  
"read":"public",  
"v4IP":"0.0.0.0",  
"write":"private"  
}  
],  
"cookie": 1603135659}' \  
-k https://10.88.0.82/xhrsnmppost.jsp
```

13. Change DHCP/IP Settings

FROM DHCP to STATIC

First set the IP Configuration from Static to DHCP and Follow it a 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:

```
cis@ldap:~$ 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}cis@ldap:~$ 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 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
```

14. 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:

```
cis@ldap:~$ 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
{"upststatus": 1}
cis@ldap:~$ curl -X POST -H 'Content-Type: application/json' -d '{"cookie": 825060319, "seldPdu": 1, "reset": 1}' -k https://10.88.0.82/xhrresetdevset.jsp
{"upststatus": 1}
cis@ldap:~$
```

Note the response {"upststatus":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 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
```

15. 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:

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

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
```

16. 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:

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

CURL Command Formatted:

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

Configuring NTP Server

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"server1": "0.north-america.pool.ntp.org", "server2": "1.north-america.pool.ntp.org", "cookie": 1312994984}' -k https://10.88.0.235/xhrntpcheckpost.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{
    "server1": "0.north-america.pool.ntp.org",
    "server2": "1.north-america.pool.ntp.org",
    "cookie": 1312994984
}' \
-k https://10.88.0.235/xhrntpcheckpost.jsp
```

17. Configuring Date & Time Server – Including 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":"13
9.59.15.185","ipesecondtimeserv":"144.24.146.96","offset":0,"cookie":385047644}' -k
https://10.10.105.59/xhrdatetimestepost.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/xhrdatetimestepost.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:

```
cis@ldap:~$ 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/xhrdatetimestepost.jsp
{"uptstatus": 1}cis@ldap:~$
```

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/xhrdatetimestepost.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
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
01	(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
3101	(UTC+06:30) Yangon (Rangoon)
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

18. Daylight Saving Time

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{ "s_month": 3, "s_week": 4, "s_day": 1, "s_hour": 1, "s_minute": 0, "s_second": 0, "e_month": 11, "e_week": 1, "e_day": 1, "e_hour": 1, "e_minute": 0, "e_second": 0, "offset": 60, "enable": true, "cookie": 1312994984 }' -k https://10.88.0.235/dst\_set
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "s_month": 3,\
  "s_week": 4,\
  "s_day": 1,\
  "s_hour": 1,\
  "s_minute": 0,\
  "s_second": 0,\
  "e_month": 11,\
  "e_week": 1,\
  "e_day": 1,\
  "e_hour": 1,\
  "e_minute": 0,\
  "e_second": 0,\
  "offset": 60,\
  "enable": true,\
  "cookie": 1312994984\
}' \
-k https://10.88.0.235/dst\_set
```

Note:

Parameters	Type	Range
Cookie	Int	Recorded from Session Token
enable	Boolean	True/False
s_month	Int	1 to 12
s_week	Int	1 to 5
s_day	Int	1 to 7 (Sunday to Saturday)
s_hour	Int	0 to 23
s_minute	Int	0 to 59
s_second	Int	0 to 59
e_month	Int	1 to 12
e_week	Int	1 to 5
e_day	Int	1 to 31
e_hour	Int	0 to 23
e_minute	Int	0 to 59
e_second	Int	0 to 59
offset	Int	30/60

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/xhrhttpost.jsp
```

Screen Capture From Linux Box:

```
cis@ldap:~$ 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/xhrhttpost.jsp
{"uptstatus": 1}cis@ldap:~$
```

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/xhrhttpost.jsp
```

19. 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.

```
{
  "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

Screenshot from Postman Tool:

The screenshot displays a Postman interface for a POST request to `https://10.88.0.57/xhroutset.jsp`. The request body is raw JSON, and the response is also raw JSON.

Request Body (Raw):

```
1 {
2   "name": "OUTLET 2 - CHANGE_API",
3   "dlyon": 0,
4   "dlyoff": 0,
5   "id": 2,
6   "pduid": 1,
7   "start": 1,
8   "rebotdur": 5,
9   "cookie": 1859771896
10 }
```

Annotations in the image point to the `"name"` field (labeled "Outlet Name") and the `"id"` field (labeled "Outlet ID").

Response Body (Raw):

```
1 {
2   "uptstatus": 1
3 }
```

The interface includes tabs for Params, Authorization, Headers (9), Body (selected), Pre-request Script, Tests, and Settings. The Body tab is further divided into none, form-data, x-www-form-urlencoded, raw (selected), binary, GraphQL, and Text. The response view includes tabs for Body (selected), Cookies, Headers (7), and Test Results, with a Pretty view selected.

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
```

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
```



CURL 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

20. 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
```

CURL 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

21. 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 https://10.88.0.235/xhroutset.jsp
```

CURL 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 https://10.88.0.235/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

22. ETH1 Settings (eth0)

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{ "ipmode": 3, "ipautoconfiguration": 1, "ipaddress": "0.0.0.0", "netmask": "0.0.0.0", "gateway": "0.0.0.0", "ipv6_local_address": "", "ipv6_auto_address": "", "ipv6autoconfig": 1, "prefix_v6": 0, "gateway_v6": "::2:0:0", "cookie": 1312994984 }' -k https://10.88.0.235/xhrseteth1.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "ipmode": 3,\
  "ipautoconfiguration": 1,\
  "ipaddress": "0.0.0.0",\
  "netmask": "0.0.0.0",\
  "gateway": "0.0.0.0",\
  "ipv6_local_address": "",\
  "ipv6_auto_address": "",\
  "ipv6autoconfig": 1,\
  "prefix_v6": 0,\
  "gateway_v6": "::2:0:0",\
  "cookie": 1312994984\
}' \
-k https://10.88.0.235/xhrnetworkset.jsp
```

Note:

Parameters	Type	Range
Cookie	Int	Recorded from Session Token
Ipmode	Enum/int	1-IPv4, 2-IPv6, 3 -Both IPv4 and IPv6
ipautoconfiguration	Enum/int	0- Static, 1- Autoconfig
ipv6autoconfig	Enum/int	0- Static, 1- Autoconfig
ipaddress	string	64
netmask	string	64
Gateway	string	64
ipv6_local_address	string	64
ipv6_auto_address	string	64
prefix_v6	int	2096 (Usually prefix is from 0-128)
gateway_v6	string	64

23. ETH2 Settings (eth1)

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{ "ipmode": 3, "ipautoconfiguration": 1, "ipaddress": "0.0.0.0", "netmask": "0.0.0.0", "gateway": "0.0.0.0", "ipv6_local_address": "", "ipv6_auto_address": "", "ipv6autoconfig": 1, "prefix_v6": 0, "gateway_v6": "::2:0:0", "cookie": 1312994984 }' -k https://10.88.0.235/xhrseteth1.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "ipmode": 3,\
  "ipautoconfiguration": 1,\
  "ipaddress": "0.0.0.0",\
  "netmask": "0.0.0.0",\
  "gateway": "0.0.0.0",\
  "ipv6_local_address": "",\
  "ipv6_auto_address": "",\
  "ipv6autoconfig": 1,\
  "prefix_v6": 0,\
  "gateway_v6": "::2:0:0",\
  "cookie": 1312994984\
}\
-k https://10.88.0.235/xhrseteth1.jsp
```

Note:

Parameters	Type	Range
Cookie	Int	Recorded from Session Token
Ipmode	Enum/int	1-IPv4, 2-IPv6, 3 -Both IPv4 and IPv6
ipautoconfiguration	Enum/int	0- Static, 1- Autoconfig
ipv6autoconfig	Enum/int	0- Static, 1- Autoconfig
ipaddress	string	64
netmask	string	64
Gateway	string	64
ipv6_local_address	string	64
ipv6_auto_address	string	64
prefix_v6	int	2096 (Usually prefix is from 0-128)
gateway_v6	string	64

24. DNS

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"override_server": 0, "override_names": 0, "primary_dns": "0.0.0.0", "secondary_dns": "0.0.0.0", "hostname": "", "domain_name": "", "cookie": 1312994984}' -k https://10.88.0.235/xhrdnsset.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "override_server": 0,\
  "override_names": 0,\
  "primary_dns": "0.0.0.0",\
  "secondary_dns": "0.0.0.0",\
  "hostname": "",\
  "domain_name": "",\
  "cookie": 1312994984\
}' \
```

-k <https://10.88.0.235/xhrdnsset.jsp>

Note:

Parameters	Type	Range
Cookie	Int	Recorded from Session Token
override_server	enum/int	0-disable, 1-enable
override_names	enum/int	0-disable, 1-enable
Primary_dns	String	64
Secondary_dns	String	64
Hostname	String	64
Domain_name	String	64

25. HTTP / HTTPS Port

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"cookie": 1312994984, "gui_http_port": 80, "gui_https_port": 443, "gui_http_enable": false, "gui_https_enable": true, "redfish_enable": true}' -k https://10.88.0.235/xhrhttppost.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "cookie": 1312994984,\
  "gui_http_port": 80,\
  "gui_https_port": 443,\
  "gui_http_enable": false,\
  "gui_https_enable": true,\
  "redfish_enable": true\
}' \
```

-k <https://10.88.0.235/xhrhttppost.jsp>

Note:

Parameters	Type	Range
Cookie	Int	Recorded from Session Token
gui_http_port	Int	1-65535
gui_https_port	Int	1-65535
gui_http_enable	Boolean	True/False
gui_https_enable	Boolean	True/False
redfish_enable	Boolean	True/False

26. SSH Setting

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"sshPort": 22, "chkSshAcs": true, "cookie": 1312994984}' -k https://10.88.0.235/xhrsshpost.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "sshPort": 22,\
  "chkSshAcs": true,\
  "cookie": 1312994984\
}\
'\
-k https://10.88.0.235/xhrsshpost.jsp
```

Note:

Parameters	Type	Range
Cookie	Int	Recorded from Session Token
sshPort	Int	1-65535
chkSshAcs	Boolean	True/False

27. FTPS Setting

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{ "ftpport": 21, "chkftpac": true, "cookie": 312994984 }' -k https://10.88.0.235/xhrftppost.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{
  "ftpport": 21,
  "chkftpac": true,
  "cookie": 1312994984
}' \
-k https://10.88.0.235/xhrftppost.jsp
```

Note:

Parameters	Type	Range
Cookie	Int	Recorded from Session Token
Ftpport	Int	1-65535
chkftpac	Boolean	True/False

28. SYSLOG SERVER

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{ "syslogaddr": "10.10.104.250", "syslogport": 514, "chksyslog": 1, "syslogprotocol": 0, "syslogfile": "", "cookie": 348494352 }' -k https://10.88.0.235/xhrsyslogpost.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{
  "syslogaddr": "10.10.104.250",
  "syslogport": 514,
  "chksyslog": 1,
  "syslogprotocol": 0,
  "syslogfile": "",
  "cookie": 348494352
}' \
-k https://10.88.0.235/xhrsyslogpost.jsp
```

29. LOG CONFIGURATION

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"loginterval": 1, "logenable": 1, "cookie": 983243538}' -k https://10.88.0.235/xhrdatalogset.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '{
"loginterval": 1,
"logenable": 1,
"cookie": 1983243538
}' \
-k https://10.88.0.235/xhrdatalogset.jsp
```

Note:

Parameters	Type	Range
Cookie	Int	Recorded from Session Token
Loginterval	Int	1-1440
Logenable	Int/Flag	0 or 1

EMAIL SETUP

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"servername": "10.88.0.158", "username": "admin", "password": "12345678", "senderemail": "pdu@pdumgmt.com", "port": 25, "chkreqauth": 1, "timeintervalforretries": 6, "nosendingretries": 3, "cookie": 1312994984}' -k https://10.88.0.235/xhrsetsmtppost.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '{
"servername": "10.88.0.158",
"username": "admin",
"password": "12345678",
"senderemail": "pdu@pdumgmt.com",
"port": 25,
"chkreqauth": 1,
"timeintervalforretries": 6,
"nosendingretries": 3,
"cookie": 1312994984
}' \
-k https://10.88.0.235/xhrsetsmtppost.jsp
```

Note:

Parameters	Type	Range
Cookie	Int	Recorded from Session Token
Servename	string	Ipv4/Ipv6/FQDN, 63
Username	string	31
password	String/pwd	31
Senderemail	string	63
Port	Int	1-65535
Chkreqauth	Int/flag	0/1
Timeintervalforretries	Int	0-255
nosendingretries	int	0-255

30. ADD EMAIL USERS

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{ "receivers": [ { "enable": true, "address": pdu-admin@datacenter_admin.com" }, { "enable": false, "address": "" }, { "enable": false, "address": "" }, { "enable": false, "address": "" }, { "enable": false, "address": "" } ], "cookie": 1312994984 }' -k https://10.88.0.235/smtp_set
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '{ \n{\n  "receivers": [\n    {\n      "enable": true,\n      "address": "pdu-admin@datacenter_admin.com"\n    },\n    {\n      "enable": false,\n      "address": ""\n    },\n    {\n      "enable": false,\n      "address": ""\n    },\n    {\n      "enable": false,\n      "address": ""\n    },\n    {\n      "enable": false,\n      "address": ""\n    }\n  ],\n  "cookie": 1312994984\n}' \n-k https://10.88.0.235/smtp_set
```


