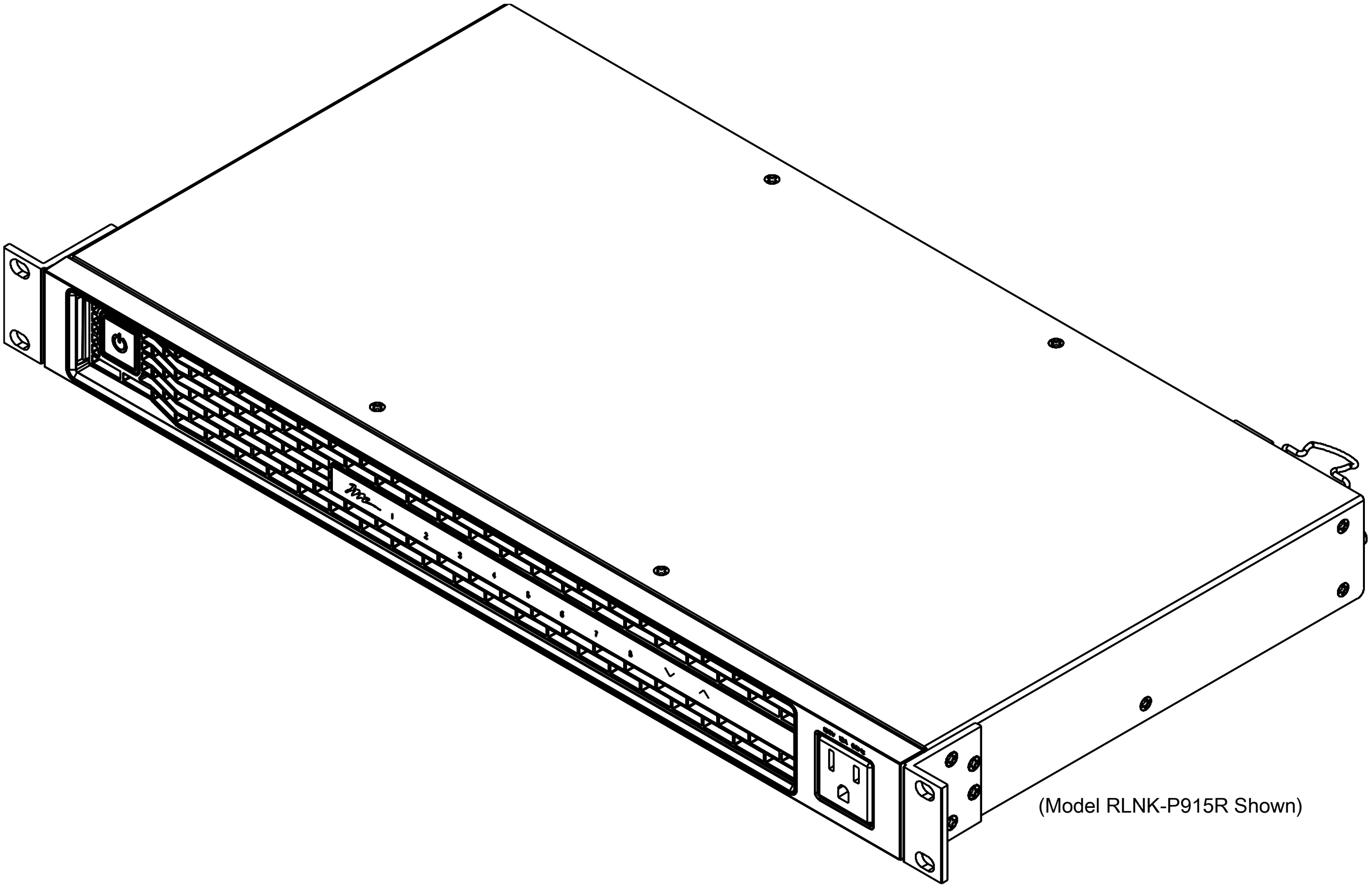
User Manual

Premium+ PDU with RackLink™

Monitor | Control | Alert | Report | Analyze



(Model RLNK-P915R Shown)

THANK YOU

Thank you for purchasing a Premium+ PDU with RackLink™ product. Please read these instructions thoroughly before installing or assembling this product.

Middle Atlantic Products

I-00826 Rev C

Contents

Appendix A: Specifications 200

Appendix B: Resetting to Factory Defaults 205

Appendix C: Installing the Device Discovery Software and Accessing a Connected PDU’s Web Interface 208

IMPORTANT SAFETY INSTRUCTIONS

- Read these instructions.
- Keep these instructions.
- Heed all warnings.
- Follow all instructions.
- Clean only with dry cloth.
- Only use attachments/accessories specified by the manufacturer.

DANGER HAZARDOUS VOLTAGE: The lightning flash with the arrowhead symbol, within an equilateral triangle is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

WARNING: A warning alerts you to a situation that could result in serious personal injury or death.

CAUTION: A caution alerts you to a situation that may result in minor personal injury or damage to the product and/or property.

NOTE: A note is used to highlight procedures pertaining to the installation, operation, or maintenance of the product.

DANGER HAZARDOUS VOLTAGE: To reduce the risk of electrical shock: Always unplug this device from the electrical outlet before cleaning.

WARNING: Failure to read, understand and follow the following information can result in serious personal injury, damage to the equipment or voiding of the warranty. It is the responsibility of the Installer/User to ensure that this product is loaded according to specifications.

WARNING: Risk of Electric Shock: Connect the device to a properly grounded outlet only. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong is provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.

WARNING: The apparatus shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the apparatus.

WARNING: To reduce the risk of burns, fire, electric shock, or injury to persons:

- Unplug from outlet before putting on or taking off parts.
- Close supervision is necessary when this device is used by, or near children, invalids, or disabled persons.
- Use this device only for its intended use as described in these instructions. Do not use attachments not recommended by the manufacturer.
- Never operate the device if it has a damaged cord or plug, if it is not working properly, if it has been dropped or damaged, or dropped into water. Return the device to a service center for examination and repair.
- Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
- Keep the cord away from heated surfaces.
- Never drop or insert any object into any opening.
- Do not use outdoors.
- Do not operate where aerosol (spray) products are being used or where oxygen is being administered.
- To disconnect, turn all controls to the off position, then remove plug from outlet.

CAUTION: The socket-outlet shall be installed near the equipment and shall be easily accessible.

CAUTION: Use indoor in dry locations only.

Safety Instructions: Rack Mount

Elevated Operating Ambient: If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

Reduced Air Flow: Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical Loading: Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuit might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Earthing: Reliable earthing of rack-mounting equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Disconnect Device (Pluggable Equipment): The socket-outlet shall be installed near the equipment and shall be easily accessible.

When using electrical products, basic precautions should always be followed, including the following:

- Read and follow all instructions before using.
- There are no user-serviceable components within this device. Removal of the cover from this device may present a shock hazard, and void the warranty.
- The mains plug is used as your disconnect device. This device shall remain readily operable.
- Unplug this apparatus during lightning storms or when unused for long periods of time.
- Do not overload the wall outlet where this device is being connected. Do not overload this device. Ensure the total load to this device does not exceed that which is listed in the specifications section of this manual.
- Ensure this device is connected to a properly grounded AC power source. Ensure the device is plugged into a source providing the required 120V. Do not use a plug adapter that defeats the ground pin of the AC plug.

Waste Electrical and Electronic Equipment (WEEE) Directive

Correct disposal of this product: This symbol indicates that this product must not be disposed of with household waste, according to the WEEE Directive (2012/19/EU) and your national law. This product should be taken to a collection center licensed for the recycling of waste electrical and electronic equipment (EEE). The mishandling of of this type of waste could have a possible negative impact on the environment and human health due to potentially hazardous substances that are generally associated with EEE. At the same time, your cooperation in the correct disposal of this product will contribute to the efficient use of natural resources. For more information about where you can take your waste equipment for recycling, please contact your local city office or your household waste collection service.

REGULATORY COMPLIANCE

Federal Communications Commission (FCC) Compliance Statement

> **CAUTION**: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Industry Canada (IC)

ICES-003 Class B Notice. This Class B digital apparatus complies with Canadian ICES-003.

INSTRUCTIONS IMPORTANTES SUR LA SÉCURITÉ

- Lire ces instructions.
- Conservez ces instructions.
- Respectez tous les avertissements.
- Suivez toutes les instructions.
- Nettoyer uniquement avec un chiffon sec.
- N'utilisez que des accessoires spécifiés par le fabricant.

DANGER TENSION DANGEREUSE: Le symbole de la pointe de flèche, dans un triangle équilatéral, est destiné à alerter l'utilisateur sur la présence de tension dangereuse non isolée dans l'enceinte du produit qui peut être d'une ampleur suffisante pour constituer un risque d'électrocution.

AVERTISSEMENT: Un avertissement vous avertit d'une situation pouvant entraîner des blessures graves ou la mort.

ATTENTION: Une attention vous avertit d'une situation pouvant entraîner des blessures mineures ou des dommages au produit et/ou à la propriété.

REMARQUE: Une remarque est utilisée pour mettre en évidence les procédures relatives à l'installation, au fonctionnement ou à l'entretien du produit.

DANGER TENSION DANGEREUSE: Pour réduire le risque de choc électrique: Toujours débrancher le meuble de la prise électrique avant de le nettoyer.

AVERTISSEMENT: Ne pas lire, comprendre et suivre les informations suivantes peut entraîner des blessures graves, des dommages à l'équipement ou de la nullité de la garantie. Il incombe à l'installateur/utilisateur de s'assurer que ce produit est chargé conformément aux spécifications.

AVERTISSEMENT: Risque de choc électrique: Brancher le meuble uniquement à une prise correctement mise à la terre. Ne pas détériorer le dispositif de sécurité de la fiche polarisée ou de la fiche de terre. Une fiche polarisée possède deux broches, dont l'une plus large que l'autre. Une fiche de type terre possède deux broches et une troisième de mise à la terre. La broche large ou la troisième fiche sont fournies pour des raisons de sécurité. Si la fiche fournie n'entre pas dans votre prise de courant, veuillez faire appel à un électricien pour remplacer la prise obsolète.

AVERTISSEMENT: L'appareil ne doit pas être exposé à des éclaboussures et aucun objet rempli de liquide, comme des vases, ne doit être placé sur l'appareil.

AVERTISSEMENT: Pour réduire les risques de brûlures, d'incendie, de choc électrique ou de blessures:

- Débrancher de la prise électrique avant d'installer ou de retirer des pièces.
- Surveiller étroitement ce meuble s'il est utilisé par ou à proximité d'un enfant, d'une personne invalide ou handicapée.
- N'utiliser ce meuble que pour l'usage auquel il est destiné, tel que décrit dans la présente fiche d'instructions. Ne pas utiliser d'accessoires non recommandés par le fabricant.
- Ne jamais utiliser ce meuble si le cordon ou la prise est endommagé, s'il ne fonctionne pas correctement, s'il est tombé ou est endommagé, ou s'il est tombé dans l'eau. Renvoyer le meuble à un centre de service après-vente pour qu'il soit examiné et réparé.
- Le cordon d'alimentation doit être placé de manière à éviter qu'il soit piétiné ou pincé, notamment au niveau des prises, des réceptacles et à la sortie de l'appareil.
- Garder le cordon d'alimentation loin des surfaces chauffées.
- Ne jamais faire tomber ou introduire un objet dans une ouverture.
- Ne pas utiliser en extérieur.
- Ne pas utiliser dans des lieux où des produits aérosols sont utilisés ou à proximité d'une source d'oxygène.
- Pour débrancher, placer tous les boutons en position off, puis retirer la fiche de la prise électrique.

ATTENTION: La prise de courant doit être installée près de l'équipement et doit être facilement accessible.

ATTENTION: Pour être utilisé en intérieur dans un endroit sec seulement.

Consignes de sécurité: montage en rack
Température de fonctionnement: Si installé dans un rack fermé ou à unités multiples , la température ambiante de fonctionnement de l'environnement du rack peut être supérieure à ambiante de la pièce. Par conséquent, il faudrait envisager d'installer l'équipement dans un environnement compatible avec la température ambiante maximale (Tma) spécifiée par le constructeur.
Réduction Air accréditives: Installation de l'équipement dans un rack doit être telle que la quantité de flux d'air nécessaire au bon fonctionnement de l'équipement ne soit pas compromise.
Chargement mécanique: Le montage de l'équipement dans le rack doit être telle qu'une condition dangereuse ne lié à un chargement mécanique irrégulier.
Surcharge des circuits: Il faudrait envisager à la connexion de l'équipement au circuit d'alimentation et l' effet que la surcharge du circuit pourrait avoir sur la protection contre les surintensités et le câblage d'alimentation. Examen approprié des équipements évaluations de la plaque signalétique doit être utilisée pour traiter de cette préoccupation.
Mise à la terre fiable: Fiable mise à la terre de l'équipement de montage en rack doit être maintenue. Une attention particulière devrait être accordée aux connexions d'alimentation autres que les connexions directes vers le circuit de dérivation (par exemple de l'utilisation de bandes de puissance).
Appareil Disconnect (Équipement Pluggable): La prise de courant doit être installée à proximité du matériel et doit être facilement accessible.
Lors de l'utilisation des produits électriques, des précautions de base doivent toujours être respectées, y compris les suivantes:

- Lire et suivre toutes les instructions avant l'utilisation du matériel.
- Il n'ya pas de composants réparables par l'utilisateur au sein de cet appareil. Retrait de la couverture de cet appareil peut présenter un dangerd'électrocution et annuler la garantie.
- La fiche secteur est utilisée comme sectionneur de courant. Ce dispositif doit rester en état de marche.
- Débrancher cet appareil pendant les orages ou s'il n'est pas utilisé pendant de longues périodes.
- Ne surchargez pas le réceptacle de mur ou le circuit qui fournit l'énergie à ce appareil. Ne pas surcharger cette appareil. S'assurer que la charge totale à cet appareil ne dépasse pas celle qui est répertoriée dans la section desspécifictions de ce manuel.
- Assurez-vous cet appareil est connecté à une source d'alimentation C/A avecmise à la terre. Assurez-vous cet appareil est branché sur une sourced'alimentation fournissant les nécessaires 120V. Ne pas utiliser un adaptateurqui contrecarre la broche de terre de la prise du cordon d'alimentation.

Directive sur les déchets d'équipements électriques et électroniques (WEEE)

Elimination correcte de ce produit: Ce symbole indique que ce produit ne doit pas être éliminé avec les ordures ménagères, conformément à la directive WEEE (2012/19/EU) et à votre législation nationale. Ce produit doit être déposé dans un centre de collecte agréé pour le recyclage des déchets d'équipements électriques et électroniques (EEE). La mauvaise manipulation de ce type de déchets pourrait avoir un impact négatif possible sur l'environnement et la santé humaine en raison de substances potentiellement dangereuses généralement associées aux EEE. Dans le même temps, votre coopération dans l'élimination correcte de ce produit contribuera à une utilisation efficace des ressources naturelles. Pour plus d'informations sur les lieux de recyclage de vos équipements usagés, veuillez contacter votre mairie ou votre service de collecte des ordures ménagères.