Note:

Parameters	Type	Range
Cookie	Int	Recorded from Session Token
Servername	string	Ipv4/Ipv6/FQDN, 63
Username	string	31
password	String/pwd	31
Senderemail	string	63
Port	Int	1-65535
Chkreqauth	Int/flag	0/1
Timeintervalforretries	Int	0-255
nosendingretries	int	0-255

31. EVENT NOTIFICATIONS

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"SPSC": 0, "CALA": 196608, "WALA": 196608, "CBSC": 196608, "OLSC": 196608, "ESSC": 196608, "PDUC": 196608, "FMUP": 196608, "NCRS": 196608, "CSSC": 196608, "DCSC": 196608, "EBLM": 196608, "USRA": 196608, "PSWC": 196608, "ROSC": 196608, "USSC": 196608, "LDAP": 196608, "POWS": 196608, "CONF": 196608, "cookie": 200996683}' -k https://10.88.0.235/xhrevtruleset.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '{
{
    "SPSC": 0,
    "CALA": 196608,
    "WALA": 196608,
    "CBSC": 196608,
    "OLSC": 196608,
    "ESSC": 196608,
    "PDUC": 196608,
    "FMUP": 196608,
    "NCRS": 196608,
    "CSSC": 196608,
    "DCSC": 196608,
    "EBLM": 196608,
    "USRA": 196608,
    "PSWC": 196608,
    "ROSC": 196608,
    "USSC": 196608,
    "LDAP": 196608,
    "POWS": 196608,
    "CONF": 196608,
    "cookie": 200996683}' \
-k https://10.88.0.235/xhrevtruleset.jsp
```

Note:

EVENT ABBREVIATION	EVENT
CALA	Critical Alarm
WALA	Warning Alarm
CBSC	Circuit Breaker Status
OLSC	Outlet Status
ESSC	Sensor Status
PDUC	PDU Config
FMUP	Firmware Upgrade
NCRS	Network Reset
CSSC	Communication Status
DCSC	Daisy Status
EBLM	USB Status
SPSC	Server Status
USRA	User Activity
PSWC	Password Change
ROSC	Role Status
USSC	User Status
LDAP	Ldap Status
ROSC	Rack Status
POWS	Power Share Status
CONF	Config Item Status

Each item in above table should contain a value from below table based on selection

NOTIFICATIONS – ON/OFF	Value
EMAIL - OFF SNMP TRAP - OFF SYSLOG - OFF	0
EMAIL - OFF SNMP TRAP - OFF SYSLOG - ON	262144
EMAIL - OFF SNMP TRAP - ON SYSLOG - OFF	131072
EMAIL - ON SNMP TRAP - OFF SYSLOG - OFF	65536
EMAIL - OFF SNMP TRAP - ON SYSLOG - ON	393216
EMAIL - ON SNMP TRAP - OFF SYSLOG - ON	327680
EMAIL - ON SNMP TRAP - ON SYSLOG - OFF	196608
EMAIL - ON SNMP TRAP - ON SYSLOG - ON	458752

Examples Curl Commands:

Email – OFF | SNMP Trap – OFF | Syslog – OFF

```
curl -X POST -H "Content-Type: application/json" -d '{
"SPSC":0,"CALA":0,"WALA":0,"CBSC":0,"OLSC":0,"ESSC":0,"PDUC":0,"FMUP":0,"NCRS":0,"CSSC":0,"DCSC":0,"EBLM":0,"USRA":0,"PSWC":0,"ROSC":0,"USSC":0,"LDAP":0,"POWS":0,"CONF":0,"cookie":839063399}' -k
https://10.88.0.235/xhrevtruleset.jsp
```

Email – ON | SNMP Trap – ON | Syslog – ON

```
curl -X POST -H "Content-Type: application/json" -d '{"SPSC":0,"CALA":458752,"WALA":458752,"CBSC":458752,"OLSC":458752,"ESSC":458752,"PDUC":458752,"FMUP":458752,"NCRS":458752,"CSSC":458752,"DCSC":458752,"EBLM":458752,"USRA":458752,"PSWC":458752,"ROSC":458752,"USSC":458752,"LDAP":458752,"POWS":458752,"CONF":458752,"cookie":348494352}' -k
https://10.88.0.235/xhrevtruleset.jsp
```

Email – ON | SNMP Trap – OFF | Syslog – OFF

```
curl -X POST -H "Content-Type: application/json" -d '{"SPSC":0,"CALA":65536,"WALA":65536,"CBSC":65536,"OLSC":65536,"ESSC":65536,"PDUC":65536,"FMUP":65536,"NCRS":65536,"CSSC":65536,"DCSC":65536,"EBLM":65536,"USRA":65536,"PSWC":65536,"ROSC":65536,"USSC":65536,"LDAP":65536,"POWS":65536,"CONF":65536,"cookie":348494352}' -k
https://10.88.0.235/xhrevtruleset.jsp
```

Email – OFF | SNMP Trap – ON | Syslog – OFF

```
curl -X POST -H "Content-Type: application/json" -d '{"SPSC":0,"CALA":131072,"WALA":131072,"CBSC":131072,"OLSC":131072,"ESSC":131072,"PDUC":131072,"FMUP":131072,"NCRS":131072,"CSSC":131072,"DCSC":131072,"EBLM":131072,"USRA":131072,"PSWC":131072,"ROSC":131072,"USSC":131072,"LDAP":131072,"POWS":131072,"CONF":131072,"cookie":348494352}' -k
https://10.88.0.235/xhrevtruleset.jsp
```

Email – OFF | SNMP Trap – OFF | Syslog – ON

```
curl -X POST -H "Content-Type: application/json" -d '{"SPSC":0,"CALA":262144,"WALA":262144,"CBSC":262144,"OLSC":262144,"ESSC":262144,"PDUC":262144,"FMUP":262144,"NCRS":262144,"CSSC":262144,"DCSC":262144,"EBLM":262144,"USRA":262144,"PSWC":262144,"ROSC":262144,"USSC":262144,"LDAP":262144,"POWS":262144,"CONF":262144,"cookie":348494352}' -k
https://10.88.0.235/xhrevtruleset.jsp
```

Email – ON | SNMP Trap – ON | Syslog – OFF

```
curl -X POST -H "Content-Type: application/json" -d '
```

```
{"SPSC":0,"CALA":196608,"WALA":196608,"CBSC":196608,"OLSC":196608,"ESSC":196608,"PDUC":196608,"FMU  
P":196608,"NCRS":196608,"CSSC":196608,"DCSC":196608,"EBLM":196608,"USRA":196608,"PSWC":196608,"RO  
SC":196608,"USSC":196608,"LDAP":196608,"POWS":196608,"CONF":196608,"cookie":348494352}' -k
```

<https://10.88.0.235/xhrevtruleset.jsp>

Email – OFF | SNMP Trap – ON | Syslog – ON

```
curl -X POST -H "Content-Type: application/json" -d '
```

```
{"SPSC":0,"CALA":393216,"WALA":393216,"CBSC":393216,"OLSC":393216,"ESSC":393216,"PDUC":393216,"FMU  
P":393216,"NCRS":393216,"CSSC":393216,"DCSC":393216,"EBLM":393216,"USRA":393216,"PSWC":393216,"RO  
SC":393216,"USSC":393216,"LDAP":393216,"POWS":393216,"CONF":393216,"cookie":348494352}' -k
```

<https://10.88.0.235/xhrevtruleset.jsp>

Email – ON | SNMP Trap – OFF | Syslog – ON

```
curl -X POST -H "Content-Type: application/json" -d '
```

```
{"SPSC":0,"CALA":327680,"WALA":327680,"CBSC":327680,"OLSC":327680,"ESSC":327680,"PDUC":327680,"FMU  
P":327680,"NCRS":327680,"CSSC":327680,"DCSC":327680,"EBLM":327680,"USRA":327680,"PSWC":327680,"RO  
SC":327680,"USSC":327680,"LDAP":327680,"POWS":327680,"CONF":327680,"cookie":348494352}' -k
```

<https://10.88.0.235/xhrevtruleset.jsp>

32. TRAP RECEIVERS

V1:

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d
'{"cookie":348494352,"v1_trap_servers":[{"name":"icecubes","host":"5.5.5.5","port":162,"comm":"public","enable":true},{"name":"icecubes","enable":true,"host":"5.5.5.5","port":162,"comm":"public"},{"name":"","host":"","port":162,"comm":"public","enable":false},{"name":"","host":"","port":162,"comm":"public","enable":false},{"name":"","host":"","port":162,"comm":"public","enable":false}]} -k https://10.88.0.235/xhrsnmppost.jsp
```

CURL Command Formatted:

```
curl -X POST -H \
"Content-Type: application/json" \
-d\
{
    "cookie":348494352,
    "v1_trap_servers":[
        {
            "name":"icecubes",
            "host":"5.5.5.5",
            "port":162,
            "comm":"public",
            "enable":true
        },
        {
            "name":"icecubes",
            "enable":true,
            "host":"5.5.5.5",
            "port":162,
            "comm":"public"
        },
        {
            "name":"","
            "host":"","
            "port":162,
            "comm":"public",
            "enable":false
        },
        {
            "name":"","
            "host":"","
            "port":162,
            "comm":"public",
            "enable":false
        }
    ]
}
```

} \

-k <https://10.88.0.235/xhrsnmppost.jsp>

Note :

Parameters	Type	Range
Cookie	Int	Recorded from Session Token
Name	String	31
Enable	Boolean	True/False
Port	Int	1-65535
Comm	String	32
Host	String	Ipv4/ipv6 or an FQDN
V1_trap_servers	Array of Object	Up to 5 users

V3:

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"cookie": 1240545048,"v3_trap_servers": [{"name": "v3_user", "enable": true, "host": "5.5.5.5", "port": 162, "auth_type": 2, "password": "auth_password", "key": "privacy_key", "priv_algo": 3, "auth_algo": 0 }, {"host": "", "port": 162, "name": "", "auth_type": 0, "password": "", "key": "", "auth_algo": 0, "priv_algo": 3, "enable": false }, { "host": "", "port": 162, "name": "", "auth_type": 0, "password": "", "key": "", "auth_algo": 0, "priv_algo": 3, "enable": false }, {"host": "", "port": 162, "name": "", "auth_type": 0, "password": "", "key": "", "auth_algo": 0, "priv_algo": 3, "enable": false }, {"host": "", "port": 162, "name": "", "auth_type": 0, "password": "", "key": "", "auth_algo": 0, "priv_algo": 3, "enable": false } ]}' -k https://10.88.0.235/xhrsnmppost.jsp
```

CURL Command Formatted:

```
curl -X POST -H \
"Content-Type: application/json" \
-d \
{
"cookie": 1240545048,
"v3_trap_servers": [
{
"name": "v3_user",
"enable": true,
"host": "5.5.5.5",
"port": 162,
"auth_type": 2,
"password": "auth_password",
"key": "privacy_key",
"priv_algo": 3,
"auth_algo": 0
},
{
"host": "",
"port": 162,
"name": "",
"auth_type": 0,
"password": "",
"key": "",
"auth_algo": 0,
"priv_algo": 3,
"enable": false
},
{
"host": "",
"port": 162,
"name": "",
"auth_type": 0,
"password": "",
"key": "",
"auth_algo": 0,
"priv_algo": 3,
"enable": false
},
{
"host": "",
"port": 162,
"name": "",
"auth_type": 0,
"password": "",
"key": "",
"auth_algo": 0,
"priv_algo": 3,
"enable": false
}
]
```

```
"enable": false
},
{
  "host": "",
  "port": 162,
  "name": "",
  "auth_type": 0,
  "password": " ",
  "key": " ",
  "auth_algo": 0,
  "priv_algo": 3,
  "enable": false
},
{
  "host": "",
  "port": 162,
  "name": "",
  "auth_type": 0,
  "password": " ",
  "key": " ",
  "auth_algo": 0,
  "priv_algo": 3,
  "enable": false
}
]
}\
-k https://10.88.0.235/xhrsnmppost.jsp
```

Note :

Parameters	Type	Range
cookie	int	Recorded from Session Token
name	string	31
auth_type	int	2 - Auth Priv, 1 Auth No Priv, 0 No Auth No Priv
password	text/password	31
key	text/password	31
auth_algo	integer	0-MD5, 1-SHA
priv_algo	int	0-DES, 1-AES128, 2-AES192, 3-AES256
enable	boolean	True/False
Port	int	1-65535
Host	string	Ipv4/ipv6 or an FQDN

33. THRESHOLDS – Power Threshold

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"cookie": 910630780, "threshold": 0, "delay": 0, "pduid": 1, "lowcritical": 0, "lowwarning": 0, "upwarning": 0, "upcritical": 0, "cblowcritical": 1, "cblowwarning": 1, "cbupwarning": 1, "cbupcritical": 0}' -k https://10.88.0.235/xhrpdualarmset.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "cookie": 910630780,\
  "threshold": 0,\
  "delay": 0,\
  "pduid": 1,\
  "lowcritical": 0,\
  "lowwarning": 0,\
  "upwarning": 0,\
  "upcritical": 0,\
  "cblowcritical": 1,\
  "cblowwarning": 1,\
  "cbupwarning": 1,\
  "cbupcritical": 0\
}' \
-k https://10.88.0.235/xhrpdualarmset.jsp
```


Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
threshold	int	2147483000
delay	int	0-100
pduid	int	upto 64
lowcritical	int	0-2147483000
lowwarning	int	0-2147483000
upwarning	int	0-2147483000
upcritical	int	0-2147483000
cblowcritical	int	0/1
cblowwarning	int	0/1
cbupwarning	int	0/1
cbupcritical	int	0/1

34. THRESHOLDS – Current Threshold

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{ "lowcritical": 0, "lowwarning": 0, "upcritical": 8000, "upwarning": 22000, "threshold": 1000, "delay": 0, "cblowcritical": 1, "cbupwarning": 0, "cblowwarning": 1, "cbupcritical": 0, "cookie": 910630780, "pduid": 1, "phase": 2 }' -k https://10.88.0.235/xhripscurrentalarmset.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "lowcritical": 0,\
  "lowwarning": 0,\
  "upcritical": 28000,\
  "upwarning": 22000,\
  "threshold": 1000,\
  "delay": 0,\
  "cblowcritical": 1,\
  "cbupwarning": 0,\
  "cblowwarning": 1,\
  "cbupcritical": 0,\
  "cookie": 910630780,\
  "pduid": 1,\
  "phase": 2\
}' \
-k https://10.88.0.235/xhripscurrentalarmset.jsp
```

Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
threshold	int	1000
delay	int	0-100
pduid	int	upto 64
lowcritical	int	0-PDU Rating
lowwarning	int	0-PDU Rating
upwarning	int	0-PDU Rating
upcritical	int	0-PDU Rating
cblowcritical	int	0/1
cblowwarning	int	0/1
cbupwarning	int	0/1
cbupcritical	int	0/1
phase	int	1,2 and 3

35. THRESHOLDS – Voltage Threshold

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"lowcritical": 180000, "lowwarning": 190000, "upcritical": 260000, "upwarning": 250000, "threshold": 2000, "delay": 0, "cblowcritical": 0, "cbupwarning": 0, "cblowwarning": 0, "cbupcritical": 0, "cookie": 910630780, "pduid": 1, "phase": 2}' -k https://10.88.0.235/xhripsvoltagealarmset.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "lowcritical": 180000,\
  "lowwarning": 190000,\
  "upcritical": 260000,\
  "upwarning": 250000,\
  "threshold": 2000,\
  "delay": 0,\
  "cblowcritical": 0,\
  "cbupwarning": 0,\
  "cblowwarning": 0,\
  "cbupcritical": 0,\
  "cookie": 910630780,\
  "pduid": 1,\
  "phase": 2\
}' \
-k https://10.88.0.235/xhripsvoltagealarmset.jsp
```

Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
threshold	int	1000
delay	int	0-100
pduid	int	upto 64
lowcritical	int	0-PDU Rating
lowwarning	int	0-PDU Rating
upwarning	int	0-PDU Rating
upcritical	int	0-PDU Rating
cblowcritical	int	0/1
cblowwarning	int	0/1
cbupwarning	int	0/1
cbupcritical	int	0/1
phase	int	1,2 and 3

36. THRESHOLDS – Circuit Breaker Threshold

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"cookie": 910630780, "pduid": 1, "cb": 2, "dly": 0, "thld": 1000, "cblowc": 1, "cbloww": 1, "cbupc": 0, "cbupw": 0, "lowc": 0, "loww": 0, "upw": 14000, "upc": 16000}' -k https://10.88.0.235/xhrccbsalarmset.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "cookie": 910630780,\
  "pduid": 1,\
  "cb": 2,\
  "dly": 0,\
  "thld": 1000,\
  "cblowc": 1,\
  "cbloww": 1,\
  "cbupc": 0,\
  "cbupw": 0,\
  "lowc": 0,\
  "loww": 0,\
  "upw": 14000,\
  "upc": 16000\
}' \
-k https://10.88.0.235/xhrccbsalarmset.jsp
```

Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
thld	int	1000
dly	int	0-100
pduid	int	upto 64
lowc	int	
low	int	
upw	int	
upc	int	
cblowc	int/flag	0/1
cbloww	int/flag	0/1
cbupc	int/flag	0/1
cbupw	int/flag	0/1
cb	int	0 to upto 16

37. THRESHOLDS – Outlet Threshold

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{ "cblowcritical": 0, "cblowwarning": 1, "cbupcritical": 1, "cbupwarning": 1, "cookie": 910630780, "delay": 0, "id": 2, "lowcritical": 0, "lowwarning": 0, "pduid": 1, "threshold": 0, "upcritical": 0, "upwarning": 0}' -k https://10.88.0.235/xhroutalarmset.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '{ \
{
  "cblowcritical": 0,
  "cblowwarning": 1,
  "cbupcritical": 1,
  "cbupwarning": 1,
  "cookie": 910630780,
  "delay": 0,
  "id": 2,
  "lowcritical": 0,
  "lowwarning": 0,
  "pduid": 1,
  "threshold": 0,
  "upcritical": 0,
  "upwarning": 0
}' \
-k https://10.88.0.235/xhroutalarmset.jsp
```

Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
threshold	int	1000
delay	int	0-100
pduid	int	upto 64
lowcritical	int	
lowwarning	int	
upwarning	int	
upcritical	int	
cblowcritical	int	0/1
cblowwarning	int	0/1
cbupwarning	int	0/1
cbupcritical	int	0/1
id	int	1 to upto 64

38. THRESHOLDS – Detect Threshold Set

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"threshold": 130, "cookie": 910630780}' -k https://10.88.0.235/outlet\_detect\_threshold\_set
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "threshold": 130,\
  "cookie": 910630780\
}' \
-k https://10.88.0.235/outlet\_detect\_threshold\_set
```

Note:

Parameters	Type	Range
cookie	Int	Recorded from Session Token
threshold	int	0-200

CHANGE TEMPERATURE PREFERENCE

CURL Command:

```
curl -X POST -H "Content-Type: application/json" -d '{"cookie": 1761158407, "username": "admin", "temperature": 0}' -k https://10.88.0.235/xhrchangeTemperature.jsp
```

CURL Command Formatted:

```
curl -X POST -H "Content-Type: application/json" -d '\
{\
  "cookie": 1761158407,\
  "username": "admin",\
  "temperature": 0\
}' \
-k https://10.88.0.235/xhrchangeTemperature.jsp
```

Note:

Parameters	Type	Range
cookie	int	Recorded from Session Token
username	string	cookie should match the user session
temperature	int	0-Celsius, 1- Fahrenheit

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
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 /xhresetdevset.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 PDU 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 Stand alone PDU to perform a Firmware upload is anywhere in between 150-200 sec. 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.
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

```
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]
```

options:

CLI COMMANDS

EN2.0>?

sys: system setting

usage:

sys [date/time] [2012-09-11/14:16:20]

sys ntp [on/off]

sys ntp [server1] [server2]

sys ntp gmtoffset [UTCoffset/help]

sys [ver/def]

sys rst [pduid]

sys upd [conf/all]

sys log [del/edit] [event/data] [on/off] [interval]

sys dualinput get

sys dualinput set [NA/EMEA]

sys cordtype [TYPE]

sys updatehid [motor/rfid] [pduid] [0(hot)/ 1(cold)]

sys updatercm rcm

sys ledcolor

sys ledcolor [pduid]/all] [red/green/yellow/blue/pink/cyan/white/dark]

user: user setting

usage:

usr list

usr login

usr unlock [username]

usr options [interactive/non-interactive]

[add/del/edit]

[username]

[password]

[confirm_password]

[role:admin/user/manager]

usr roleoptions [interactive/non-interactive]

[add/del/edit]

[rolename]

[Admin Privilege required? : yes/no]

[roledescription]

usr rolelist

usr pwdpolicy [interactive/non-interactive]

[get/set]

[pwd_age_interval : | 7 | 14 | 30 | 60 | 90 | 180 | 365 | Never Expire |]

[min_len]

[max_len]

[at least 1 lower character must be in password: yes/no]

[at least 1 upper character must be in password: yes/no]

[at least 1 numerical character must be in password: yes/no]

[at least 1 special character must be in password: yes/no]

usr sessionmgmt [interactive/non-interactive]

[get/set]

[sign in retries allowed? : yes/no]

[number_retry: 3 to 10]

[sesssion_timeout from list: | 1 | 10 | 20 | 30 | 60 | 120 | 240 | 360 | 720 | 1440 |]

[lockout_time from list : | 1 | 2 | 3 | 4 | 5 | 10 | 15 | 20 | 30 | 60 | 120 | 240 | 360 | 720 | infinite

|]

net: network configuration command

usage:

```
net [ssh/telnet/ftps/http/https/redfish/redirect] [on/off]
net telnet [on/off]
net telnet port [portnumber]
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 scp <full_localfilepath> <remoteuser>@<remotehost> <full_remotefilepath>
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]
net eap [eth0/eth1] [enable/disable] outer TLS identity [Identity] passphrase [private key passphrase]
net eap [eth0/eth1] [enable/disable] outer PEAP inner TLS identity [Identity] passphrase [private key
passphrase]
net eap [eth0/eth1] [enable/disable] outer PEAP inner MSCHAP identity [Identity] password [password]
```

dev: device setting

usage:

```
dev daisy [rna/qna] [init] [create]
dev outlet [pduID] status
dev outlet [pduID] [outletindex/outletname] get status
dev outlet [pduID] [outletindex/outletname] set [outletname/poweronstate/ondelay/offdelay/rebootdelay]
[name/value]
dev outlet [pduID] [outletindex/outletname] [on/off/ondelay/offdelay/rebootdelay/reboot]
dev outletgroups list
dev outletgroups [groupindex/groupname] get status
dev outletgroups add [groupname] [pduID] [outlets]
dev outletgroups edit [groupindex/groupname] [pduID] [outlets]
dev outletgroups del [groupindex/groupname]
dev outletgroups [groupindex/groupname] [on/off/reboot]
dev usb [on/off]
```



```
dev sensor unit [pduid]
dev ledstrip [on/off]
dev powershare
dev powershare [pduID] func [on/off]
dev handle [pduID] [cold/hot] [lock/unlock]
dev hid [cold/hot] [lock/unlock]
dev tempscale [get/set] [c/f]
dev rcm [PDUID] [status/fwver/hwver/selftest [start/result]]
dev olp [pduID] get
dev olp [pduid] set [LoadRating OverloadThreshold ResetTimer]
dev olp [pduID] [on/off]
```

pwr: pdu information

usage:

```
pwr unit [idx]
pwr [outlet/phase/cb] [pduid] [idx]
pwr rcm [pduid]
```

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/ time] [hh:mm:ss]	Query on PDU date and time	EN2.0>sys date SUCCESS Date:2024-05-17 Time:00:11:46 EN2.0>SUCCESS Date:2024-05-17 Time:00:12:06
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 [server1] [server2]	Sets the NTP It is required that the valid primary IP address is added, but the secondary IP address is not mandatory.	EN2.0>sys ntp 129.6.15.28 129.6.15.29 SUCCESS
sys ntp gmtoffset [UTCoffset]	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.	EN2.0>sys ntp gmtoffset +05:31 SUCCESS Reboot required for change to take effort System Reboot now, Are you sure?(Y/N):
sys ntp gmtoffset help	NTP help string to display the UTC code for every offset of all the region	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
sys ntp gmtoffset	Displays the current NTP offset of the PDU	EN2.0>sys ntp gmtoffset SUCCESS GMT Name : Chennai, Kolkata, Mumbai, Delhi GMT Offset : UTC+05:30

Sys Commands	Description	Example
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 rst [pduid]	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 dualinput get	Displays the current region of the PDU	EN2.0>sys dualinput get SUCCESS EMEA rating is active Rating: 346–415 V, 32 A, 22.0 kVA, 50/60 Hz
sys dualinput set [NA/EMEA]	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 cordtype sys cordtype [type] ys cordtype help	Displays the SKU/cord type information set User can select one of the available cord types Command gives us the list of available SKU/cord types	EN2.0>sys cordtype SUCCESS SKU : EN13UA_20A3WYE EN2.0>sys cordtype 16A3WYE SUCCESS SKU : EN13UA_16A3WYE

Sys Commands	Description	Example
sys updatehid [motor/rfid] [pduid] [0(hot)/ 1(cold)]	Updates the handle rfid or motor firmware	EN2.0>sys updatehid motor 1 1 Updating HID motor firmware, please wait... Handle update is SUCCESS, PDU will reboot now EN2.0>sys updatehid rfid 1 1 Updating HID RFID firmware, please wait... Handle update is SUCCESS, PDU will reboot now
sys updatercm rcm	Updates the RCM firmware using the rcm.bin to the fw folder	EN2.0> sys updatercm rcm Updating RCM firmware, please wait... EN2.0> sys updatercm rcm Updating RCM firmware, please wait RCM update is SUCCESS, PDU will reboot now
sys ledcolor	Displays color of the LED	EN2.0>sys ledcolor SUCCESS ledcolor: blue
sys ledcolor [pduid]/all [dark/ red/green/yellow/blue/ pink/ cyan/white]	Update color of LED	EN2.0>sys ledcolor pduid dark SUCCESS

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 redirect [on/off]	Sets port redirection On or Off	EN2.0>net redirect on SUCCESS Status: ON EN2.0>net redirect off SUCCESS Status: OFF
net telnet [on/off]	Sets telnet on/off	EN2.0>net telnet on SUCCESS Reboot required for change to take effect System Reboot now, Are you sure?(Y/N): Y

Net Commands	Description	Example
net telnet port	Sets the port number for TELNET	EN2.0>net telnet port 23 Reboot required for change to take effect Telnet port is changed, Please reboot to validate System Reboot now, Are you sure?(Y/N): Y
net snmp [v1v2c/v3] [on/off]	Sets SNMP On or Off	EN2.0>net snmp v1v2c: on / net snmp v3: on SUCCESS EN2.0>net snmp v1v2c off / net snmp v3: off SUCCESS
net snmp port[portnumber]	Sets SNMP port number	EN2.0>>net snmp port 162 Reboot required for change to take effect SNMP port is changed, Please reboot to validate system Reboot now, Are you sure? (Y/N): Y
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 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 Commands	Description	Example
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 scp <full_localfilepath> <remoteuser>@ <remotehost> <full_remotefilepath>	Copies the event logs to the specified system	EN2.0>net scp SUCCESS : scp enabled EN2.0>net scp /system/log/eventlog.txt buildserver@10.10.105.255/home/buildserver The authenticity of host '10.10.105.255 (10.10.105.255)' can't be established. ED25519 key fingerprint is SHA256:F+FVTej0G4bvsDzOnx9jSklo77LQcduF1BCFCZFwuhM. This key is not known by any other names Are you sure you want to continue connecting (yes/no/[fingerprint])? Yes Warning: Permanently added '10.10.105.255' (ED25519) to the list of known hosts. buildserver@10.10.105.255's password: eventlog.txt 100% 11 KB 739.8 KB/s 00:00 File successfully uploaded.
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 Commands	Description	Example
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):
net eap	Displays the current authentication information	EN2.0>net eap SUCCESS ETH0 AUTH :EAP-TLS ETH0 IDENTITY :SmartPower ETH1 AUTH :EAP-TLS ETH1 IDENTITY :SmartPower

Net Commands	Description	Example
net eap [eth0/eth1] [enable/disable] outer TLS identity [Identity] passphrase [private key passphrase]	Setting the an authentication information for EAP-TLS configuration to any specific ethernet port. Note – Upload CA Certificate, Client Key and Client Certificate via FTPS, before setting via CLI.	EN2.0>net eap eth0 enable outer TLS identity system_bangalore_center01 passphrase smartpower SUCCESS Reboot required for change to take effect Network is reconfigured, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y
net eap [eth0/eth1] [enable/disable] outer PEAP inner TLS identity [Identity] passphrase [private key passphrase]	Setting the an authentication information for PEAP-TLS configuration to any specific ethernet port. Note – Upload CA Certificate, Client Key and Client Certificate via FTPS, before setting via CLI.	EN2.0>net eap eth0 enable outer PEAP inner TLS identity system_bangalore_center01 passphrase smartpower SUCCESS Reboot required for change to take effect Network is reconfigured, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y
net eap [eth0/eth1] [enable/disable] outer PEAP inner MSCHAP identity [Identity] password [password]	Setting the an authentication information for PEAP-MSCHAPV2 configuration to any specific ethernet port. Note – Upload CA Certificate via FTPS, before setting via CLI.	EN2.0>net eap eth1 enable outer PEAP inner MSCHAP identity system_bangalore_center01 passphrase smartpower SUCCESS Reboot required for change to take effect Network is reconfigured, Please reboot to validate System Reboot now, Are you sure?(Y/N):Y

USR COMMANDS

Usr Commands	Description	Example
usr list	Lists out the PDU users	<pre>EN2.0>usr list SUCCESS Usr Role Privilege Role id ===== admin Administrator 1 user 2 manager Administrator 3</pre>
usr login	Displays the logged in user details	<pre>EN2.0>usr login SUCCESS username: admin ip address: 10.10.94.211 client type: SSH</pre>
usr unlock [username] usr options [interactive/non- interactive] [add/del/edit] [username] [password] [confirm_passwo rd] [role:admin/user/manag er]	Unlocks the blocked user Add Users and set credentials, define roles using interactive and non- interactive method.	<pre>EN2.0>usr unlock en_user SUCCESS EN2.0>usr options INTERACTIVE APPROACH* usr options interactive add/edit/del username password Confirm_pass word admin/user/manager NON-INTERACTIVE APPROACH** usr options non-interactive add/edit/del username password confirm_password (admin/manager/user)</pre>

Usr Commands	Description	Example
usr roleoptions [interactive/non-interactive] [add/del/edit] [rolename] [Admin Privilege required? : yes/no] [roledescription]	Add Users and set credentials, define roles and privileges using interactive and non-interactive method.	<pre> EN2.0>usr roleoptions INTERACTIVE APPROACH* usr roleoptions interactive add/del/edit rolename admin privilege yes/no role description NON-INTERCTIVE APPROACH** usr roleoptions non- interactive add/del/edit rolename admin privilege(yes/no) role description </pre>
usr rolelist	Displays the rolist with privilege and role descriptions.	<pre> EN2.0>usr rolelist SUCCESS Role Privilege Role Description ===== admin admin admin operation user user user operation manager admin redfish user </pre>

Usr Commands	Description	Example
usr pwdpolicy [interactive/non-interactive] [get/set] [pwd_age_interval : 7 14 30 60 90 180 365 Never Expire] [min_len] [max_len] [at least 1 lower character must be in password: yes/no] [at least 1 upper character must be in password: yes/no] [at least 1 numerical character must be in password: yes/no] [at least 1 special character must be in password: yes/no]	Get/Set data for the password fields as per user requirements in two approaches – interactive or non- interactive	EN2.0>usr pwdpolicy [interactive/non-interactive] [get/set] INTERACTIVE APPROACH* usr pwdpolicy interactive get/set [pwd_age_interval : 7 14 30 60 90 180 365 Never Expire] [min_len] [max_len] [at least 1 lower character must be in password: yes/no] [at least 1 upper character must be in password: yes/no] [at least 1 numerical character must be in password: yes/no] [at least 1 special character must be in password: yes/no] NON_INTERACTIVE ** usr pwdpolicy non-interactive set/get [pwd_age_in terval [min_len] [max_len] [at least 1 lower character must be in password: yes/no] [at least 1 upper character must be in password: yes/no] [at least 1 numerical character must be in password: yes/no] [at least 1 special character must be in password: yes/no]
usr sessionmgmt [interactive/non-interactive] [get/set] [sign in retries allowed? : yes/no] [number_retry: 3 to 10] [sesssion_timeout from list: 1 10 20 30 60 120 240 360 720 1440] [lockout_time from list : 1 2 3 4 5 10 15 20 30 60 120 240 360 720 infinite]	Get/Set data for the sessions management as per user requirements in two approaches – interactive or non-interactive	Apc>usr sessionmgmt [interactive/non-interactive] [get/set] INTERACTIVE APPROACH* usr sessionmgmt interactive get/set [sign in retries allowed?: yes/no] [number_retry: 3 to 10] [sesssion_timeout from list: 1 10 20 30 60 120 240 360 720 1440] [lockout_time from list : 1 2 3 4 5 10 15 20 30 60 120 240 360 720 infinite] NON-INTERACTIVE APPROACH** usr sessionmgmt non-interactive get/set

		[sign in retries allowed? : yes/no] [number_retry: 3 to 10] [sesssion_timeout from list: 1 10 20 30 60 120 240 360 720 1440] [lockout_time from list : 1 2 3 4 5 10 15 20 30 60 120 240 360 720 infinite]
--	--	---

INTERACTIVE APPROACH*

When the user selects an Interactive Approach, user will be prompted for each parameter/option to perform the respective action.

NON-INTERACTIVE APPROACH**

When the user selects a Non-Interactive Approach, user needs to enter all the parameters as per the syntax in a single line.