CONFORMITÉ RÉGLEMENTAIRE

Déclaration de conformité de la Federal Communications Commission (FCC)

ATTENTION: Les changements ou modifications non expressément approuvés par le fabricant peuvent annuler le droit de l'utilisateur à utiliser l'équipement.

REMARQUE: Cet équipement a été testé et jugé conforme aux limites d' un dispositif numérique de classe B, conformément à la partie 15 des règles de la FCC. Ces limites sont conçues pour fournir une protection raisonnable contre les interférences nuisibles dans une installation résidentielle. Cet équipement génère, utilise et peut émettre de l'énergie radiofréquence et, si non installé et utilisé conformément aux instructions, peut provoquer des interférences dans les communications radio. Cependant, il n'y a aucune garantie que des interférences ne se produiront pas dans une installation particulière. Si cet équipement provoque des interférences nuisibles à la réception radio ou de télévision, ce qui peut être déterminé en allumant et éteignant l'équipement, l'utilisateur est encouragé à essayer de corriger l'interférence par une ou plusieurs des mesures suivantes:

- Réorienter ou déplacer l' antenne de réception.
- Augmenter La distance entre l'équipement et le récepteur.
- Brancher l'équipement dans une prise sur un circuit différent de celui sur lequel est branché le récepteur.
- Consulter le revendeur ou un technicien radio/TV expérimenté.

Industrie Canada (IC)

ICES-003 Avis NMB-003, Classe B. Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Chapter 1: Introduction

Thank you for purchasing Middle Atlantic Products Premium+ PDU with RackLink (referred to in this document as PDU). The complete set of instructions for your PDU is available from www.middleatlantic.com and includes the following documents:

- The Quick Start Guide (I-00827 for Rackmount Units, I-00864 for Compact Units)
- The User Manual (I-00826)
- The Advanced User Manual (I-00852)
- The Environmental Sensors User Manual (I-00853)

Before You Begin

Perform the following activities prior to installation:

- Unpack the product and components and compare the serial number of the equipment with the number on the packing slip located on the outside of the box and make sure they match.
- Prepare the installation site.
- Check the branch circuit rating.

Where to Find Your IP Address

Note: The default network interface address: ***`192.168.1.200`***

1. On Rackmount PDUs only, use the front panel controls to determine the device's IP address. For more information, see ***Viewing PDU Information on the Front Panel Display*** on page 14.
2. Use the RackLink Device Discovery program to locate your device's IP address on the network. For more information, see Appendix C: Installing the Device Discovery Software and Accessing a Connected PDU's Web Interface on page 208.
3. Use the command line interface. For more information, refer to the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.

Note: To configure your IP address, see ***Ethernet Interface Settings*** *on page 85.*

Panel Components

All PDU models come with the following components on the outer panels.

- Power Button (Rackmount PDUs Only)
- Inlet
- Outlets
- Front Panel Display (Rackmount PDUs Only)
- I/O Panel
- Reset button

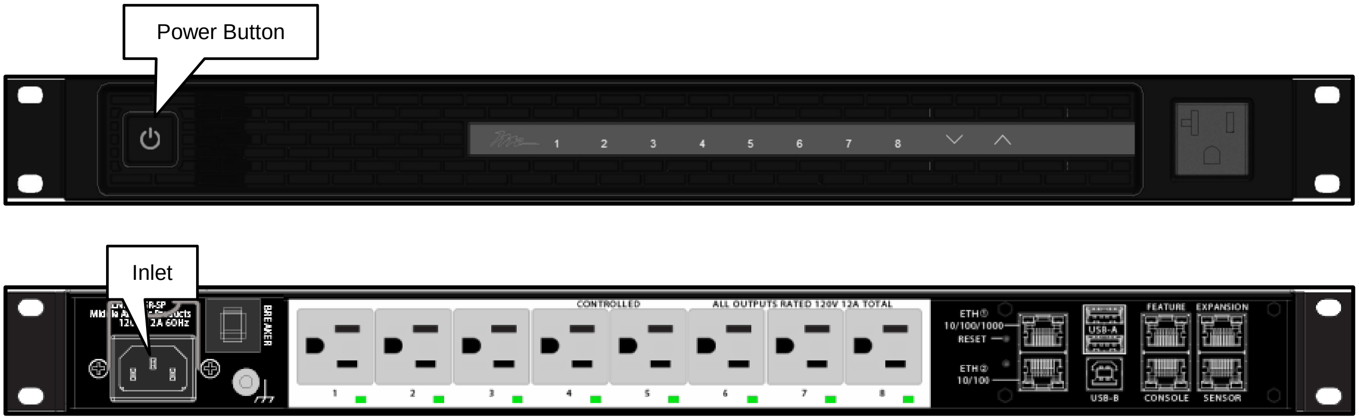
Power Button and Inlet

Note: A power button is only provided on the Rackmount PDU.

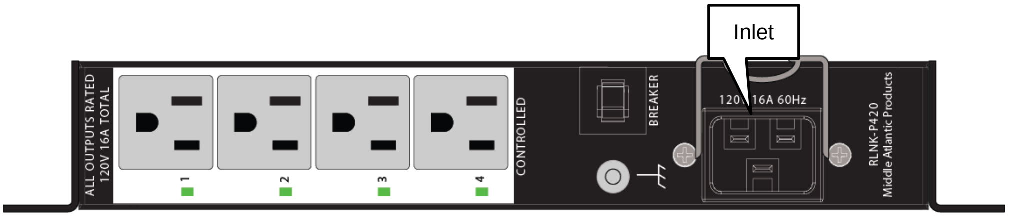
Connect your PDU to an appropriately rated branch circuit. See the markings on your PDU for appropriate input ratings or range of ratings.

For more information about power connections, see ***Connecting the PDU to a Power Source*** on page 20.

Rackmount PDU (Power Button Color Amber: OFF and White: ON)



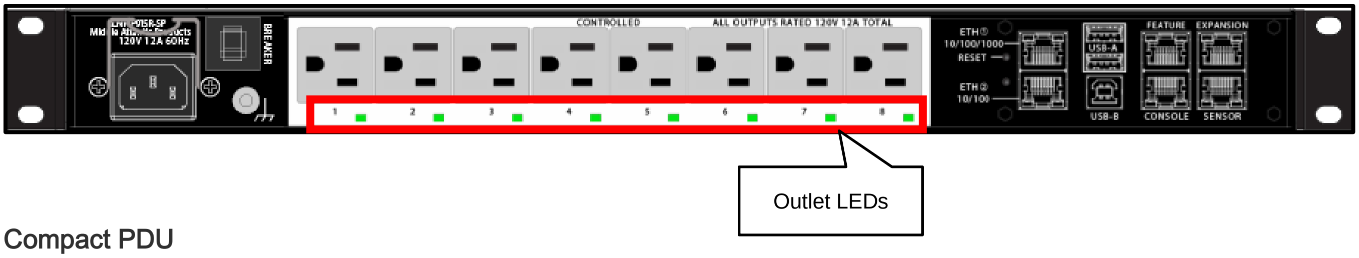
Compact PDU



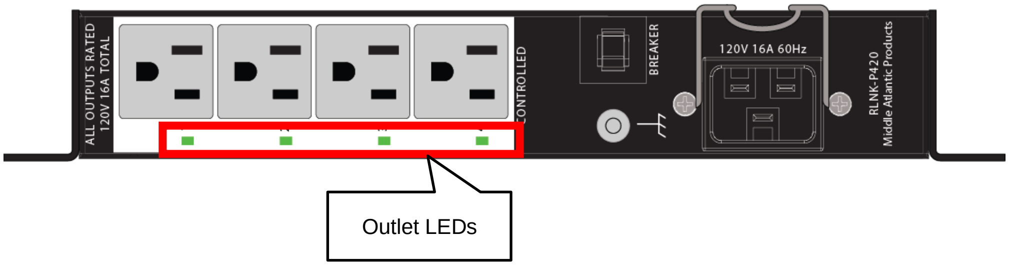
Outlets

A small LED adjacent to each outlet indicates the outlet or PDU state. The PDU is shipped from the factory with all outlets turned ON.

Rackmount PDU



Compact PDU



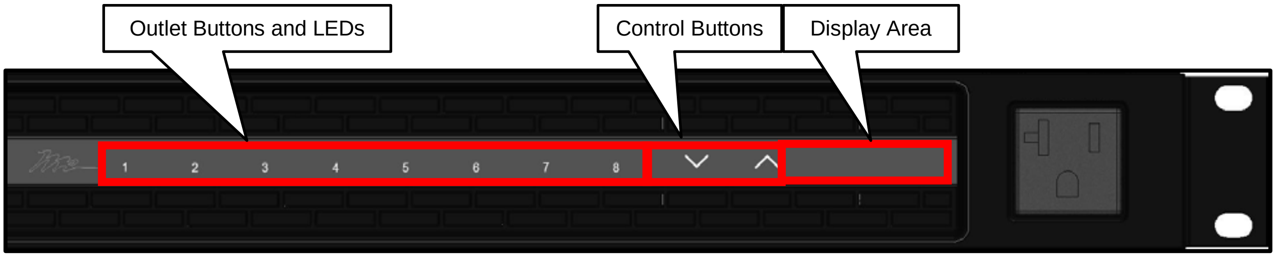
The table below explains how to interpret different outlet LED states.

LED state	Outlet status	What it means
Not lit	Powered OFF	The outlet is not connected to power, or the control circuitry's power supply is broken.
Red	OFF	The outlet is turned off and power is available when the outlet is turned on.
Green	ON and LIVE	LIVE power. The outlet is on and power is available.
Green flashing	ON and LIVE	The current flowing through the outlet is greater than the upper warning (non-critical) threshold.
Cycling through Red, Green and Yellow	n/a	The PDU has just been plugged in and its management software is loading. LED color cycling does not interrupt power to outlets. It is an indication of firmware loading.

Note: When a PDU powers up, it proceeds with the power-on self test and software loading for a few moments. At this time, the outlet LEDs cycle through different colors. When the software has completed loading, the outlet LEDs show a steady color and the front panel display illuminates.

Front Panel (Rackmount PDUs Only)

The following diagram shows the front panel layout.



You can use the front panel to view PDU information and even switch an outlet. It consists of:

- (8x) outlet buttons
- (2x) control buttons
- A front panel display

Viewing PDU Information on the Front Panel Display

The front panel display shows the MAIN MENU which includes the following measurements in this specific order:

1. INPUT VOLTAGE Title

   Input Voltage Measurement (example: 120.7 VOLTS)

2. ALARMS Title

   Alarm Amount or Value (example: NO ALARMS or 2 ALARMS)

3. TEMPERATURE Title

   Temperature Sensor Measurement (example: 78.3 F)

4. ACTIVE POWER Title

   Active Power Measurement (example: 458.7 WATTS)

5. CURRENT DRAW Title

   Current Draw Measurement (example: 3.8 AMPS)

▶ Normal Operation:

- During normal operation, the front panel display cycles through items 1-5 with a 2 second delay.

▶ Pressing Control Buttons:

- Pressing a control button will step you through the titles. After no control button is pressed for 2 seconds, the display will resume the normal operation display cycle.

▶ Retrieving the IP Address and Other Information From the Front Panel:

1. Press both control buttons and hold for 5 seconds.
2. The front panel display shows the DEVICE MENU which includes the following measurements in this specific order:
    a. IPv4 ADDR (ADDRESS) Title

       IPv4 Address Value (example: 192.168.1.200)

    b. SURGE STATUS Title

       On Series Surge Models:

       – Surges Value (example: 2 SURGES)

       On Protected Fault (MOV) Models:

       – Fault Valule (example: PROTECTED or FAULT)

    c. FW (FIRMWARE) VERSION Title

       Firwmare Version Value (example: 3.3.0.5-0)

    d. SERIAL NUM (NUMBER) Title

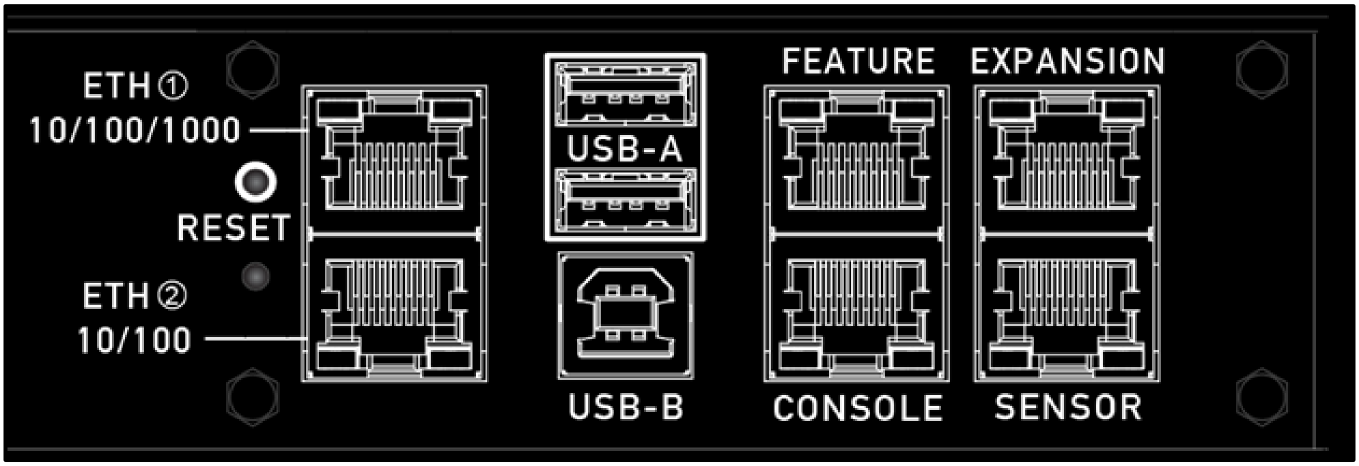
       Serial Number Value (example: RLNK-P415-001048)

    e. MAC ADDR (ADDRESS) Title

       MAC Address Value (example: 00:1E:C5:00:10:48)
3. After no control button is pressed for 2 seconds, the front panel display cycles through items a-e with a 2 second delay.
4. Press both control buttons and hold for 5 seconds and the MAIN MENU display titles appear.

I/O Panel

The I/O panel is the same on rackmount and compact PDUs and looks like the following image.



- Ethernet ports (1 and 2)
- Reset button
- (2x) USB-A port
- USB-B port
- Feature port
- Expansion port
- Console port
- Sensor port

Connection Port and Reset Button Functions

The table below explains the function of each port and the reset button.