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/outletname] [get] [status] >> dev outlet [pduID] [outletindex] get status >> dev outlet [pduID] [outletname] [get] [status]	Displays the status of the PDU Outlets	EN2.0>dev outlet 1 status SUCCESS Relay Outlet S.No : Name : Status : OnDelay : OffDelay : RebootDelay : PowerOnState 1 : OUTLET1 : Close : 7200 : 7200 : 60 : ON 2 : OUTLET2 : Open : 0 : 0 : 5 : ON 3 : OUTLET 3 : Open : 0 : 0 : 5 : ON 4 : OUTLET 4 : Open : 0 : 0 : 5 : ON 5 : OUTLET 5 : Open : 0 : 0 : 5 : ON 6 : OUTLET 6 : Open : 0 : 0 : 5 : ON 7 : OUTLET 7 : Open : 0 : 0 : 5 : ON 8 : OUTLET 8 : Open : 0 : 0 : 5 : ON 9 : OUTLET 9 : Open : 0 : 0 : 5 : ON 10 : OUTLET10 : Open : 0 : 0 : 5 : ON

Dev Commands	Description	Example
<pre>dev outlet [pduID] [outletindex/outletname] [set] >>dev outlet [pduID] [outletindex] [set] [outletname] [name] >>dev outlet [outletname/ poweronstate/ondelay/off delay/rebootdelay] [name/on/ off/value] >>dev outlet [pduID] [outletindex/outletname] [set] poweronstate [on/off/ lastknown] >>dev outlet [pduID] [outletindex/outletname] [set] ondelay/offdelay/rebootdelay value</pre>	<p>Displays the status of the PDU</p> <p>Outlets with reference to outlet index, outlet name, power state, on delay, off delay and reboot delay</p>	<pre>EN2.0>dev outlet 1 outletname set outlet42 SUCCESS EN2.0>dev outlet 1 outlet42 set outletname OUTLET42OUTLET42 SUCCESS EN2.0>dev outlet 1 outlet42/ 42 set poweronstate on SUCCESS EN2.0>dev outlet 1 outlet42 set poweronstate off SUCCESS EN2.0>dev outlet 1 outlet42 set poweronstate lastknown SUCCESS EN2.0>dev outlet 1 42 set ondelay 7200 SUCCESS EN2.0>dev outlet 1 42 set offdelay 7200 SUCCESS EN2.0>dev outlet 1 42 set rebootdelay 60 SUCCESS</pre>
<pre>dev outlet pduID [outletindex] [on/off/rebootdelay/ ondelay/ offdelay]</pre>	<p>Command to Turn on/off/off delay/ ondelay/rebootdelay the outlet power</p>	<pre>EN2.0>dev outlet 1 1 on SUCCESS EN2.0>dev outlet 1 1 rebootdelay SUCCESS</pre>

Dev Commands	Description	Example
dev outletgroups list	Lists the Outlet Group Names	<pre>EN2.0>dev outletgroups list SUCCESS Idx Group Name ----- 1 Group1 2 Group2</pre>
dev outletgroups [groupindex/groupname] get status	Gets the details of the outlet groups on the basis of Group index or Group name	<pre>EN2.0>dev outletgroups Group1 get status SUCCESS Group name: Group1 Group id: 1 Group Members: PDU 1:1-Open 3-Open 5-Open 7-Open 9-Open 11-Open 13-Open 15-Open 17-Open 19-Open 21-Open 23-Open 25-Open 27-Open 29-Open 31-Open PDU 3:2-Open 4-Open 6-Open 8-Open 10-Open Group Active Power : 0.000W Group Apparent Power : 0.000W</pre>
dev outletgroups add [groupname] [pduID] [outlets]	Add Group names and Group the outlets in each of the PDUs Use a semi colon separator to add multiple outlets to the same Group name.	<pre>EN2.0>dev outletgroups add Group3 1 2,4,6,8,10; 2 1,3,5,7,9; SUCCESS</pre>
dev outletgroups edit [groupindex/groupname] [pduID] [outlets]	Edit Group and Group outlets in each of the PDUs Use a semi colon separator to add multiple outlets details to be edited.	<pre>EN2.0>dev outletgroups edit Group3 1 2,4,6,8; SUCCESS</pre>
dev outletgroups del [groupindex/groupname]	Deletes the outlet group name or index specified.	<pre>EN2.0>dev outletgroups del Group3 SUCCESS</pre>
dev outletgroups [groupindex/groupname] [on/off/reboot]	Outlets grouped together can be switched On or Off or Rebooted by specifying the group name.	<pre>EN2.0>dev outletgroups Group3 on SUCCESS EN2.0>dev outletgroups Group3 off SUCCESS EN2.0>dev outletgroups Group3 reboot SUCCESS</pre>

Dev Commands	Description	Example
dev usb [ON/OFF]	Turn on/off the USB	EN2.0>dev usb on SUCCESS
dev sensor unit [pdu id]	Lists out the connecte d sensors on PDU	EN2.0>dev sensor unit 2 SUCCESS Idx Name Type Serial No. Value 0 TEMPERATURE1PDU2 TEMP CAWELK0170 27.0C 1 TEMPERATURE2PDU2 TEMP CAWELK0170 27.0C 2 HUMIDITYPDU2 HUM I CAWELK0170 47% 3 TEMPERATURE3PDU2 TEMP CAWELK0170 26.0C 4 Sigma_T4 TEMP C25JB00002 27.0C 5 Sigma_H1 HUM I C25JB00002 45%
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 powershare [pduID] func [on/off]	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

Dev Commands	Description	Example
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 tempscale [get/set] [c/f]	Display information about the Temperature scale and set the temperature scale unit	EN2.0>dev tempscale get SUCCESS Temperature Scale : Celsius EN2.0>dev tempscale set f SUCCESS
dev rcm [PDUID] [status/fwver/hwver/selftest [start/result]]		<p>EN2.0>dev rcm 1 status RCM support is enabled for PDU 1 RCM Communication status is OK SUCCESS</p> <p>EN2.0>dev rcm 1 fwver RCM Firmware version :53 SUCCESS</p> <p>EN2.0>dev rcm 1 hwver RCM Hardware version :16 SUCCESS</p> <p>EN2.0>dev rcm 1 selftest start RCM self test initiated successfully for PDU 1 SUCCESS</p> <p>EN2.0>dev rcm 1 selftest result Last Self Test has Passed SUCCESS</p>

Dev Commands	Description	Example
dev olp [pduID] get	Get Overload Prevention configured values.	EN2.0>dev olp 1 get SUCCESS PDU 1 OLP status: OverLoad Prevention is disabled OLP load rating: 60 OLP Threshold : 5 OLP reset timer: 60 EN2.0>
dev olp [pduid] set [LoadRating OverloadThreshold ResetTimer]	Set the Overload Prevention values.	EN2.0>dev olp 1 set Load Rating should be b/w 1 VA and Max SKU Power rating in VA
dev olp [pduID] [on/off]	Enable or disable the Overload Prevention values.	EN2.0>dev olp 1 on SUCCESS EN2.0>

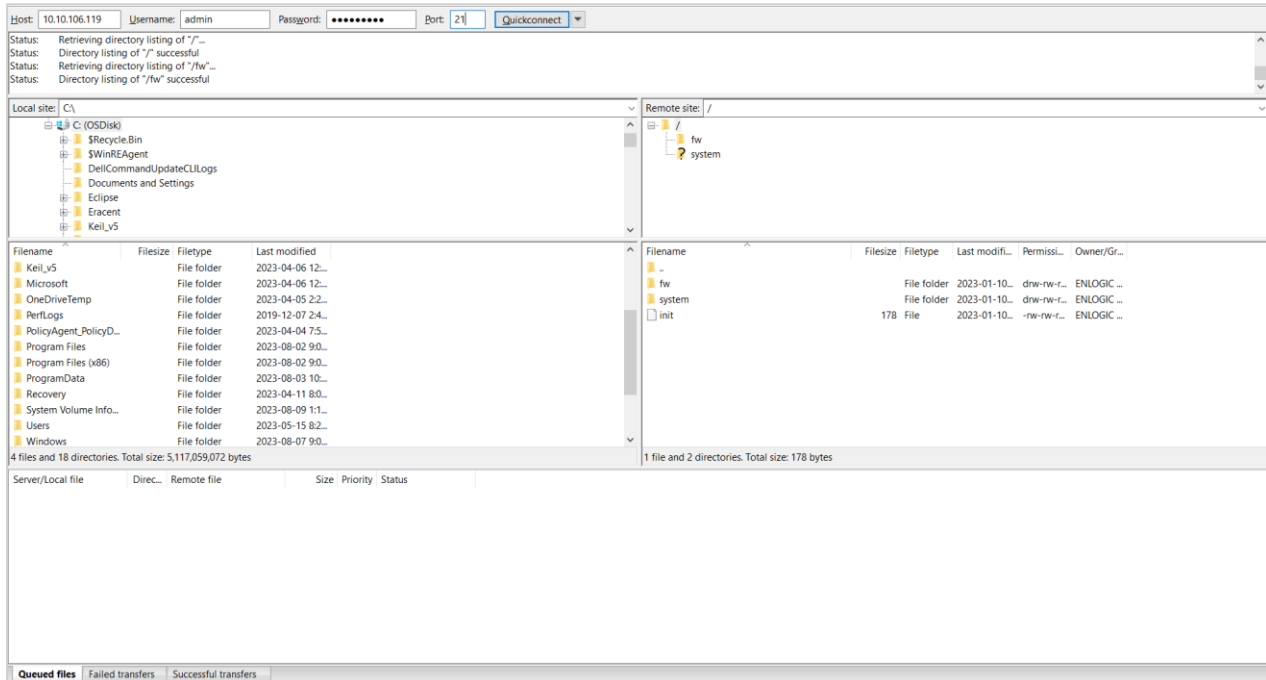
PWR COMMANDS

Dev Commands	Description	Example
pwr unit [idx]	Displays Power readings for the PDU	EN2.0>pwr unit 2 SUCCESS UNIT power Feature voltage : 217.0 V current : 0.0 A activepower : 0.0 W apparentpower : 0.0 VA powerfactor : 1.00 energy : 0.201 kWh
pwr [outlet/phase/cb] [pduid] [idx]	Displays the power readings	EN2.0>pwr outlet 1 3 SUCCESS PDU ID 1 : OUTLET 3 power Feature voltage : 0.0V current : 0.0A activepower : 0.0W apparentpower : 0.0VA powerfactor : 0.00 energy : 0.000kWh EN2.0>pwr phase 1 2 SUCCESS PDU ID 1 : PHASE 2 power Feature voltage : 0.0V current : 0.0A activepower : 0.0W apparentpower : 0.0VA powerfactor : 1.00 energy : 0.000kWh EN2.0>pwr cb 1 3 SUCCESS PDU ID 1 : CB 3 power Feature voltage : 0.0V current : 0.0A activepower : 0.0W apparentpower : 0.0VA powerfactor : 1.00 energy : 0.000kWh
pwr rcm [pduid]	Display RCM Current for the PDU	EN2.0>pwr rcm 1 RCM CURRENT:3 mA

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



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
- Air flow Sensor
- Alarm Beacon Sensor
- RJ45-DB9 Cable
- USB to RS232 Cable
- HID RACK Access kit
- ehandle with RFID
- ehandle with RFID + PIN

SENSOR OVERVIEW

nVent 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.

nVent 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 nVent 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
5. Advantage Secure User Manual for instructions on how to create custom cord lengths using the RJ45 Quick Disconnect Coupler.

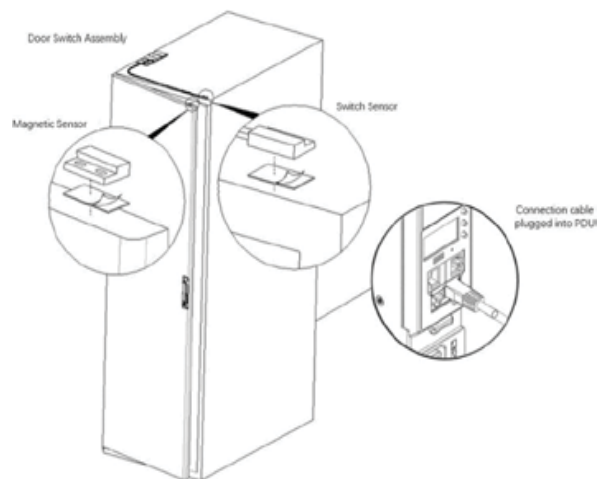
Note: Use either the 1.8m Ethernet cable included with the Enlogic sensor or any other CAT5 or CAT6 Ethernet cable with a standard RJ45 plug.

6. 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)

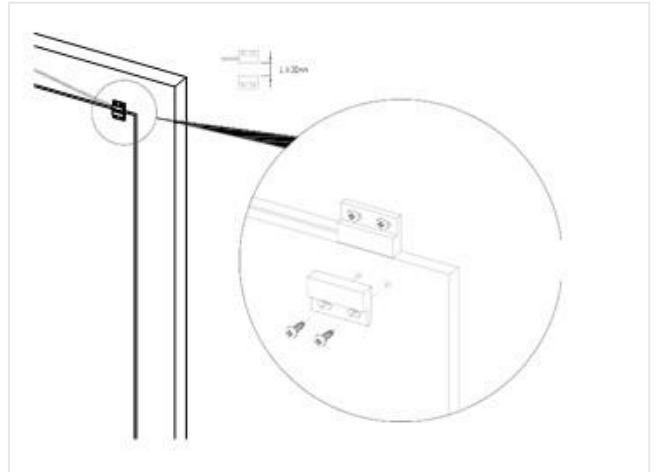
Top Door Mounting Option

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 door 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 10 mm.



DRY CONTACT CABLE INSTALLATION INSTRUCTIONS (EA9110)

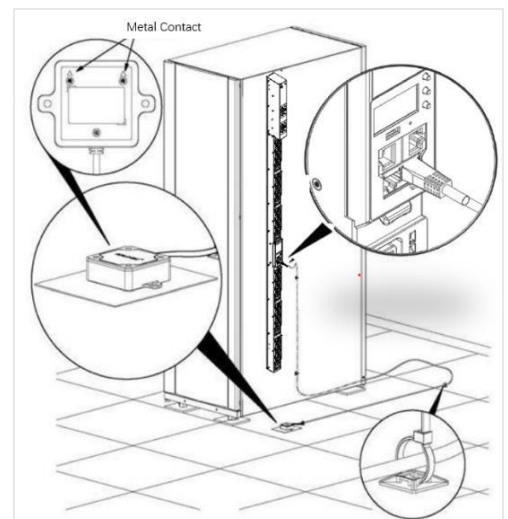
1. Attach the open wire leads on the dry contact cable to a dry contact sensor. Refer to instructions for the dry contact sensor for this step.
2. Connect the RJ-45 jack of the nVent Enlogic Dry Contact Cable to a sensor port on the PDU, Inline Energy Meter, or Sensor Hub (model EA9106).
3. Go to the nVent 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 nVent Enlogic iPDU, Inline Energy Meter, or Sensor Hub (model EA9106).
3. Go to the nVent 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:

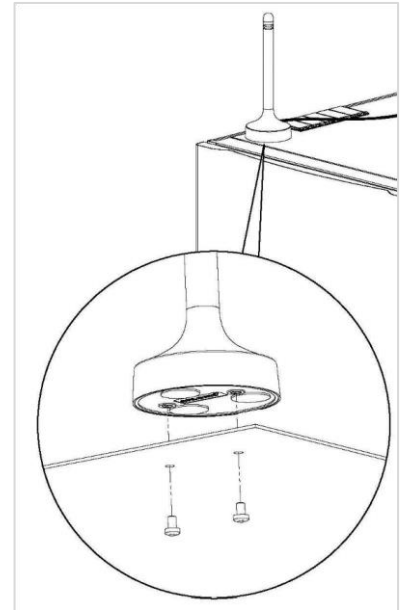
- The wire mount (shown here) is for installation on the floor or ground surface. This must be used in the detection area.
- If mounting to a cabinet or wall, use the adhesive-backed mount (provided). The adhesive backed is mounted in the detection area to prevent and notify delay leakage.

AIR FLOW SENSOR INSTALLATION INSTRUCTIONS (EA9205)

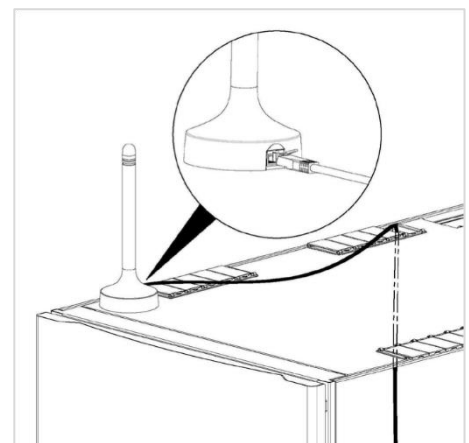
18. Secure the sensor box to the perforated rack enclosure door by threading a cable tie through the recessed channel in the sensor box and through the door.
19. Note: There are two recessed channels on the back of the sensor box which also includes a magnet to help secure the sensor.
20. Connect the RJ45 cable along the desired path to the PDU using the remaining cable ties.
21. Use the RJ45 Quick Disconnect Coupler of the sensor input cable and/or to serve as an easy disconnect point for rack door removal. Refer to the EN Series User Manual for instructions on how to create custom cord lengths using the RJ45 Quick Disconnect Coupler.
22. Secure the cable to the vicinity of the MEMS flow sensor using cable ties.

ALARM BEACON INSTALLATION INSTRUCTIONS (EA9101)

23. The Enlogic Alarm Beacon is designed to create a visible alarm notification of a trouble condition (or other user-defined situation) in an effort to notify personnel quickly and efficiently. The Alarm Beacon can be extended (up to 30.5 m) using a standard RJ-45 coupling.
24. Attach the Alarm Beacon to the top of the rack using the attached magnet or M5 screws.
25. Connect the network cable (EW00133) to the Alarm Beacon. Thread this cable down through the rack.



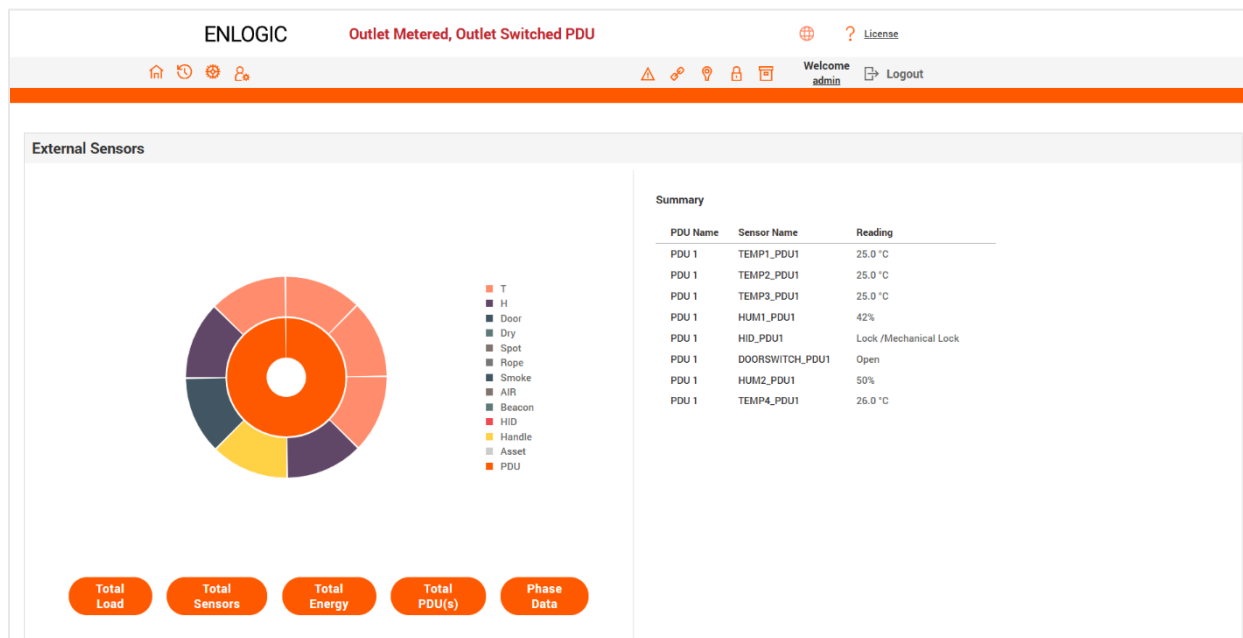
26. Plug the other end of the network cable into the Sensor 1 or Sensor 2 port on the PDU/Inline Energy Meter or the Sensor Hub



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



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

The screenshot shows the ENLOGIC web interface. At the top, there is a navigation bar with the ENLOGIC logo, a status indicator 'Outlet Metered, Outlet Switched PDU', and a 'License' link. Below the navigation bar, there is a 'Welcome admin' message and a 'Logout' button. The main content area is titled 'Identification' and is divided into three sections: System Information, PDU Information, and External Sensors.

System Information

Name	Value	Name	Value
System Name		MAC Address	C8-42-44-99-2B-35
Contact Name		IPv4 Address	10.20.15.82
Contact Email		IPv6 Link Local Address	fe80:6492:1d9e:6437:499
Contact Phone		IPv6 Auto Configured Address	2001:1111:1111:1121:debe:84:6:9887:772f
Contact Location			

PDU Information

PDU1 1-1

1	Name	-
	Cable Location	-
	Cable U Position	-
	Model	300-240V, 40A, 14.4kVA, 50/60Hz
	Part Number	ES6001
	Serial Number	
	Boot Version	1.2
	Web Version	3.0.6
	Firmware Version	3.2.4.D
	Hardware Version	
	PDU Power Rating (kVA)	14.4
	PDU Input Rating (A)	40
	PDU Breaker Rating (A)	20

External Sensors

External Sensors, Type	Sensor Name	Serial Number	Sensor ID	PDU	Location
Temperature	TEMP1_PDU1	AWELK0247	1	PDU#1	
Temperature	TEMP2_PDU1	AWELK0247	2	PDU#1	
Temperature	TEMP3_PDU1	AWELK0247	3	PDU#1	
Humidity	HUM1_PDU1	AWELK0247	4	PDU#1	
Handle	HDL_PDU1	N012590A3	5	PDU#1	Hot Aisle
Door	DOORSWITCH_PDU1	N012590A3	6	PDU#1	Hot Aisle
Humidity	HUM2_PDU1	N012590A3	7	PDU#1	Hot Aisle
Temperature	TEMP4_PDU1	N012590A3	8	PDU#1	Hot Aisle

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.

ENLOGIC
Outlet Metered, Outlet Switched PDU
License

Home, Refresh, Settings, Users
Alerts, Lock, Light, Padlock, Document
Welcome admin Logout

PDU Thresholds

Device Detection Threshold

Threshold(mA) 150

Power Threshold
Input Phases
Circuit Breaker
Control Management
External Sensors
Phase Power
Overload Prevention

External Sensors(1:1)	
Name	TEMP1_PDU1
Type	Temperature
Low Critical	15
Low Warning	34
High Warning	35
High Critical	36

External Sensors(1:2)	
Name	TEMP2_PDU1
Type	Temperature
Low Critical	15
Low Warning	34
High Warning	35
High Critical	36

External Sensors(1:3)	
Name	TEMP3_PDU1
Type	Temperature
Low Critical	15
Low Warning	33
High Warning	36
High Critical	38

External Sensors(1:4)	
Name	HUM1_PDU1
Type	Humidity
Low Critical	20
Low Warning	50
High Warning	60
High Critical	80

External Sensors(1:6)	
Name	DOORSWITCH_PDU1
Type	Door
Value	Off

External Sensors(1:7)	
Name	HUM2_PDU1
Type	Humidity
Low Critical	10
Low Warning	10

External Sensors(1:8)	
Name	TEMP4_PDU1
Type	Temperature
Low Critical	0
Low Warning	0

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

The screenshot shows the ENLOGIC User Settings page. At the top, the header includes 'ENLOGIC', 'Outlet Metered, Outlet Switched PDU', and a 'License' link. Below the header, there are navigation icons and a 'Welcome admin' message with a 'Logout' button. The main content area is titled 'User Settings' and features a temperature unit toggle set to '°C'. There are two buttons: 'Add Role' and 'Add User'. The page is divided into several sections:

- Users:** A table with columns 'Username', 'Unit', 'Role', and 'Action'. It lists three users: 'admin' (Unit: °C, Role: admin), 'user' (Unit: °C, Role: user), and 'manager' (Unit: °C, Role: manager).
- LDAP Configuration:** A list of settings including 'Enable' (checked), 'LDAP Server', 'Security' (none), 'Port' (389), 'Type' (OpenLDAP), 'Base DN', 'Bind Password' (****), 'Search User DN', 'Login Name Attribute', and 'User Entry Object Class'.
- Radius Configuration:** A table with columns 'Enable', 'Server', 'Port', 'Secret', and 'Action'. It lists two servers, both with '1812' as the port and '*****' as the secret.
- Roles:** A table with columns 'Role', 'Description', and 'Action'. It lists three roles: 'admin' (admin operation), 'user' (user operation), and 'manager' (redfish user).
- Session Management:** A list of settings including 'Sign-in retries allowed' (checked), 'Number of Retries Allowed' (3), 'Session Timeout Value' (10 [Minutes of Inactivity]), and 'Lockout Time' (3 [Minutes]).
- Password Policy:** A list of settings including 'Password Aging Interval' (60d), 'Minimum Password Length' (8), 'Maximum Password Length' (32), and four enforcement rules for character types (lower case, upper case, numeric, and special characters).

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

The screenshot shows the ENLOGIC User Settings page with the temperature unit toggle set to '°F'. The layout is identical to the previous screenshot, but the 'Unit' column in the Users table now shows '°F' for all three users: 'admin', 'user', and 'manager'. The rest of the configuration sections (LDAP, Radius, Roles, Session Management, Password Policy) remain the same.

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.

The screenshot shows the ENLOGIC web interface. At the top, it displays 'ENLOGIC' and 'Outlet Metered, Outlet Switched PDU'. Below the navigation bar, the 'PDU Thresholds' section is active. Underneath, there's a 'Device Detection Threshold' set to 150 mA. The 'External Sensors' tab is selected, showing a grid of sensor configurations for various PDU units. Each sensor entry includes its name, type, and various threshold levels (Low Critical, Low Warning, High Warning, High Critical) with their corresponding values.

External Sensors(1.1)	External Sensors(1.2)	External Sensors(1.3)	External Sensors(1.4)
Name: TEMP1_PDU1	Name: TEMP2_PDU1	Name: TEMP3_PDU1	Name: HUM1_PDU1
Type: Temperature	Type: Temperature	Type: Temperature	Type: Humidity
Low Critical: 15	Low Critical: 15	Low Critical: 15	Low Critical: 20
Low Warning: 34	Low Warning: 34	Low Warning: 33	Low Warning: 50
High Warning: 35	High Warning: 35	High Warning: 36	High Warning: 60
High Critical: 36	High Critical: 36	High Critical: 38	High Critical: 80

External Sensors(1.6)	External Sensors(1.7)	External Sensors(1.8)
Name: DOORSWITCH_PDU1	Name: HUM2_PDU1	Name: TEMP4_PDU1
Type: Door	Type: Humidity	Type: Temperature
Value: Off	Low Critical: 10	Low Critical: 0
	Low Warning: 10	Low Warning: 0

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

The 'Edit' panel for 'External Sensors(1:1)' shows a list of settings. Each setting has a value and an 'Enable' checkbox with a red checkmark. The 'Enable Low Critical' checkbox is highlighted with a red border.

High Critical	36	Enable High Critical	<input checked="" type="checkbox"/>
High Warning	35	Enable High Warning	<input checked="" type="checkbox"/>
Low Warning	34	Enable Low Warning	<input checked="" type="checkbox"/>
Low Critical	15	Enable Low Critical	<input checked="" type="checkbox"/>

Save

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

1. Follow below steps to setup the connection up to 64 PDUs of the same SKU via single IP address: Configure the PDU, which is first in line on the Daisy Chain.

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

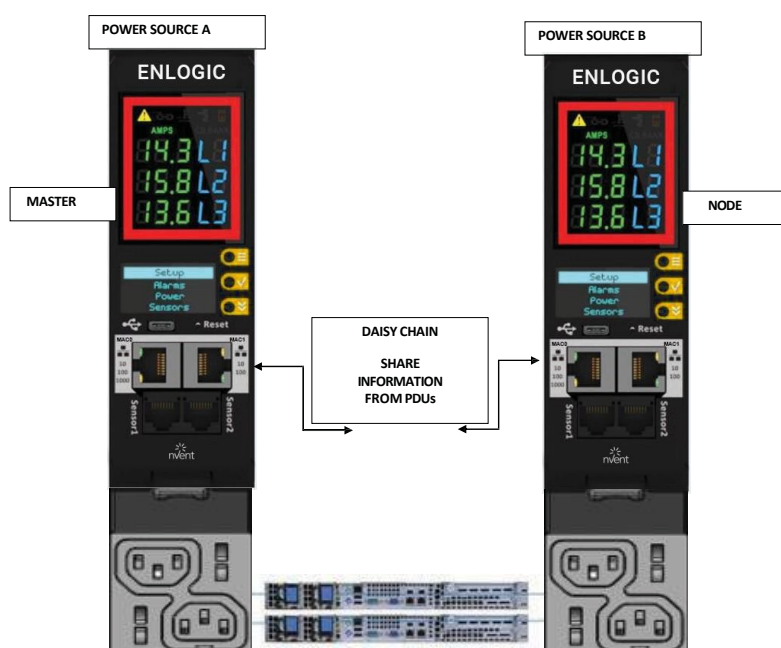
2. After the initial PDU is configured, connect the Ethernet cord from the 10/100 port (on the configured PDU) to the 10/100/1000 port (on the second PDU) in the daisy chain line.
3. Repeat **step 2**, connecting PDUs from the 10/100 port to the 10/100/1000 port for up to **64** PDUs.

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

nVent 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 nVent Enlogic RNA, the landlord and tenant maintain two separate private networks that do not overlap.
- nVent 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 nVent 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):

ZERO TOUCH PROVISIONING (ZTP)

The **Zero Touch Provisioning (ZTP)** feature streamlines the configuration process for new PDUs deployed within a network, eliminating the need for manual intervention. ZTP is an effective solution for automating the deployment and configuration of PDUs in a network environment. Here are the key features:

- Eliminates manual work: ZTP removes the need for manual deployment of PDUs, making the process more efficient.
- Accelerates deployment: The automated nature of ZTP speeds up the deployment process.
- Reduces errors: By automating the configuration, ZTP minimizes the errors that are often associated with manual configuration.

Additionally, the firmware supports various protocols and configurations to ensure seamless operation:

- TFTP: The PDU firmware supports the Trivial File Transfer Protocol for downloading configuration and firmware files.
- DHCP Options: The firmware supports DHCP Option 43 (Vendor Specific Information) and Option 60 (Vendor Class Identifier).

ZTP is enabled by default. When the PDUs are powered on or ethernet cables are connected to eth0/eth1 ports, they receive TFTP server details in the DHCP OFFER response. Based on the content of the "control.cfg" file, the type of provisioning is determined (i.e., provisioning of conf only or provisioning of firmware only or provisioning of both conf and firmware).

- ZTP is attempted on each lease renewal as long as the DHCP server is active.
- ZTP works only if the PDU is not configured with a static IP address.
- The ZTP (Zero Touch Provisioning) process involves the PDU (Power Distribution Unit) accepting three options from the DHCP server, identified by the Vendor Class Identifier. These options must be configured before using the ZTP feature on the PDU. In a Linux environment, these details are found in the "dhcpd.conf" file.
- The Vendor Class Identifier on the DHCP server should specify "ENLOGIC" as the identifier, matching the text in Option 60 of the DHCP DISCOVER message.

Options to be configured in DHCP server:

1. **IP Address of TFTP Server:** This is the IPv4 address of the TFTP server where the configuration and firmware files are stored.
2. **Magic Number:** Any number from 1 to $(2^{32}-1)$ can be specified as the magic number. It serves as an identifier to determine when the PDU should be provisioned, preventing repeated provisioning with the same configuration and firmware files. The magic number on the DHCP server is compared with the one on the PDU, and provisioning occurs only if they differ. To re-enable provisioning on the same PDU, change the magic number on the DHCP server each time.
3. **Control File and Device List file Location:** This is the path where "control.cfg" and "devicelist.csv" files are stored on the TFTP server.

File Details:

- **Control.cfg File:** This file specifies what needs to be provisioned on the PDU, listing details in key-value pairs identified by the delimiter '='.
- **Devicelist.csv File:** This file lists the serial numbers of PDUs to be provisioned and optionally includes other details to be applied to the PDU being provisioned. If details are present, the PDU will be updated with the information listed against its serial number.

Configuration Details:

1. **Configuring DHCP Server:** Configure the DHCP server to support Option 43 (Vendor Specific Information) and Option 60 (Vendor Class Identifier). The DHCP server should include the IP address of the TFTP server, a magic number, and the control file path.

Sample DHCP server configuration details is shown in the below screenshot. The sample shows the TFTP server IP address as **192.168.1.10** (of type ip-address) and Magic number as **"0710240427"** (of type text) and control file path on the TFTP server as **"system"** (of type text).