Port	Used for...
FEATURE	Reserved for Future Use
RESET	Reboots the PDU. See ***Reset Button*** (on page 18).

Port	Used for...
ETH①10/100/1000, ETH②10/100	The PDU has two Ethernet ports. • ETH①10/100/1000 supports up to 1000 Mbps. This is "ETH1". • ETH②10/100 supports up to 100 Mbps. This is "ETH2". You can use either Ethernet port for your network connection. *Note: The yellow LED of the ETH② 10/100 port has NO function so it will not be lit regardless of the communication status.*
USB-A	**This is a "host" port, which is powered, per USB 2.0 specifications.** • Connecting a USB device, such as a wireless LAN adapter.
USB-B	• Establishing a USB connection between a computer and the PDU for using the command line interface or performing the disaster recovery. For disaster recovery instructions, contact Technical Support.
SENSOR (RJ-45)	• Connection for environmental sensors. • For more information, refer to the Premium+ PDU With RackLink Environmental Sensors User Manual www.middleatlantic.com.
CONSOLE (RJ-45)	Establishing a serial connection between the PDU and a computer. Use a third-party RJ-45 to DB9 adapter/cable to connect the PDU to your computer. See ***RJ45-to-DB9 Cable Requirements for Computer Connections*** (on page 202).

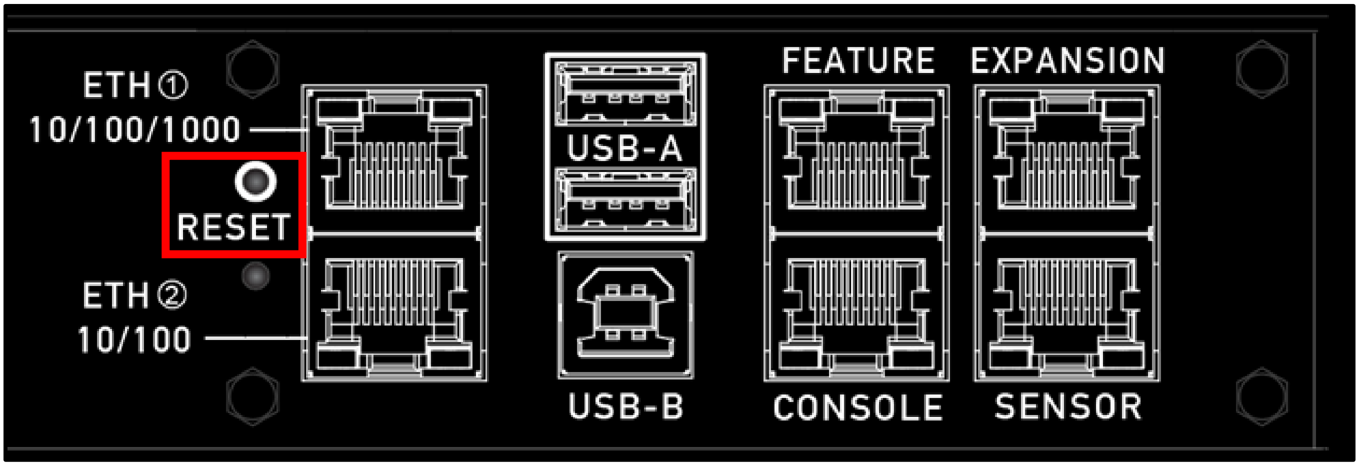
Reset Button

The reset button is located inside the small hole above the the label on the PDU.

The PDU can be reset to its factory default values using this button when a serial connection is available. See *Appendix B: Resetting to Factory Defaults* (on page 205).

Without the serial connection, pressing this reset button restarts the PDU's software without any loss of power to outlets.

The following image illustrates the location of the reset button.



Circuit Breakers

The circuit breakers automatically trip (disconnect power) when the current flowing through the circuit breaker exceeds its rating.

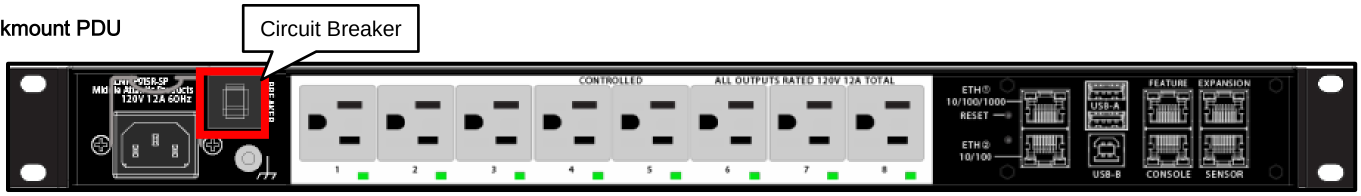
When a circuit breaker trips, power flow ceases to all outlets connected to it. You must manually reset the circuit breaker so that affected outlets can resume normal operation.

Resetting the Circuit Breaker

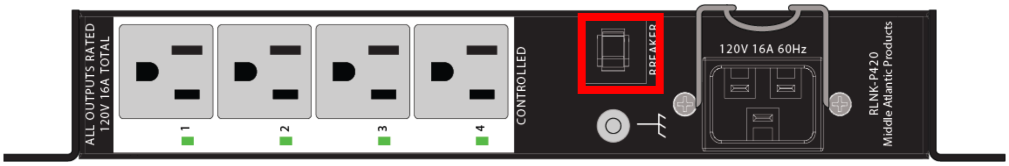
▶ To reset the breaker:

1. Locate the breaker on the unit as shown.

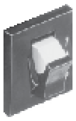
Rackmount PDU


Circuit Breaker

Compact PDU

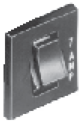


2. If the breaker is tripped, the button resembles the following image:



3. Examine your PDU and the connected equipment to remove or resolve the cause that results in the overload or short circuit. **This step is required, or you cannot proceed with the next step.**

4. Press the switch to reset the breaker. When the breaker is reset, the button resembles the following image:



Chapter 2: Connecting Your PDU

This chapter explains how to connect your PDU.

Connecting the PDU to a Power Source

1. Connect the power cable to an appropriately rated branch circuit.
2. **Rackmount PDUs Only**: Press the power button on the front left (facing) of your PDU.
3. When your PDU powers up, it proceeds with the power-on self-test and software loading for a few moments. At this time, the outlet LEDs cycle through different colors

Note: All devices have overcurrent protection mechanisms. Connect each device to an appropriately rated branch circuit. See the markings on your PDU for appropriate input ratings or range of ratings.

4. When the software has completed loading, the outlet LEDs show a steady color and the front panel display illuminates. The factory default state powers on all of the outlets.

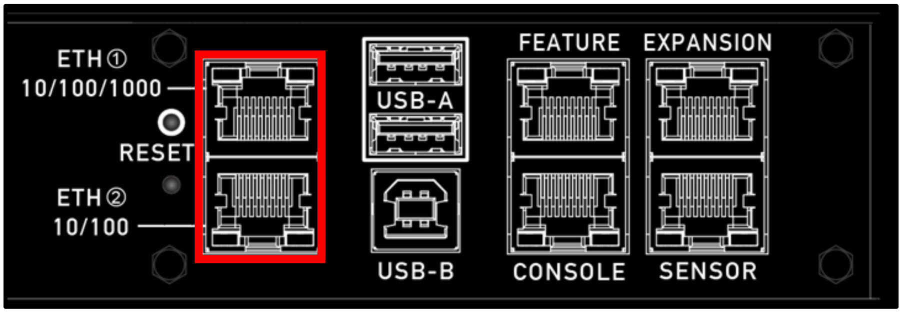
Connecting the PDU to Your Network

To remotely administer the PDU, it must be connected to your local area network (LAN). Your PDU can be connected to a wired or wireless network.

The Ethernet port must be enabled for this connection to work properly. Per default, the Ethernet port is enabled. See ***Wired Network Settings*** (on page 83).

▶ To make a wired connection:

1. Connect a standard Cat5e cable (or better, not provided) to the ETHERNET port on your PDU.
2. Connect the other end of the cable to your network.
3. The following image shows the ETHERNET port.



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

ATTENTION: Le branchement accidentel d'un connecteur RJ-45 RS-232 dans le port ETHERNET peut causer des dommages permanents au matériel Ethernet.

Making a Wireless Connection With The USB WIFI Dongle

▶ To make a wireless connection with the USB WIFI Dongle:

Do one of the following:

- Connect the USB WIFI Dongle to the PDU (the USB WIFI Dongle is available as an accessory).
- Connect a USB hub to the USB-A port on the PDU. Then, plug the USB WIFI Dongle into the appropriate USB port on the hub.

Note: The PDU supports the A/B/G/N 802.11 protocols.

Supported Wireless LAN Configuration

If wireless networking is preferred, ensure that the wireless LAN configuration of your PDU matches the access point. Use the following LAN configurations:

- Network type: 802.11 A/B/G/N
- Protocol: WPA2 (RSN)
- Key management: WPA-PSK, or WPA-EAP with PEAP and MSCHAPv2 authentication
- Encryption: CCMP (AES)

Important: Supported 802.11 network protocols vary according to the wireless LAN adapter being used with the PDU. For more information, refer to *USB Wireless LAN Adapters* in the Advanced User Manual at www.middleatlantic.com.

Chapter 3: Using the Web Interface

This chapter explains how to use the web interface to administer your PDU.

Supported Web Browsers

- Internet Explorer® 11
- Windows Edge
- Firefox® 25 and later
- Safari® (Mac)
- Google® Chrome® 52 and later
- Android 4.2 and later
- iOS 7.0 and later

Note: Depending on the browser you use, spin controls similar to ⬍ *may or may not appear in the numeric input fields.*

Login, Logout, and Password Change

Access the web interface. The first time you log in to your PDU, use the factory default "admin" user credentials. The network interface and account defaults are as follows:

- Default web interface address:

  192.168.1.200

- Default administrator account credentials:

  Username: **`admin`**

  Password: **`admin`**

After logging in for the first time, the system forces you to change default passwords for security purposes.

Now you can create user accounts for other users. See ***Creating Users*** (on page 72).

Note: The user account is not active until it is set up by the administrator.

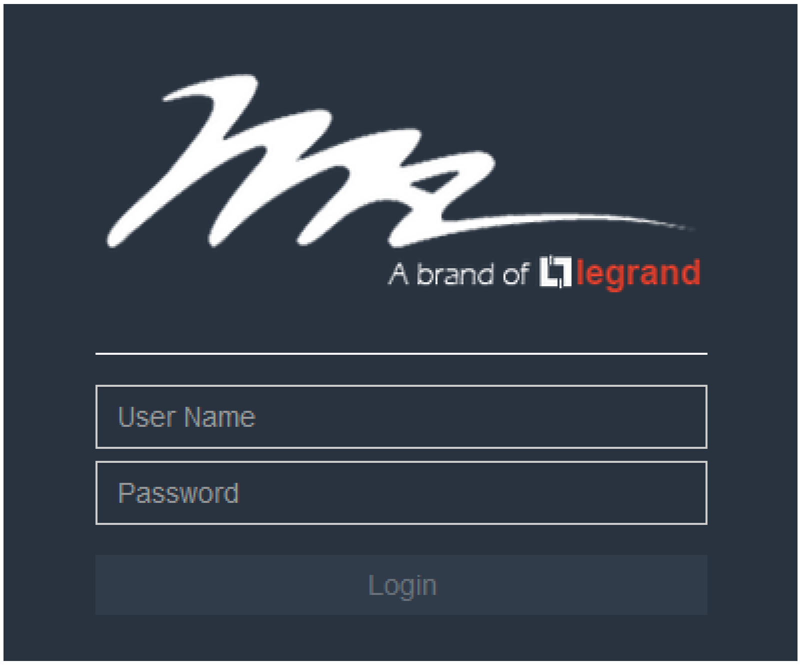
Login

To log in to the web interface:

1. Open a browser and type the IP address of the PDU.
   - If the link-local addressing has been enabled, you can type *pdu.local* instead of the IP address. Refer to ***APIPA and Link-Local Addressing*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.

*Tip: You can also enter the desired page's URL so that you can immediately go to that page after login. See **Quick Access to a Specific Page** (on page 28).*

2. If any security alert message appears, accept it.
3. The login screen displays. Type your user name and password. User credentials are case sensitive.



4. (Optional) If a security agreement is displayed, accept it. Otherwise, you cannot log in.
   - To select the agreement checkbox using the keyboard, first press Tab to go to the checkbox and then Enter.

*Note: To configure the security agreement, see **Enabling the Restricted Service Agreement** (on page 117).*

5. Click Login or press Enter. The web interface opens.

Changing Your Password on First Login

The main administrator account requires you to change the default password when first logging into the system.

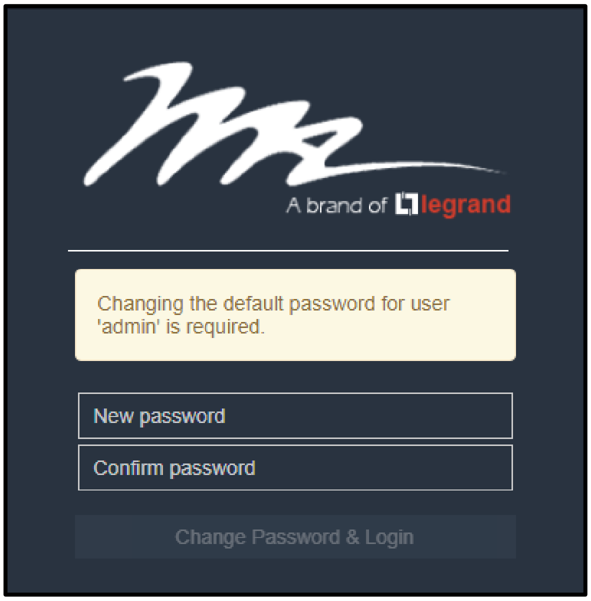
Secondary accounts require the Change Own Password permission enabled for the account to have the required rights to change their own password. See ***Creating Roles*** (on page 76).

You must have Administrator Privileges to change other users' passwords. See ***Editing or Deleting Users*** (on page 76).

For more information about passwords, see ***Changing Your Password*** (on page 79).

Password change request on first login:

On *first login*, the system forces you to change the default password for security purposes.



Changing the default password for user 'admin' is required.

- Enter and confirm your new password and click Change Password & Login.

Remembering User Names and Passwords

Common web browser password managers are supported, including:

- Microsoft Internet Explorer®
- Mozilla Firefox®
- Google Chrome®

You can save the login name and password when these browsers ask to remember them.

For information on how to activate a web browser's password manager, see the user documentation accompanying your browser.

The PDU does NOT support other browser password managers.

Logout

After finishing your tasks, you should log out to prevent others from accessing the web interface.

▶ **To log out without closing the web browser:**

- Click "Logout" on the top-right corner.

  -- OR --

- Close the tab while there are other tabs available in the browser.

▶ **To log out by closing the web browser:**

- Click ☒ on the top-right corner of the window.

  -- OR --

- Choose File > Close, or File > Exit.

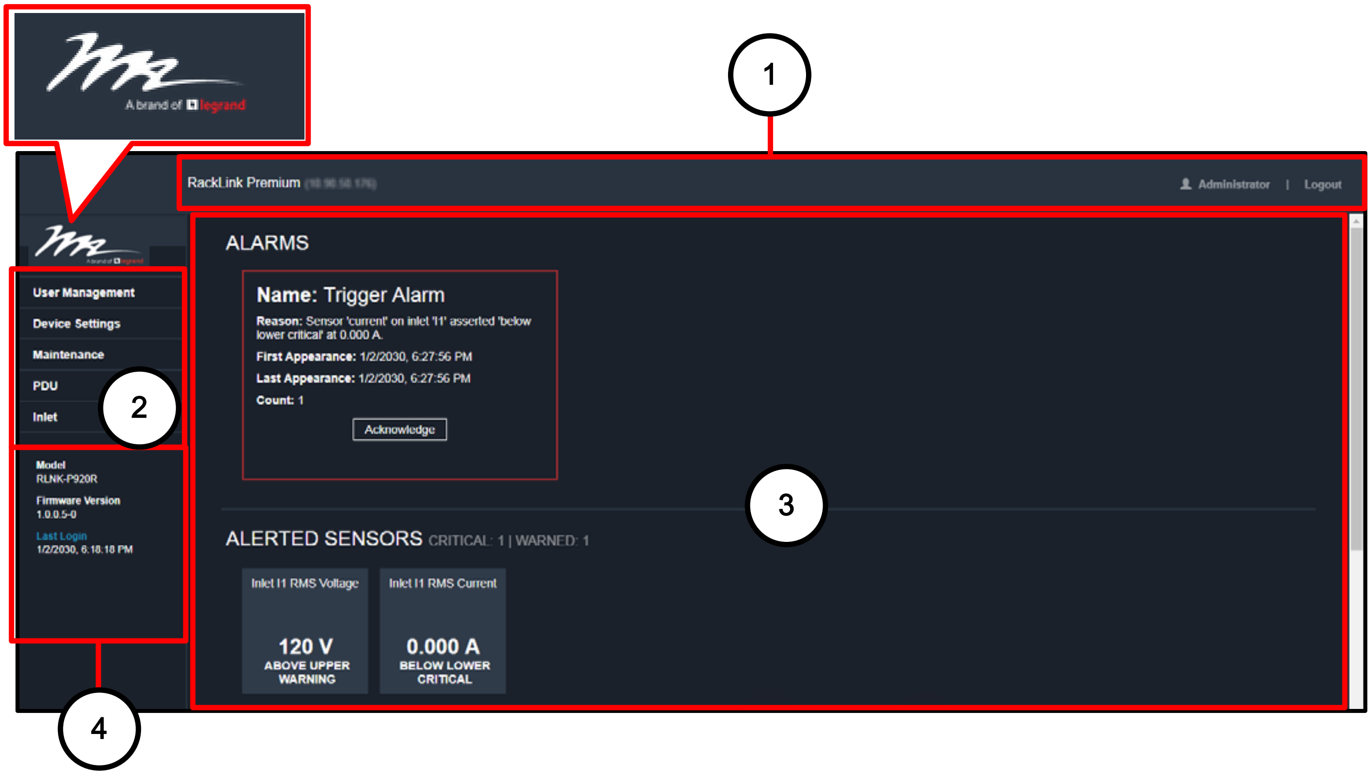
Web Interface Overview

The web interface consists of four areas as shown on the following screen.

▶ **Operation:**

1. Click any menu or submenu item in the area of ②.
2. That item's data/setup page is then opened in the area of ③.
3. Now you can view or configure settings on the opened page.

4. To return to the main menu and the Dashboard page, click on the top-left corner.



RackLink Premium [redacted]

Administrator | Logout

User Management
Device Settings
Maintenance
PDU
Inlet

Model
RLNK-P920R
Firmware Version
1.0.0.5-0
Last Login
1/2/2030, 6:18:18 PM

ALARMS

Name: Trigger Alarm

Reason: Sensor 'current' on inlet 'I1' asserted 'below lower critical' at 0.000 A.

First Appearance: 1/2/2030, 6:27:56 PM

Last Appearance: 1/2/2030, 6:27:56 PM

Count: 1

Acknowledge

ALERTED SENSORS CRITICAL: 1 | WARNED: 1

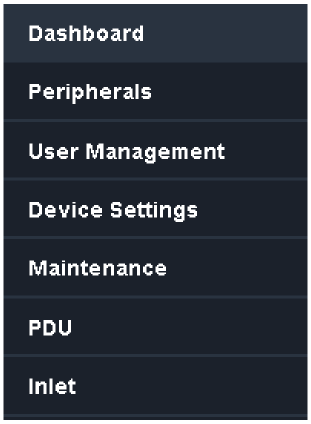
Inlet I1 RMS Voltage	Inlet I1 RMS Current
120 V ABOVE UPPER WARNING	0.000 A BELOW LOWER CRITICAL

Number	Web interface element
1	• Left side: ▪ PDU name *Note: To customize the device name, see **PDU** (on page 183).* • Right side: ▪ Your login name, which you can click to view your user account settings ▪ Logout button
2	See ***Menu*** (on page 27)
3	Content area of the screen.

Number	Web interface element
④	From top to bottom: • Your PDU model • Current firmware version • Date and time of your user account's last login ▪ Click **Last Login** to view your login history.

Menu

Depending on your model and hardware configuration, your PDU may show all or some menu items shown below.



If a menu item contains the submenu, the submenu is shown after clicking that item.

▶ To return to the previous menu list, do any of the following:

- Click the topmost link with the symbol **>**. For example, click ❮ Home.
- Press Backspace on the keyboard.
- OR click A brand of legrand on the top-left corner to return to the main menu.

Quick Access to a Specific Page

If you often visit a specific page in the web interface, you can note its URL or bookmark it with your web browser. Next time, you can simply enter its URL in the address bar of the browser prior to login. After login, the PDU immediately shows the desired page rather than the Dashboard page.

If needed, you can even send the URL to other users so that they can immediately see that page after login, using their own user credentials.

▶ URL examples:

In the following examples, it is assumed that the IP address of the PDU is 192.168.84.118.

Page	URL
Peripherals	https://192.168.84.118/#/peripherals
Event Log	https://192.168.84.118/#/maintenance/eventLog/0

Sorting a List

If any list displays this arrow ▲ in one of its column headers, you are allowed to sort the list by clicking any column header. The list will be sorted in the ascending or descending order based on the selected column.

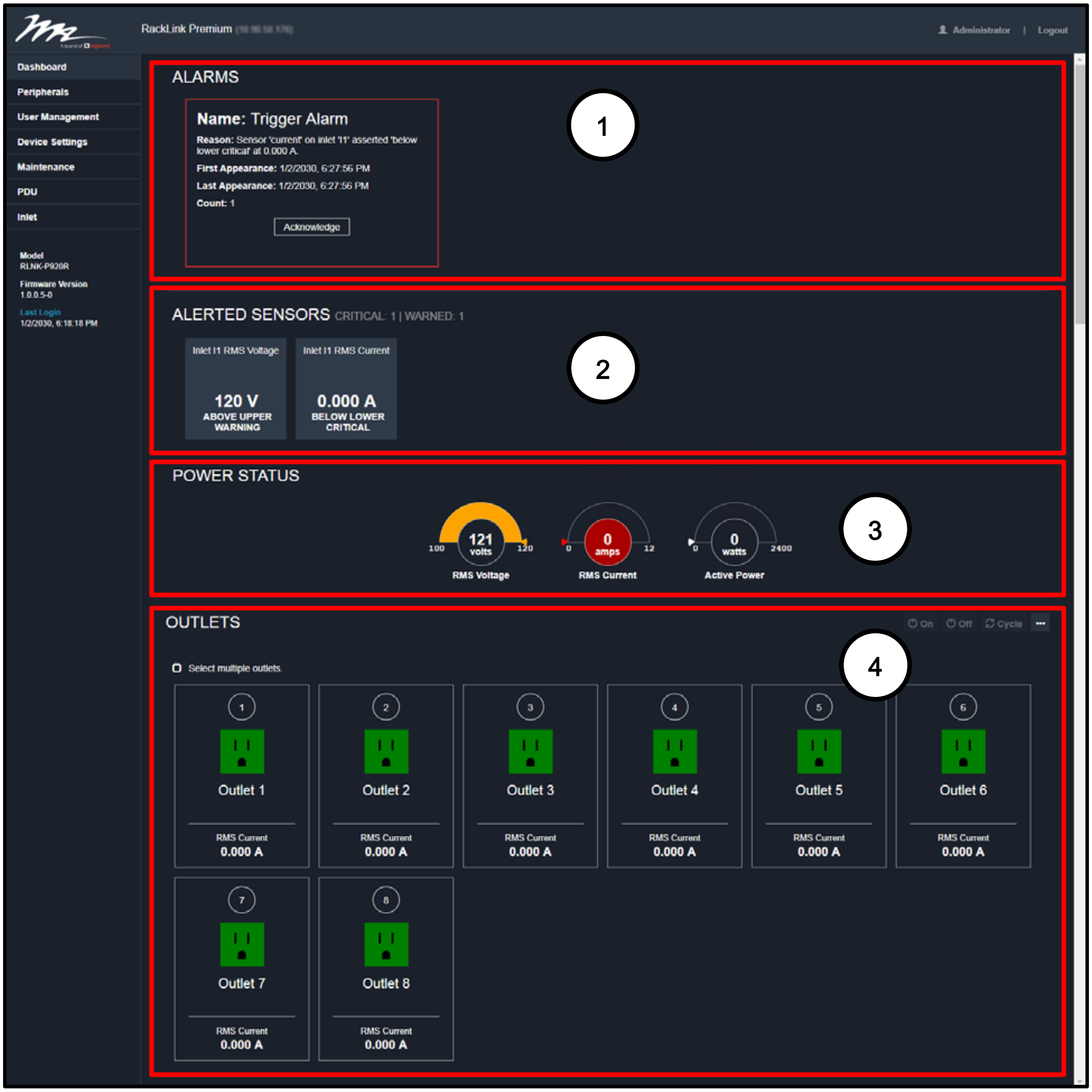
▶ Example:

1. By default, the Peripheral Devices list is sorted in the ascending order based on the # column. Therefore, the arrow ▲ is displayed adjacent to the # header.
2. To have it sorted in the descending order based on the same column, click the # header.
3. The arrow turns to ▲, indicating the list is sorted in the "descending" order. # ▼
4. To sort the list based on a different column, click a different column header.

5. The arrow ▲ now appears adjacent to the selected column header, indicating the list is sorted in the ascending order based on that column.

Dashboard

The Dashboard page contains four sections. However, the Alarms and Alerted Sensors sections only appear when applicable.



RackLink Premium [redacted]

Model
RLNK-P920R

Firmware Version
1.0.0.5-0

Last Login
1/2/2030, 6:18:18 PM

ALARMS

Name: Trigger Alarm

Reason: Sensor 'current' on inlet 'I1' asserted 'below lower critical' at 0.000 A.

First Appearance: 1/2/2030, 6:27:56 PM

Last Appearance: 1/2/2030, 6:27:56 PM

Count: 1

ALERTED SENSORS CRITICAL: 1 | WARNED: 1

Inlet I1 RMS Voltage: 120 V ABOVE UPPER WARNING

Inlet I1 RMS Current: 0.000 A BELOW LOWER CRITICAL

POWER STATUS

OUTLETS

Number	Section	Information shown
①	**Alarms**	• This section can show data only after you have set event rules requiring users to take the acknowledgment action. • When there are no unacknowledged events, this section shows the message "No Alarms." • When there are unacknowledged events, this section lists all of them. See ***Alarms*** (on page 30). • Current hardware failures, if any, also appear on this part of the dashboard. See ***Viewing Hardware Failures*** (on page 180).
②	**Alerted Sensors**	• When no sensors enter the alarmed state, this section shows the message "No Alerted Sensors." • When any sensor enters the alarmed state, this section lists all of them. See ***Alerted Sensors*** (on page 31).
③	**Power Status**	• Overview of inlet power data See ***Inlet Power Status*** (on page 32).
④	**Outlets**	• Displays outlets of your PDU for management and control. See ***Outlets*** (on page 33).

Alarms

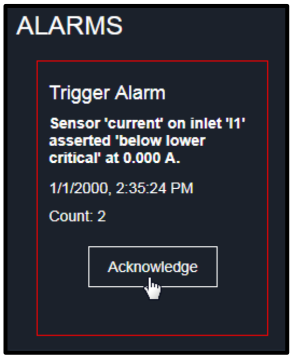
If configuring any event rules which require users to take the acknowledgment action, the Alarms section will list any event which no one acknowledges yet since event occurrence.

*Note: For information on event rules, see **Event Rules and Actions** (on page 120).*

Only users with the Acknowledge Alarms permission can manually acknowledge an alarm.

▶ To acknowledge an alarm:

- Click Acknowledge, and that alarm then disappears from the Alarms section.



ALARMS

Trigger Alarm

Sensor 'current' on inlet 'I1' asserted 'below lower critical' at 0.000 A.

1/1/2000, 2:35:24 PM

Count: 2

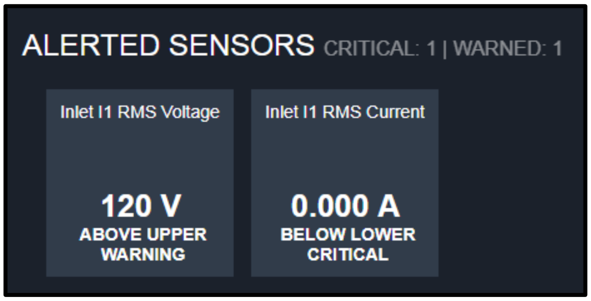
This table explains the display fields shown with an alarm.

Field	Description
Name	The customized name of the Alarm action.
Reason	The first event that triggers the alert.
First Appearance	The date and time when the event indicated in the Reason column occurred for the first time.
Last Appearance	The date and time when the event indicated in the Reason column occurred for the last time.
Count	The number of times the event indicated in the Reason column has occurred.
More Alerts	This field appears only when there are more than one type of event triggering this alert. If there are other types of events (that is, other reasons) triggering the same alert, the total number of additional reasons is displayed. You can click it to view a list of all events triggering this alert.

Alerted Sensors

When any internal sensors or environmental sensor packages connected to the PDU enter an abnormal state, the Alerted Sensors section in the Dashboard show them for alerting users.

To view detailed information or configure each alerted sensor, you can click each sensor's tile to go to individual sensor pages. See *Individual Sensor/Dry Contact Pages* (on page 67).



ALERTED SENSORS CRITICAL: 1 | WARNED: 1

Inlet I1 RMS Voltage
120 V
ABOVE UPPER WARNING

Inlet I1 RMS Current
0.000 A
BELOW LOWER CRITICAL

Summary in the section title:

Information in parentheses adjacent to the title is the total number of alerted sensors.

For example:

- **1 Critical**: 1 sensor enters the critical or alarmed state.

  Numeric sensors enter the critical state.

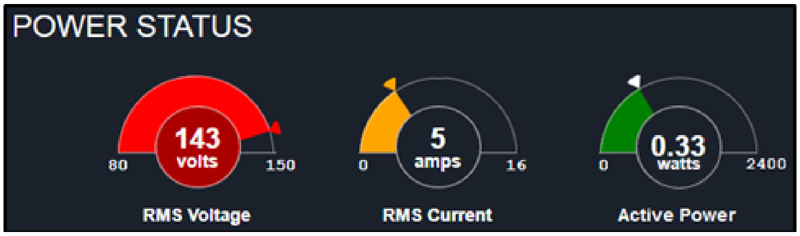
  State sensors enter the alarmed state.

- **1 Warned**: 1 'numeric' sensor enters the warning state.

For details, see *Sensor/Dry Contact States* (on page 64).

Inlet Power Status

The Power Status section of the screen shows the following PDU readings:



POWER STATUS

RMS Voltage: 143 volts (80 – 150)

RMS Current: 5 amps (0 – 16)

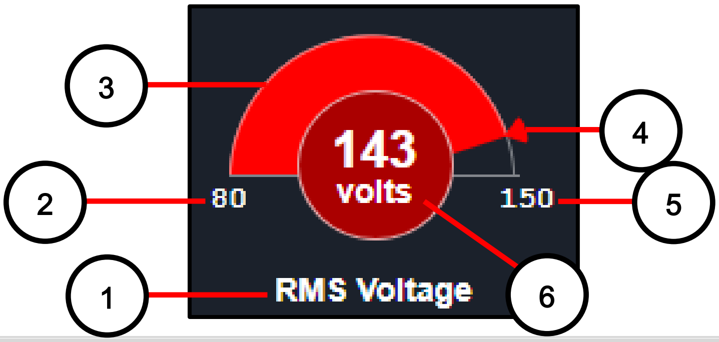
Active Power: 0.33 watts (0 – 2400)

- RMS Voltage
- RMS Current
- Active Power

For more information about these readings, see *Outlet Configuration Page* (on page 42).

Gauge Overview

The current sensor's reading value is displayed on clockwise color indicators

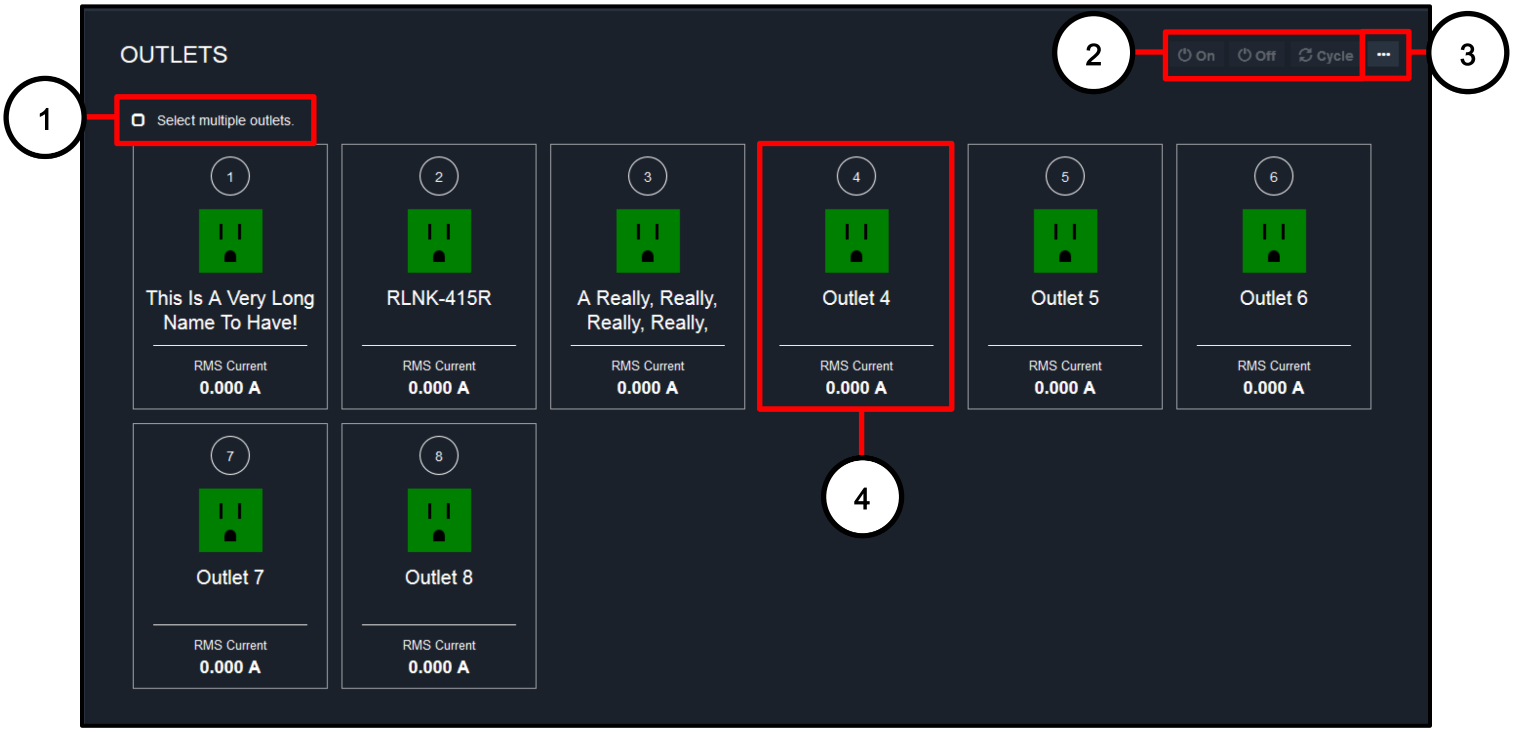


Number	Description
1	Gauge title
2	Minimum displayable gauge value.
3	Gauge reading with threshold color indication. For assigning threshold values and gauge color indicators, see ***Sensor Threshold Settings*** (on page 51).
4	The current reading indicator.
5	Maximum displayable gauge value.
6	The current reading value and unit of measure.

Outlets

The Outlets page shows a list of all outlets and the overview of outlet status and readings on your PDU. To open this page, click 'Dashboard' in the ***Menu*** (on page 27).

Outlets Overview



Number	Description
1	Select Multiple Outlets checkbox. See ***Selecting Multiple Outlets*** (on page 41).
2	Outlet buttons perform the following functions: • Power On. • Power Off. • Power Cycle. Power cycling the outlet(s) turns the outlet(s) off and then back on. *Note: These buttons are only enabled when one or more outlets are selected.*

Number	Description
③	Click the ellipsis ... to access the following additional outlet functions: • **Reset Active Energy**: Resets active energy readings of selected outlets. Only users with the "Admin" role assigned can reset active energy readings. • **Threshold Bulk Setup**: Configures thresholds for all outlets. See ***Threshold Bulk Setup*** (on page 35). • **Sequence Setup**: Configures outlet power-on sequence order and delay for all outlets. See ***Sequence Setup*** (on page 36). • **Load Shedding Setup**: Configures load shedding capabilities for all outlets. See ***Load Shedding Setup*** (on page 38). • **Activate Load Shedding**: Activates and deactivates your configured load shedding settings for all outlets. See ***Load Shedding Mode*** (on page 37). Confirm the operation when prompted.
④	An outlet. See ***Outlet Controls*** (on page 40).

Global Outlet Settings

Threshold Bulk Setup

Outlet thresholds, if enabled, help you identify whether any outlet enters the warning or critical level. See ***Yellow- or Red-Highlighted Sensors*** (on page 63). In addition, you can have the PDU automatically generate alert notifications for any warning or critical status. See ***Event Rules and Actions*** (on page 120).

You can configure the thresholds for multiple or all outlets simultaneously on the Outlets page.

▶ **To configure thresholds-related settings for multiple outlets:**

1. Click the ellipsis ... and select Threshold Bulk Setup.
2. In the "Show Outlet Sensors of Type" field, select a sensor type.

3. Use the checkboxes to select one or multiple outlets.
   - To select ALL outlets, select the topmost checkbox in the header row.
4. Click Edit Thresholds.
5. Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.

   For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** (on page 51).
6. Click Save.

Sequence Setup

By default, outlets are sequentially powered on in the ascending order from outlet 1 to the final when turning ON or power cycling all outlets on the PDU. You can change the order in which the outlets power ON. This is useful when there is a specific order in which equipment should be powered up first.

In addition, you can make a delay occur between two outlets that are turned on consecutively. For example, if the power-on sequence is Outlet 1 through Outlet 8, and you want the PDU to wait for 5 seconds after turning on Outlet 3 before turning on Outlet 4, assign a delay of 5 seconds to Outlet 3.

Setting Outlet Power-On Sequence

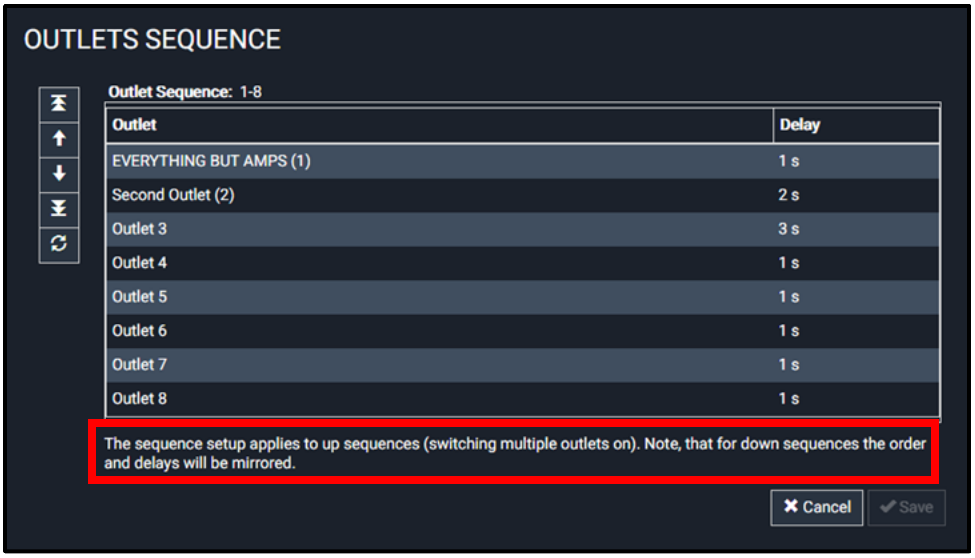
▶ **To set the outlet power-on sequence:**

1. Click the ellipsis ··· and select Sequence Setup.
2. Select one or multiple outlets by clicking them one by one in the 'Outlet' column.
3. Click the arrow buttons to change the outlet positions.

Button	Function
⤒	Top
↑	Up
↓	Down
⤓	Bottom
⟳	Restores to the default sequence

Note:

- *The next time the PDU power cycles, it will turn on all outlets based on the new outlet order.*
- *The new order also applies when performing the power-on or power-cycling operation on partial outlets.*
- *As indicated by the on-screen note, the order applies to "up" or power-on sequences and is mirrored (along with any set delays) for "down" or power-off sequences.*



OUTLETS SEQUENCE

Outlet Sequence: 1-8

Outlet	Delay
EVERYTHING BUT AMPS (1)	1 s
Second Outlet (2)	2 s
Outlet 3	3 s
Outlet 4	1 s
Outlet 5	1 s
Outlet 6	1 s
Outlet 7	1 s
Outlet 8	1 s

The sequence setup applies to up sequences (switching multiple outlets on). Note, that for down sequences the order and delays will be mirrored.

Setting Power-On Delays

► To set power-on delays for outlets:

1. Click the ellipsis ⋯ and select Sequence Setup.
2. Click the 'Delay' column of the outlet that requires a wait after it is turned on.
3. Type a new value in seconds.
4. Click Save.

The PDU inserts a power-on delay between the configured outlet and the one following it during the power-on process.

Load Shedding Mode

When a UPS supplying power to the PDU switches into battery backup operation, it may be desirable to switch off non-critical outlets to conserve UPS battery life. This feature is known as load shedding.

Outlets that are turned off when load shedding is activated are called non-critical. Outlets that are not affected by load shedding are called critical outlets. By default, all outlets are critical. To set non-critical ones, see ***Load Shedding Setup*** (on page 38).

When load shedding is activated, the PDU turns off all non-critical outlets. When load shedding is deactivated, the PDU turns back on all non-critical outlets that were ON before entering the load shedding mode.

Activation of load shedding can be accomplished using the web interface, SNMP or CLI, or triggered by the contact closure sensors.

*Note: It is highly suggested to check the non-critical outlets prior to manually entering the load shedding mode. The non-critical information can be retrieved from the Outlets page. See **Load Shedding Setup** (on page 38).*

Load Shedding Setup

Outlets that are turned off when load shedding is activated are called non-critical. Outlets that are not affected by load shedding are called critical outlets. See ***Load Shedding Mode*** (on page 37).

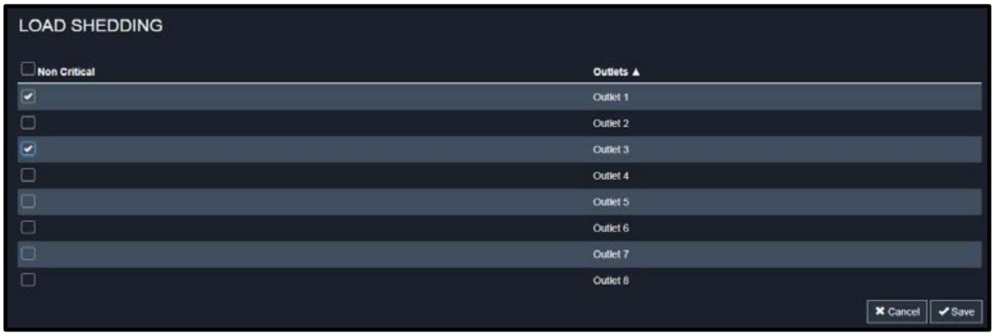
Per default, all outlets are configured as critical.

▶ To determine critical and non-critical outlets:

1. Click the ellipsis ••• and select Load Shedding Setup.

   The Load Shedding Setup screen appears.

2. Use the checkboxes to select Non-critical outlets as desired.



LOAD SHEDDING

□ Non Critical	Outlets ▲
☑	Outlet 1
□	Outlet 2
☑	Outlet 3
□	Outlet 4
□	Outlet 5
□	Outlet 6
□	Outlet 7
□	Outlet 8

3. Click Save.

Tip:

- *To select ALL outlets, select the Non Critical checkbox in the header row.*
- *You can also set up non-critical outlet setting by configuring outlets one by one. See **Viewing** (on page 47).*

Activating Load Shedding Mode

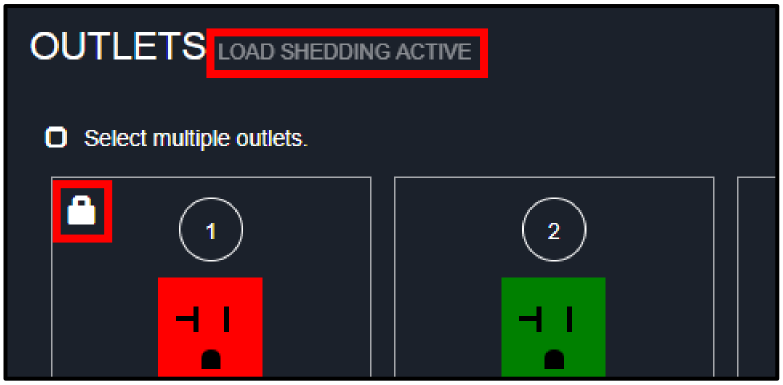
▶ To activate load shedding mode:

1. Click the ellipsis ••• and select Activate Load Shedding.

2. Click Activate on the confirmation message.

   In the load shedding mode:

   - The lock icon 🔒 appears for all non-critical outlets on the Outlets page.
   - On, Off, and Cycle options are disabled for non-critical outlets when load shedding mode is activated.
   - The message "LOAD SHEDDING ACTIVE" appears next to the 'Outlets' title.



Deactivating Load Shedding Mode

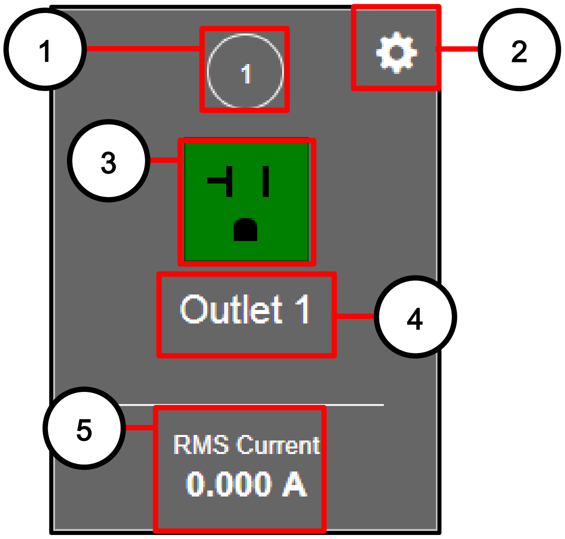
▶ **To deactivate load shedding mode:**

1. Click the ellipsis ··· and select Deactivate Load Shedding.
2. Click Deactivate on the confirmation message.

Now you can turn on/off any outlets.

Outlet Controls

Outlets are displayed on square tiles. Each tile contains information about the outlet as follows:



Number	Description
1	Outlet Number
2	Click the configuration icon ⚙ and the outlet configuration page appears. See ***Outlet Configuration Page*** (on page 42). *Note: The configuration icon only appears after selecting an individual outlet. It will not appear when multiple outlets are selected.*
3	Outlet color status icon. See ***Outlet Color*** States (on page 41).
4	Outlet Name. Configure the name in ***Viewing*** (on page 47).
5	RMS current (A) appears on the outlet.

Outlet Color States

The Outlet status is marked using one of the following colors.

Icon		Outlet status
🟩 15 Amp	🟩 20 Amp	Outlet turned on
🟥 15 Amp	🟥 20 Amp	Outlet turned off
🟨 15 Amp	🟨 20 Amp	Intermediate State – Shows the outlet is in the off state durng a cycle event.

Selecting Multiple Outlets

▶ **To select multiple outlets:**

You can switch any outlet regardless of its current power state. That is, you can turn on any outlet that is already turned on, or turn off any outlet that is already turned off.

1. Click □ Select multiple outlets. to select multiple outlets.

Tip: To perform the desired action on only one outlet, you can simply click the specific outlet without □ Select multiple outlets. *selected, and click the outlet's settings icon* ⚙*. It's outlet's data/setup page then appears.*

---

2. Select multiple outlets.

Individual Outlet Controls

▶ To power control or reset the active energy readings of multiple outlets:

You can switch any outlet regardless of its current power state. That is, you can turn on any outlet that is already turned on, or turn off any outlet that is already turned off.

1. Select the desired outlet(s). See ***Selecting Multiple Outlets*** (on page 41).
2. Click or select the desired button or command.

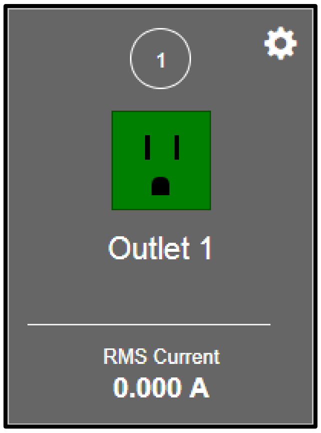
Button or Command	Action
⏻ On	Power ON.
⏻ Off	Power OFF.
↻ Cycle	Power cycle. • Power cycling the outlet(s) turns the outlet(s) off and then back on.
... Reset Active Energy	Resets active energy readings of selected outlets. Only users with the "Admin" role assigned can reset active energy readings.

3. Confirm the operation when prompted.

Tip: To reset ALL active energy counters on the unit, see ***PDU*** *(on page 183). You can also power control an outlet or reset its active energy from* ***Power Controlling a Selected Outlet*** *(on page 43).*

Outlet Configuration Page

An outlet's data/setup page is opened after clicking the outlet, and then its configuration icon ⚙ on the Global Outlets page.



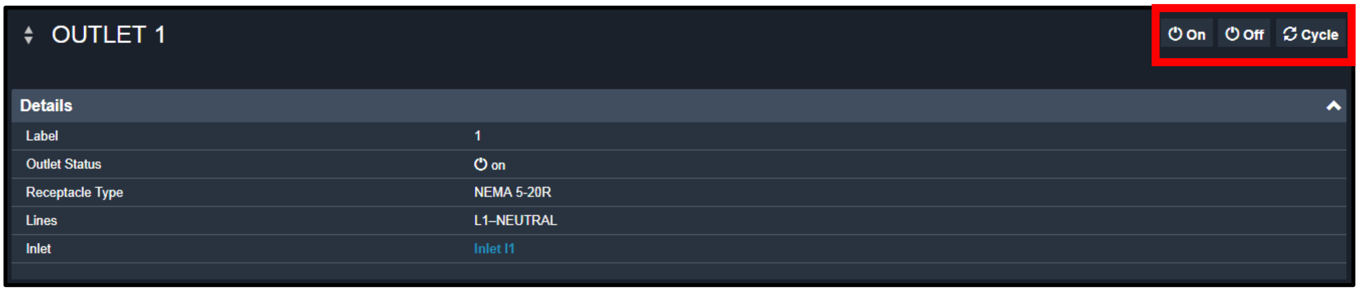
The individual outlet's page shows this outlet's detailed information. See *Viewing Detailed Information on Outlet Pages* (on page 44).

In addition, you can perform the following operations on this outlet page.

Power Controlling a Selected Outlet

▶ To power control a selected outlet:

1. Click one of the power control buttons.



Label	1
Outlet Status	⏻ on
Receptacle Type	NEMA 5-20R
Lines	L1–NEUTRAL
Inlet	Inlet I1

Button/command	Action
⏻ On	Power ON.
⏻ Off	Power OFF.
↻ Cycle	Power cycle. • Power cycling the outlet(s) turns the outlet(s) off and then back on.

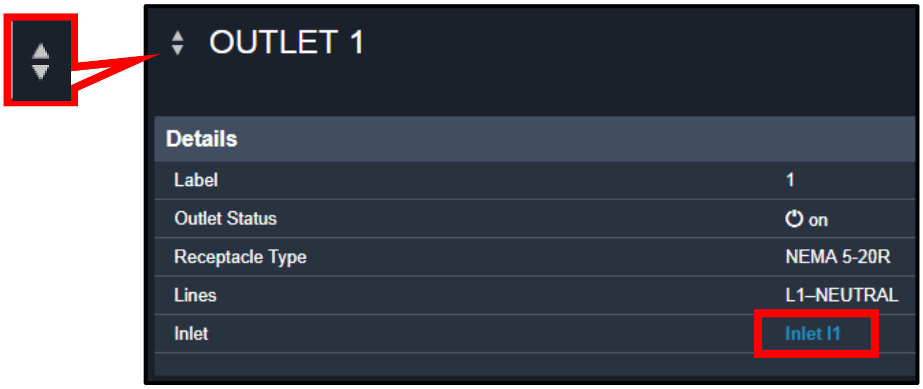
2. Click Confirm when prompted.

Navigating Outlets and Inlet Data Page Access

▶ Navigating outlets and Inlet data page access:

1. You can go to another outlet's data/setup page by clicking the button ▲▼ on the top-left corner of the Outlet Configuration page.

2. You can go to the associated Inlet's data page by clicking the Inlet link in the Details section.



OUTLET 1

Details

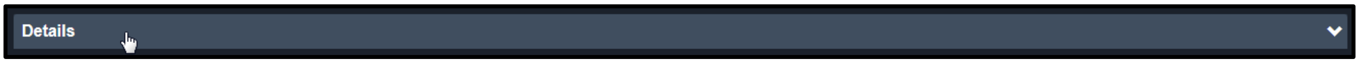
Label	1
Outlet Status	on
Receptacle Type	NEMA 5-20R
Lines	L1–NEUTRAL
Inlet	Inlet I1

Viewing Detailed Information on Outlet Pages

Each outlet's data page has a Details section for showing general outlet information and Sensors section for showing the outlet sensor status.

▶ To view outlet details:

1. Click the Details title bar as shown.



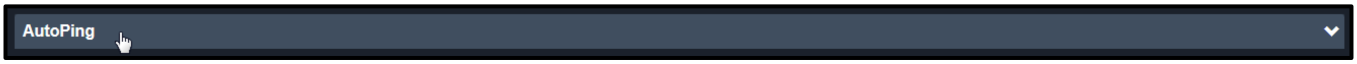
2. View the following data for your selected outlet:

Field	Description
Label	The physical outlet number
Outlet Status	On, Off, or 🔒 off (when load-shedding is activated)
Receptacle Type	This outlet's receptacle type
Lines	Lines associated with this outlet
Inlet	Inlet associated with this outlet
Enable AutoPing	Enables AutoPing functionality for the selected outlet.

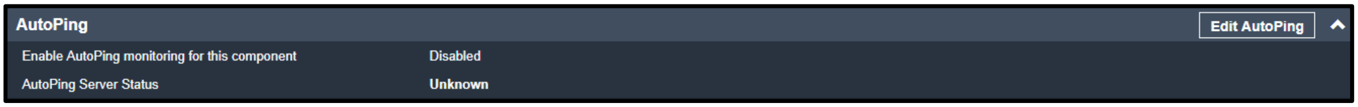
Enabling and Configuring AutoPing

▶ To enable AutoPing:

1. Click the AutoPing title bar as shown.



The following page appears.



Enable AutoPing monitoring for this component	Disabled
AutoPing Server Status	Unknown

2. Click the Edit AutoPing button.
3. Select the checkbox labeled “Enable AutoPing monitoring for this component.”

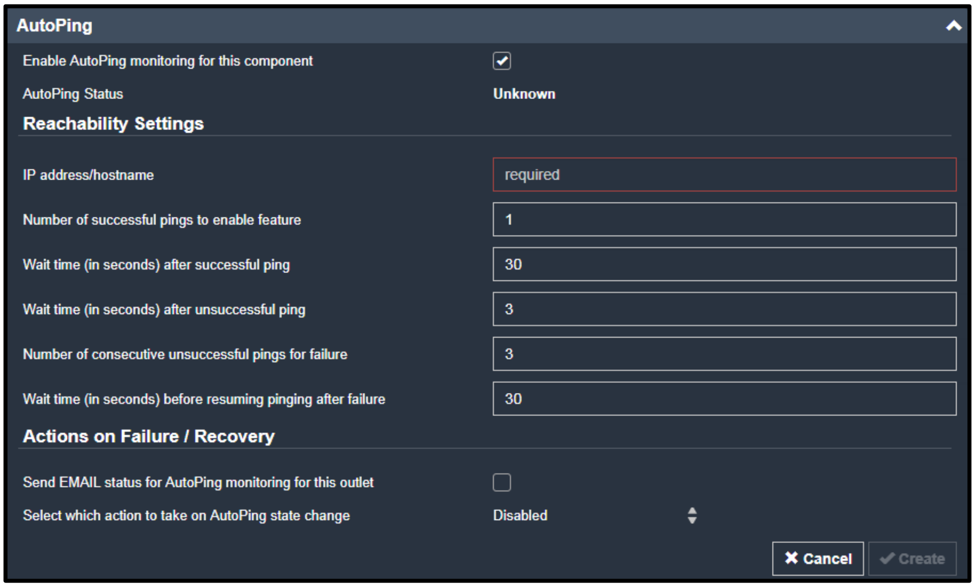
Note: The AutoPing Server Status is a display field showing one of the following component status connections:

- *Monitored*
- *Error*
- *Unreachable*
- *Unrecoverable*

▶ To configure AutoPing:

1. Click the AutoPing title bar as shown.

The AutoPing page appears.



Enable AutoPing monitoring for this component	☑
AutoPing Status	Unknown

Reachability Settings

IP address/hostname	required
Number of successful pings to enable feature	1
Wait time (in seconds) after successful ping	30
Wait time (in seconds) after unsuccessful ping	3
Number of consecutive unsuccessful pings for failure	3
Wait time (in seconds) before resuming pinging after failure	30

Actions on Failure / Recovery

Send EMAIL status for AutoPing monitoring for this outlet	□
Select which action to take on AutoPing state change	Disabled

2. View or edit the following fields in the Reachability Settings section.

Note: All fields are required on this section.

Field	Description
AutoPing Status	Display field showing one of the following component status connections: • Monitored • Error • Unreachable • Unrecoverable
IP address/hostname	Enter the IP address or host name of the component you want to monitor.
Number of successful pings to enable feature	Enter a value for The number of successful pings required to consider the monitored component as "Reachable." Valid range is 0 to 200.
Wait time (in seconds) after successful ping	Enter the wait time before sending the next ping if the previous ping responded successfully. Valid range is 5 to 600 (seconds).
Wait time (in seconds) after unsuccessful ping	Enter the wait time before sending the next ping if the previous ping did not respond. Valid range is 3 to 600 (seconds).
Number of consecutive unsuccessful pings for failure	Enter the number of consecutive pings without any response before the monitored component is considered "Unreachable." Valid range is 1 to 100.
Wait time (in seconds) before resuming pinging after failure	Enter the wait time before the PDU resumes pinging after the monitored equipment is considered "Unreachable." Valid range is 1 to 1200 (seconds).

3. View or edit the following fields in the Actions on Failure/Recovery section.

Field	Description
Send EMAIL status for AutoPing monitoring for this outlet	Select this checkbox to enable email status for AutoPing monitoring of the component.
Recipient Email Addresses	Enter email addresses (separated by commas) to receive AutoPing notifications.

Field	Description
Select which action to take on AutoPing state change	Use the drop-down to select from the following options: • Turn Outlet ON • Turn Outlet ON until Recovery • Turn Outlet OFF • Turn Outlet OFF until Recovery • Cycle Outlet • Cycle Outlet until Recovery
Time between Outlet Cycling (in seconds) *Note: This field only appears when Cycle Outlet or Cycle Outlet Until Recovery is selected in the previous field.*	Enter the number of seconds desired between outlet cycling. Valid range is 1 to 3600. The value entered in this field determines the following: • Cycle Outlet: The duration that the outlet is in the OFF state during the cycling process. • Cycle Outlet until Recovery: The duration that the outlet waits in each transition state during the cycling process (OFF, and then ON).

4. Click Save.

Note: When creating your first AutoPing, the button is labeled Create.

Viewing Sensors

When any internal sensors or environmental sensor packages connected to the PDU enter an abnormal state, the Alerted Sensors section shows them for alerting users. See ***Alerted Sensors*** (on page 31).

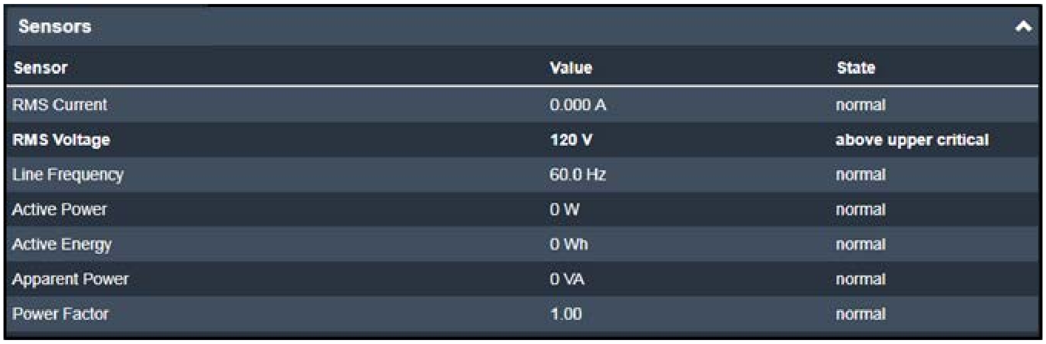
If any outlet sensor enters the alarmed state, it is highlighted in yellow or red. See ***Sensor Threshold Settings*** (on page 51). Sensors show both readings and states.

If desired, you can sort the list by clicking the desired column header. See ***Sorting a List*** (on page 28).

▶ To view sensor data:

1. Click the Sensors title bar as shown.

The sensors page appears.



Sensors

Sensor	Value	State
RMS Current	0.000 A	normal
RMS Voltage	**120 V**	**above upper critical**
Line Frequency	60.0 Hz	normal
Active Power	0 W	normal
Active Energy	0 Wh	normal
Apparent Power	0 VA	normal
Power Factor	1.00	normal

2. The following values are shown:
   - RMS current (A)
   - RMS voltage (V)
   - Active power (W)
   - Active energy (Wh)
   - Apparent power (VA)
   - Power Factor

Oulet Settings

▶ To view and edit outlet settings:

1. Click the Settings title bar as shown.

2. View the following data on the Settings page:
   - Name
   - State on device startup
   - Power off period during power cycle
   - Non-critical
3. Click the Reset Energy button reset the outlet’s active energy, if desired.
4. Click the Edit Settings button to modify the following setting values:

Field	Description
Name	Type an outlet name up to 32 characters long.

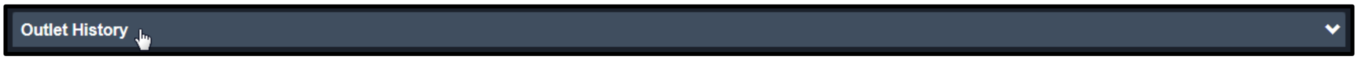
Field	Description
State on device startup	Click this field to select this outlet's initial power state after the PDU powers up. • Options: *on*, *off*, *last known* and *PDU defined*. See ***Options for Outlet State on Startup*** (on page 188). *Note:* *Any option other than "PDU defined" will override the global outlet state setting on this particular outlet.* *PDU defined (xxx) follows the global outlet state setting. The value xxx in parentheses is the currently selected global option - on, off, or last known.*
Power off period during power cycle	Select an option to determine how long this outlet is turned off before turing back on. • Options: *PDU defined (xxx)* or customized time. • PDU defined (xxx) follows the global power-off period setting, which is set on ***PDU*** (on page 183). The value xxx in parentheses is the current global value. • Customized time allows you to either click ▲▼ to select an existing time option or type a new value *with an appropriate time unit added*. See ***Time Units*** (on page 188). *Note: Any time setting other than "PDU defined" will override the global power-off period setting on this particular outlet.*
Non-critical	Select this checkbox only when you want this outlet to turn off in the load shedding mode. See ***Load Shedding Mode*** (on page 37).

5. Click Save.

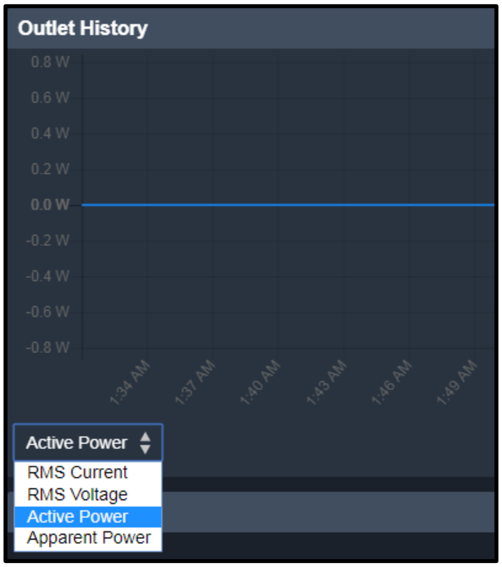
Oulet History

▶ To view outlet history:

1. Click the Outlet History tab or title bar as shown.



2. The Outlet's power waveform, or Outlet History is shown.



3. The power waveform for the outlet helps you observe whether there were abnormal events within the past tens of minutes. The default is to show the outlet's active power data.

4. Click the drop-down ⇕ beneath the diagram to choose a different data type and show the waveform of other outlet power data.

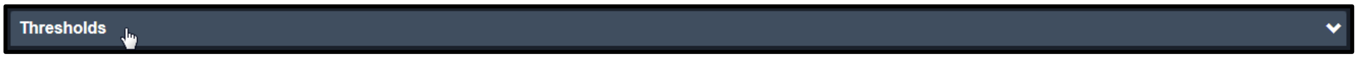
5. Available data types include:

   - RMS Current
   - RMS Voltage
   - Active Power
   - Apparent Power

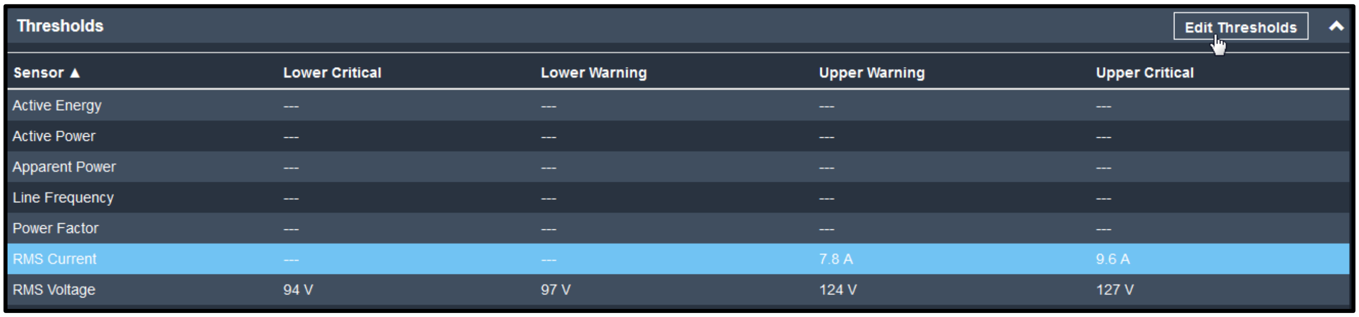
Outlet Thresholds

▶ To configure outlet thresholds:

1. Click the Thresholds tab or title bar as shown.



2. Click the desired sensor (required), and then click Edit Thresholds.



Sensor ▲	Lower Critical	Lower Warning	Upper Warning	Upper Critical
Active Energy	---	---	---	---
Active Power	---	---	---	---
Apparent Power	---	---	---	---
Line Frequency	---	---	---	---
Power Factor	---	---	---	---
RMS Current	---	---	7.8 A	9.6 A
RMS Voltage	94 V	97 V	124 V	127 V

3. Make changes as desired.

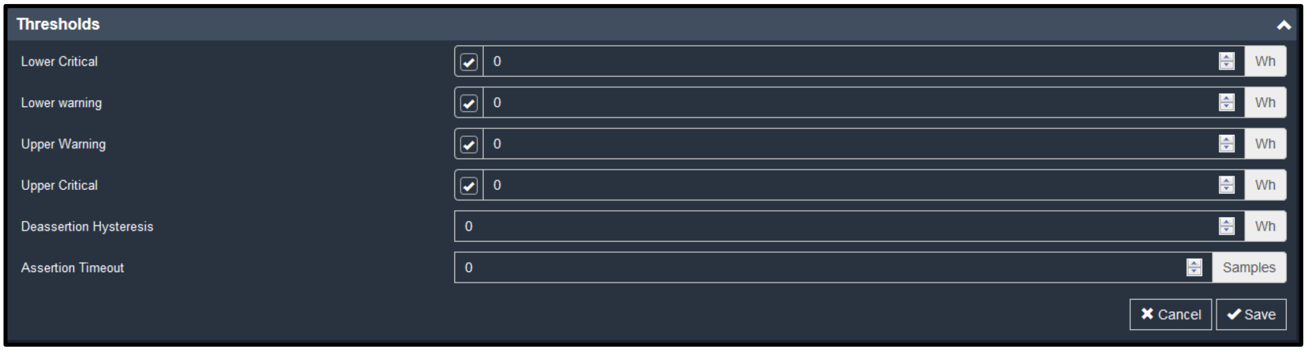
- To enable any threshold, select the corresponding checkbox.
- Type a new value in the accompanying text box.
- Or, use spin controls to dial in values.

For concepts of thresholds, deassertion The PDU and assertion timeout, see *Sensor Threshold Settings* (on page 51).

4. Click Save.

Sensor Threshold Settings

This section explains the thresholds settings for a numeric sensor.



Lower Critical	☑ 0	Wh
Lower warning	☑ 0	Wh
Upper Warning	☑ 0	Wh
Upper Critical	☑ 0	Wh
Deassertion Hysteresis	0	Wh
Assertion Timeout	0	Samples

Thresholds, Sensor States, and Colors

A numeric sensor has four thresholds: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

The threshold settings determine how many sensor states are available for a certain sensor and the range of each sensor state. The diagram below shows how each threshold relates to each state.

In the following table, "R" represents any numeric sensor's reading. The symbol <= means “less than” or "equal to."

Sensor status	Color	States shown in the interface	Description
Unknown	Transparent	unavailable	Sensor state or readings cannot be detected.
		unmanaged	Sensors are not being managed. See ***Managed vs. Unmanaged Sensors/Dry Contacts*** (on page 63). *Note: Managed and unmanaged sensors applies only to Peripherals.*
Normal	Transparent	normal	• Numeric or state sensors are within the normal range. -- OR -- • No thresholds have been enabled for numeric sensors.
Warning	Yellow	above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
		below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
Critical	Red	above upper critical	Upper Critical threshold < "R"
		below lower critical	"R" < Lower Critical threshold
Alarmed	Red	alarmed	State sensors enter the abnormal state.

Available sensor states:

The more thresholds are enabled for a sensor, the more sensor states are available for it. The "normal' state is always available regardless of whether any threshold is enabled.

For example:

- When a sensor only has the Upper Critical threshold enabled, it has two sensor states: normal and above upper critical.
- When a sensor has both the Upper Critical and Upper Warning thresholds enabled, it has three sensor states: normal, above upper warning, and above upper critical.

States of "above upper warning" and "below lower warning" are warning states to call for your attention.

States of "above upper critical" and "below lower critical" are critical states that require you to immediately handle.

Range of each available sensor state:

The value of each enabled threshold determines the reading range of each available sensor state. For details, refer to ***Sensor Threshold Settings*** (on page 51).

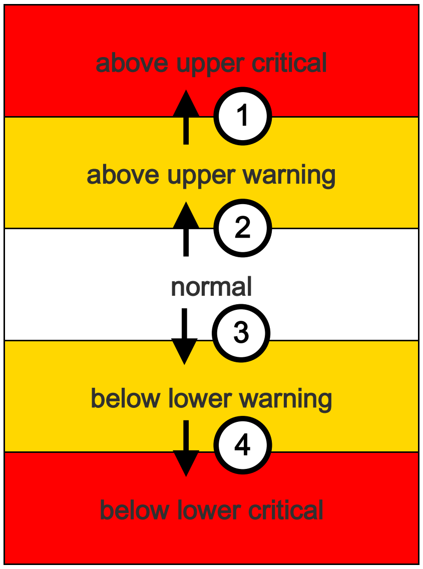
Asserting A State

If multiple sensor states are available for a specific sensor, the PDU asserts a state for it whenever a bad state change occurs.

To assert a state:

To assert a state is to announce a new, "worse" state.

Below are bad state changes that cause the PDU to assert.



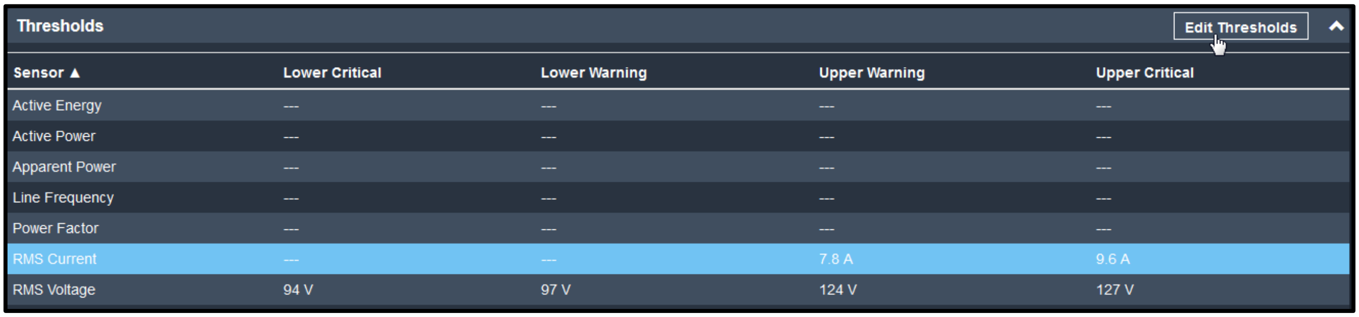
1. above upper warning --> above upper critical
2. normal --> above upper warning
3. normal --> below lower warning
4. below lower warning --> below lower critical

Configuring An Assertion Timeout

Assertion Timeout:

1. Click the Thresholds tab or title bar as shown.

2. Click the desired sensor (required), and then click Edit Thresholds.

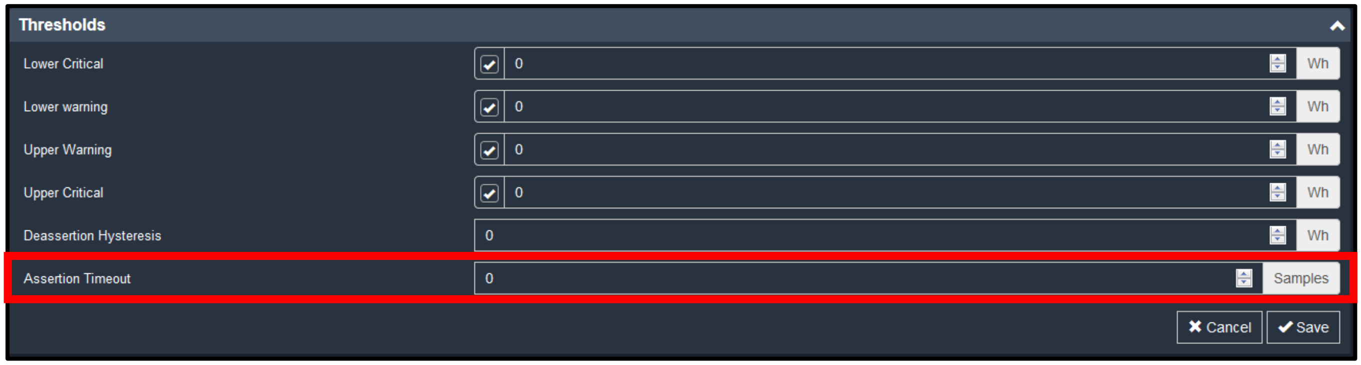


Thresholds

Sensor ▲	Lower Critical	Lower Warning	Upper Warning	Upper Critical
Active Energy	---	---	---	---
Active Power	---	---	---	---
Apparent Power	---	---	---	---
Line Frequency	---	---	---	---
Power Factor	---	---	---	---
RMS Current	---	---	7.8 A	9.6 A
RMS Voltage	94 V	97 V	124 V	127 V

The Edit Thresholds page appears.

3. Modify the Assertion Timeout field as desired.



Thresholds

Lower Critical	☑ 0	Wh
Lower warning	☑ 0	Wh
Upper Warning	☑ 0	Wh
Upper Critical	☑ 0	Wh
Deassertion Hysteresis	0	Wh
Assertion Timeout	0	Samples

In the threshold settings, the Assertion Timeout field postpones or even cancels the "assertion" action. It determines how long a sensor must be in the "worse" new state before the PDU triggers the "assertion" action. If that sensor changes its state again within the specified wait time, the PDU does NOT assert the worse state.

Note:

- *To disable the assertion timeout, set it to 0 (zero).*
- *For most sensors, the measurement unit in the "Assertion Timeout" field is sample. Sensors are measured every second, so the timing of a sample is equal to a second. BCM2 is an exception to this, with a sample of 3 seconds.*

---

4. Click Save.

How "Assertion Timeout" is helpful:

If you have created an event rule that instructs the PDU to send notifications for assertion events, setting the "Assertion Timeout" is helpful for eliminating a number of notifications that you may receive in case the sensor's readings fluctuate around a certain threshold.

Assertion Timeout Example for Temperature Sensors

Assumption:

```
Upper Warning threshold is enabled.
Upper Warning = 25 (degrees Celsius)
Assertion Timeout = 5 samples (that is, 5 seconds)
```

When a temperature sensor's reading exceeds 25 degrees Celsius, moving from the "normal" range to the "above upper warning" range, the PDU does NOT immediately announce this warning state. Instead it waits for 5 seconds, and then does either of the following:

- If the temperature remains above 25 degrees Celsius in the "above upper warning" range for 5 seconds, the PDU performs the "assertion" action to announce the "above upper warning" state.
- If the temperature drops below 25 degrees Celsius within 5 seconds, the PDU does NOT perform the "assertion" action.

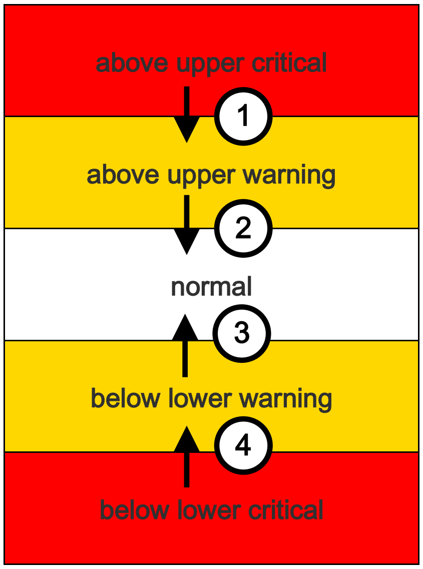
"To De-assert" and Deassertion Hysteresis

After the PDU asserts a worse state for a sensor, it may de-assert that state later on if the readings improve.

► To de-assert a state:

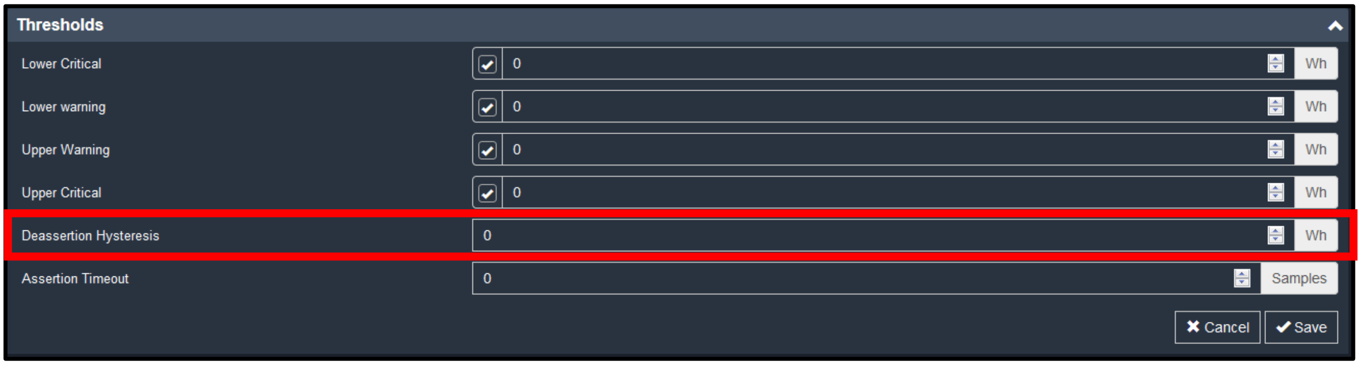
To de-assert a state is to announce the end of the previously asserted worse state.

Below are good state changes that cause the PDU to de-assert the previous state.



1. above upper critical --> above upper warning
2. above upper warning --> normal
3. below lower warning --> normal
4. below lower critical --> below lower warning

Deassertion Hysteresis:



Thresholds

Lower Critical	☑	0	Wh
Lower warning	☑	0	Wh
Upper Warning	☑	0	Wh
Upper Critical	☑	0	Wh
Deassertion Hysteresis		0	Wh
Assertion Timeout		0	Samples

In the threshold settings, the Deassertion Hysteresis field determines a new level to trigger the "deassertion" action.

This function is similar to a thermostat, which instructs the air conditioner to turn on the cooling system when the temperature exceeds a pre-determined level. "Deassertion Hysteresis" instructs the PDU to de-assert the worse state for a sensor only when that sensor's reading reaches the pre-determined "deassertion" level.

For upper thresholds, this "deassertion" level is a decrease against each threshold. For lower thresholds, this level is an increase to each threshold. The absolute value of the decrease/increase is exactly the hysteresis value.

For example, if Deassertion Hysteresis = 2, then:

- Upper Critical = 33, so its "deassertion" level = 33 - 2 = 31.
- Upper Warning = 25, so its "deassertion" level = 25 - 2 = 23.
- Lower Critical = 10, so its "deassertion" level = 10 + 2 = 12.
- Lower Warning = 18, so its "deassertion" level = 18 + 2 = 20.

To use each threshold as the "deassertion" level instead of determining a new level, set the Deassertion Hysteresis to 0 (zero).

How "Deassertion Hysteresis" is helpful:

If you have created an event rule that instructs the PDU to send notifications for deassertion events, setting the "Deassertion Hysteresis" is helpful for eliminating a number of notifications that you may receive in case a sensor's readings fluctuate around a certain threshold.

Deassertion Hysteresis Example for Temperature Sensors

Assumption:

```
   Upper Warning threshold is enabled.
   Upper Warning = 20 (degrees Celsius)
   Deassertion Hysteresis = 3 (degrees Celsius)
   "Deassertion"  level = 20-3 = 17 (degrees Celsius)
```

When the PDU detects that a temperature sensor's reading drops below 20 degrees Celsius, moving from the "above upper warning" range to the "normal" range, either of the following may occur:

- If the temperature falls between 20 and 17 degrees Celsius, the PDU does NOT perform the "deassertion" action.
- If the temperature drops to 17 degrees Celsius or lower, the PDU performs the "deassertion" action to announce the end of the "above upper warning" state.

Peripherals

If there are environmental sensor packages connected to the PDU, they are listed on the Peripherals page. For more information, refer to the Premium+ PDU with RackLink Environmental Sensors User Manual at www.middleatlantic.com.

An environmental sensor package comprises one or some of the following sensors/dry contacts:

- Numeric sensors: Detectors that show both readings and states, such as temperature sensors.
- State sensors: Detectors that show states only, such as contact closure sensors.
- Dry contacts: A dry contact controls a system or mechanism so it shows states only.

The PDU communicates with *managed* sensors/dry contacts only and retrieves their data. It does not communicate with unmanaged ones. See ***Managed vs. Unmanaged Sensors/Dry Contacts*** (on page 63).

When the number of "managed" sensors/dry contacts has not reached the maximum, the PDU automatically brings newly detected sensors/dry contacts under management by default.

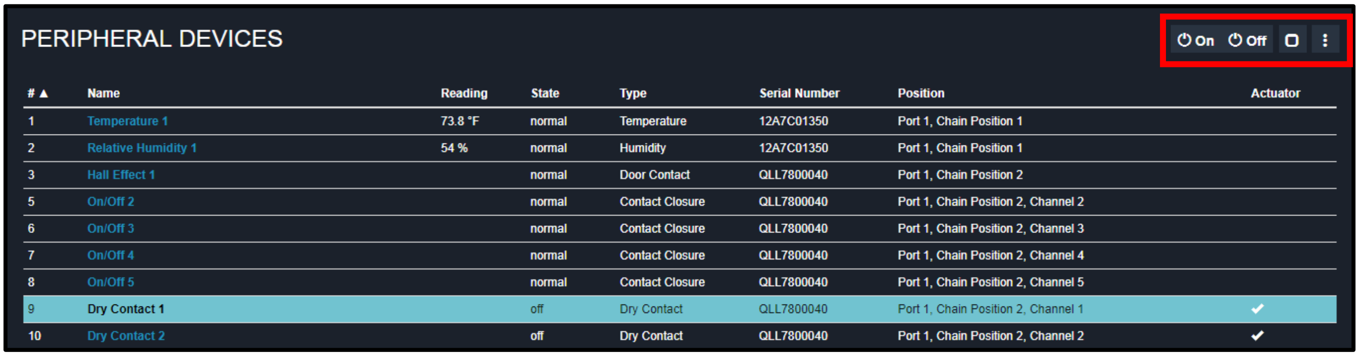
One PDU can manage a maximum of 32 sensors/dry contacts.

*Note: To disable the automatic management function, see **How the Automatic Management Function Works** (on page 188). You need to manually manage a sensor/dry contact only when it is not under management.*

When any sensor/dry contact is no longer needed, you can unmanage/release it.

Open the Peripherals page by clicking Peripherals in the ***Menu*** (on page 27). Then you can:

- Perform actions on multiple sensors/dry contacts by using the control/action icons on the top-right corner.

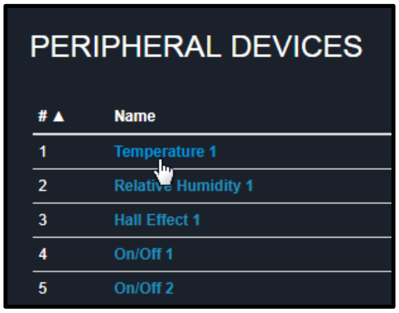


PERIPHERAL DEVICES

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	Temperature 1	73.8 °F	normal	Temperature	12A7C01350	Port 1, Chain Position 1	
2	Relative Humidity 1	54 %	normal	Humidity	12A7C01350	Port 1, Chain Position 1	
3	Hall Effect 1		normal	Door Contact	QLL7800040	Port 1, Chain Position 2	
5	On/Off 2		normal	Contact Closure	QLL7800040	Port 1, Chain Position 2, Channel 2	
6	On/Off 3		normal	Contact Closure	QLL7800040	Port 1, Chain Position 2, Channel 3	
7	On/Off 4		normal	Contact Closure	QLL7800040	Port 1, Chain Position 2, Channel 4	
8	On/Off 5		normal	Contact Closure	QLL7800040	Port 1, Chain Position 2, Channel 5	
9	