```
set vendor-string = option vendor-class-identifier;
option space ENLOGIC hash size 3;
option ENLOGIC.pdu-tftp-server code 1 = ip-address;
option ENLOGIC.pdu-refid code 2 = text;
option ENLOGIC.pdu-control-file code 3 = text;

class "ENLOGIC" {
    match if substring(option vendor-class-identifier, 0, 10) = "ENLOGIC";
    option vendor-class-identifier "ENLOGIC";
    vendor-option-space ENLOGIC;
    option ENLOGIC.pdu-tftp-server 192.168.1.10;
    option ENLOGIC.pdu-refid "0710240427";
    option ENLOGIC.pdu-control-file "system";
}
```

Note: TFTP server IP, Magic number and Control file path on the TFTP server should be listed in the same order as shown in the screenshot

2. **Updating "control.cfg" in TFTP Server:** List the key-value pair details in the "control.cfg" file. The sample "control.cfg" file is shown in below screenshot.

```
# This is a config file to control ZTP Provisioning

# Specify ztp_provision as CONF for provisioning CONF file
# Specify ztp_provision as FW for provisioning FW file
# Specify ztp_provision as BOTH for provisioning both CONF and FW files
# Specify selective_provision as devicelist.csv for provisioning specific PDUs and NA for provisioning all PDUs
# Specify conf file path where conf.ini file is present in TFTP server for conf_file_path
# Specify FW file path where .fw file is present in TFTP server for fw_file_path

[General]
ztp_provision = BOTH
selective_provision = NA
conf_file_path = /system/conf
fw_file_path = /fw
```

The key-value pair details to be listed in the file are shown below:

- a. **ztp_provision:** Specifies what is being provisioned
 - To provision only conf file, mention the value for key "ztp_provision" as CONF
 - To provision only firmware file, mention the value for key "ztp_provision" as FW
 - To provision both conf and firmware files, mention the value for key "ztp_provision" as BOTH
 - b. **selective_provision:** Specifies any specific PDUs to be provisioned and also any additional details need to be configured after applying configuration from "conf.ini" file
 - To provision specific PDUs, mention the value for key "selective_provision" as devicelist.csv (list of PDUs to provision should be included in file devicelist.csv)
 - To provision all PDUs, mention the value for key "selective_provision" as NA
 - c. **conf_file_path:** Specifies the path on the TFTP server where the conf.ini file is present. Mention the absolute path of conf.ini file on the TFTP server
 - d. **fw_file_path:** Specifies the path on the TFTP server where the firmware file is present. Mention the absolute path of firmware file on the TFTP server.
3. **Updating "devicelist.csv" in TFTP Server:** Include the serial numbers of PDUs to be provisioned in the "devicelist.csv" file. If a static IP is listed against any serial number, it will be assigned to the PDU during provisioning.

The sample content of the file "devicelist.csv" is shown in the below screenshot

SN	SystemName	Eth0StaticIP	Eth0Subnet	Eth0Gateway	Eth1StaticIP	Eth1Subnet	Eth1Gateway	PanelName
EN1	PDU1	192.168.0.222	255.255.255.0	192.168.0.1				First
EN2	PDU2							Second
EN3	PDU3							Third
EN4	PDU4							Fourth
EN5	PDU5							Fifth
EN6	PDU6							Sixth
EN7	PDU7							Seventh
EN8	PDU8	192.168.0.221	255.255.255.0	192.168.0.1				Eighth
EN9	PDU9							Ninth
EN10	PDU10							Tenth
EN11	PDU11	192.168.0.200	255.255.255.0	192.168.0.2	192.168.0.201	255.255.255.0	192.168.0.1	Eleventh

Note:

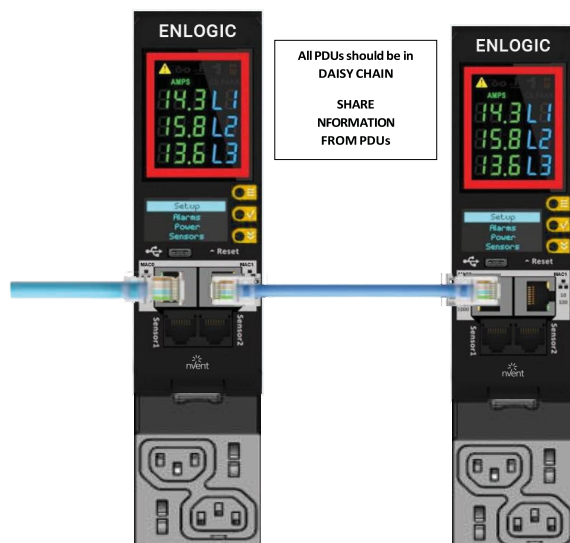
1. When specific PDUs need to be provisioned, include their serial numbers in the devicelist.csv file.
2. If a static IP is listed in the "devicelist.csv" file for any PDU's serial number, then during the provisioning of that specific PDU, the static IP along with all other details present in the file will be assigned to the PDU.
3. To ensure ZTP functions correctly, make sure the ethernet cable is connected to either eth0 or eth1 in the system. Since ZTP works with both eth0 and eth1, connecting the ethernet cable to both ports simultaneously may cause the system to attempt provisioning twice, leading to potential issues.

POWER SHARE OVER DAISY CHAIN PDUs

nVent 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.



UPCOMING FEATURES

nVent Enlogic firmware will support the following upcoming Power Share features:

1. nVent 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/alerts.
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

nVent 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

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

USB METHOD

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

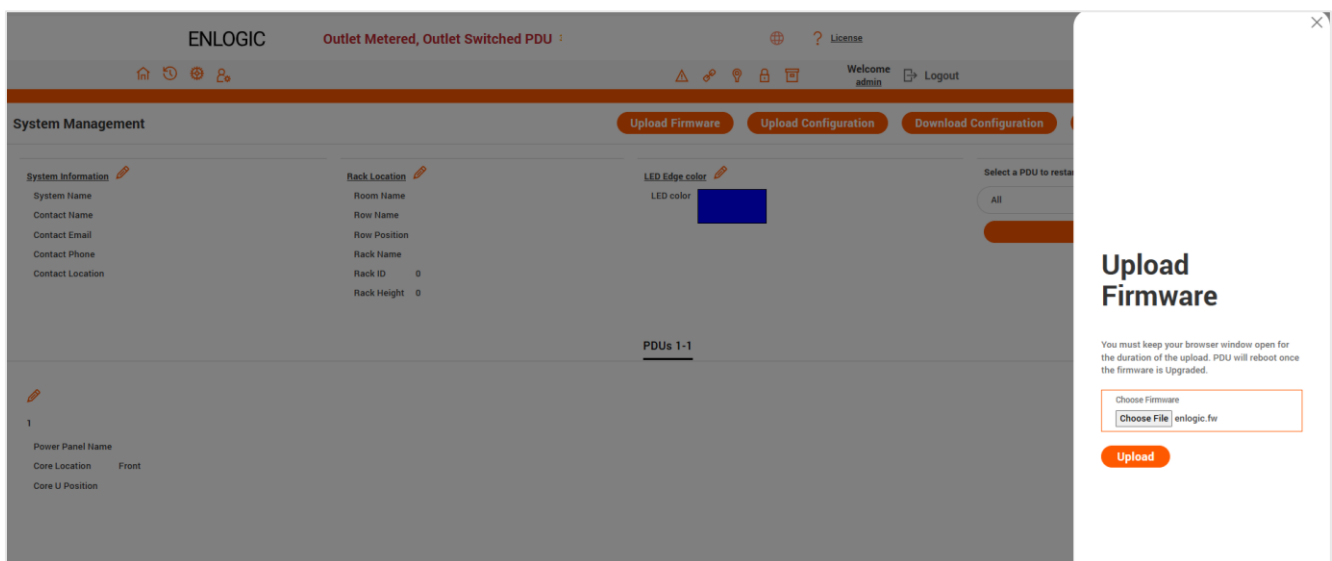
Note: The OLED will show the Firmware update progress. It also shows the process of updating. When the update is complete, the PDU will automatically reboot.

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.

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.

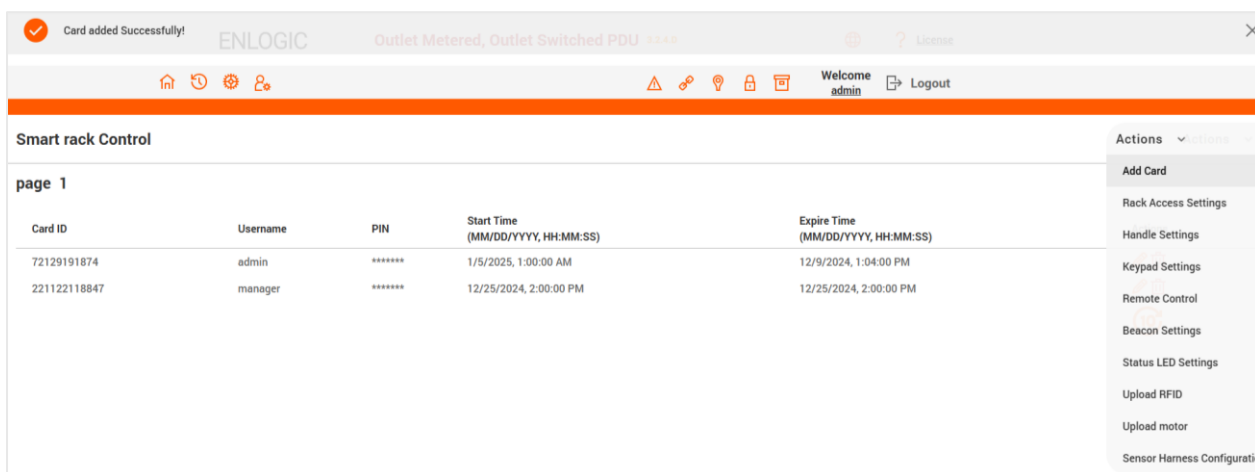
After reboot message indication in console, push the "Y" from the prompt (Y/N) displays for the PDU reboot.

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.

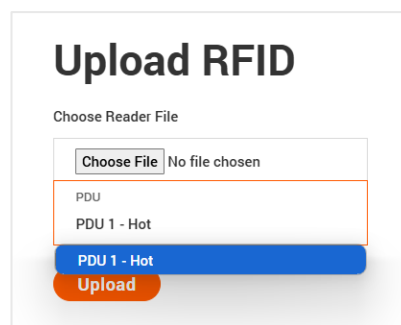
HANDLE UPDATE PROCEDURES

Web Interface Method

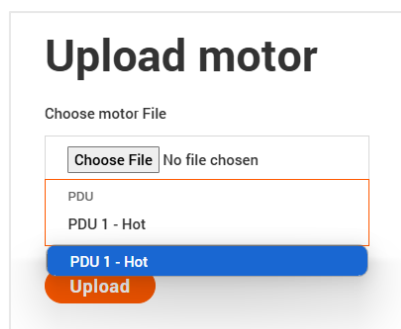
1. This page allows you to upgrade the **Handle RFID and Motor firmware** using the Smart Rack Control Page. In both cases after the firmware is updated PDU will be reset.
2. Click on the Settings icon to dropdown the Settings menu.
3. Select **Smart Rack Control** to view information.
4. Click on **Actions** button on the right side of the screen.



5. Select **Upload RFID** to upgrade the handle RFID firmware. Under the Choose Reader file, click Choose File and select 'reader.bin' file. Select the PDU id from the drop down menu. Click Upload button to start updating the firmware.

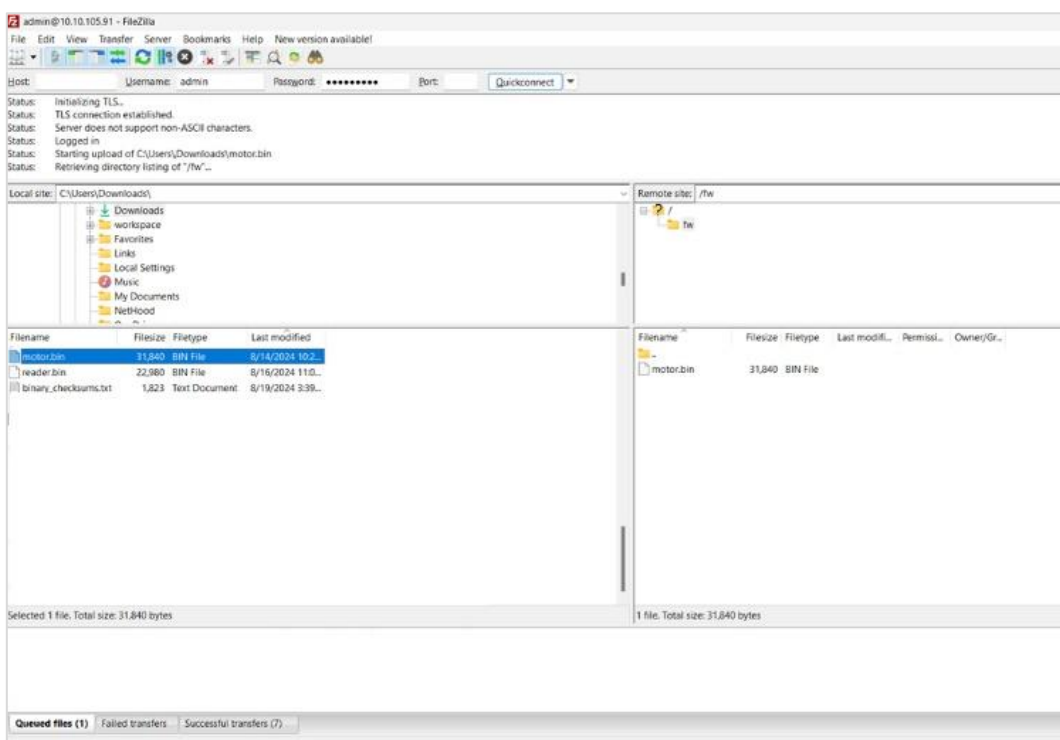
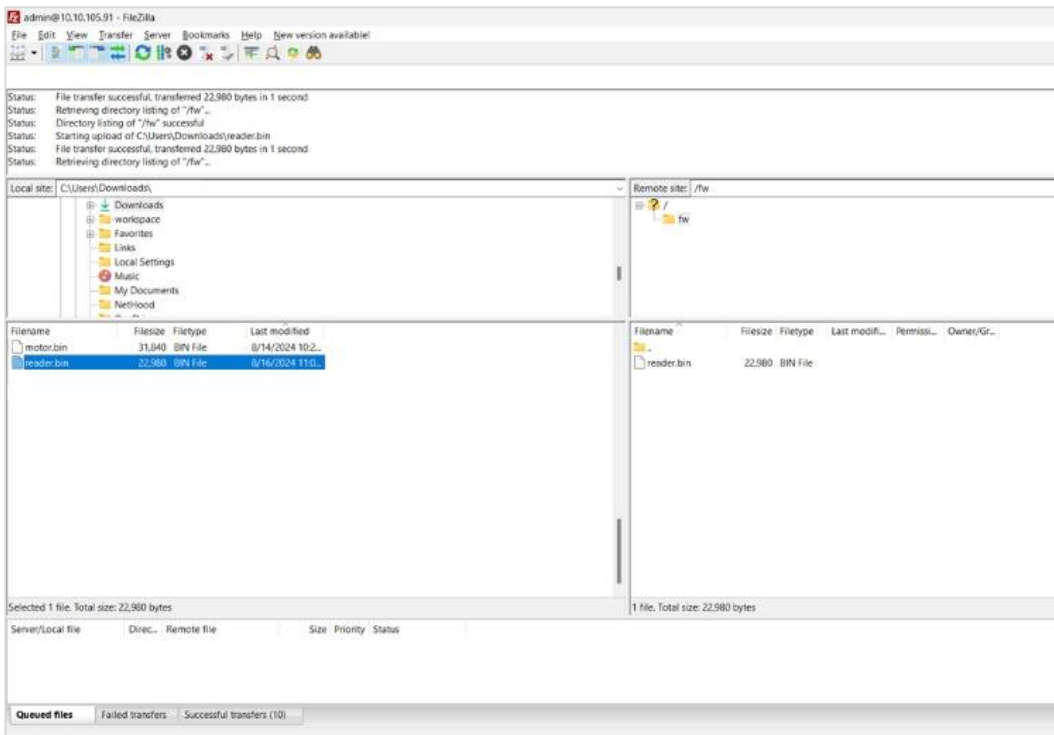


6. Select **Upload Motor** to upgrade the handle motor firmware. Under the Choose motor file, click Choose File and select 'motor.bin' file. Select the PDU id from the drop down menu. Click Upload button to start updating the firmware.



CLI/SSH Interface Method

1. To access the PDU using an FTPS program, FTPS must be enabled through the PDU Web Interface or through CLI or through SSH.
2. In the Web Interface, go to **Network Settings** -> FTPS.
3. Select the check box to enable FTPS Access.
4. Login to an FTP program with a role with administration privileges.
5. Transfer the firmware file reader.bin for RFID and motor.bin for Motor Firmware update respectively to /fw folder.



6. Connect to the PDU via SSH using a program such as TeraTerm or PUTTY.
7. Login using a role with administration privileges.
8. Execute the CLI/SSH command for RFID "sys updatehid rfid 1 1" to perform the FW upload operation.
9. Execute the CLI/SSH command for Motor "sys updatehid motor 1 1" to perform the FW upload operation.

Note: Refer the CLI commands table on page for all the CLI/SSH commands for handle RFID and Motor updates.

QUESTIONS AND ANSWERS (FAQS)

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

Answer: Advantage Secure is a new offering 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 3.2.4?

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:

- Verify if the existing firmware versions are 2.0.6.7/ 2.0.7.6 or below these versions.
- Upgrade to the Firmware version is 2.0.6.7/ 2.0.7.6 , use the following process and upgrade to the latest firmware version 3.2.4 .
- 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] flash new firmware 3.2.4 use **enlogic.fw** using USB, WEBUI & FTPS.
- USB firmware upgrade option is recommended.
- USB should be in FAT32 file system, no other files to be present during firmware upgrade.
- It is recommended to upgrade the firmware always on standalone PDU.
- If PDUs are daisy chained detach the daisy chain cable and then upgrade the firmware.

Advantage Secure NMCs:

- Firmware version 3.0.4.
- From 3.0.4, to flash new firmware 3.2.4 use enlogic.fw using USB, WEBUI & FTPS.
- USB firmware upgrade is recommended.
- USB should be in FAT32 file system, no other files to be present during firmware upgrade.
- It is recommended to upgrade the firmware always on standalone PDU.
- If PDUs are daisy chained detach the daisy chain cable and then upgrade the firmware.

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.

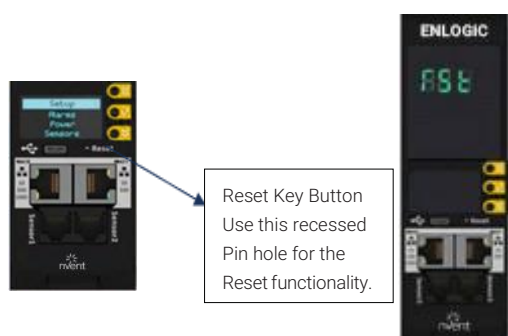
Q9. Could we understand some of the Power Share Terminologies in this document?

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.
-------------------------	---



North America

Tel +1.800.545.6258

Fax +1.800.527.5703

Tel +1.650.216.1526

Fax +1.650.474.7711

info@nVent.com

Europe, Middle East, Africa

Tel +32.16.213.511

Fax +32.16.213.603

info@nVent.com

Asia Pacific

Tel +86.21.2412.1688

Fax +86.21.5426.3167

cn.info@nVent.com

Latin America

Tel +1.713.868.4800

Fax +1.713.868.2333

info@nVent.com

Our powerful portfolio of brands:

CADDY

ERICO

HOFFMAN

ILSCO

RAYCHEM

SCHROFF

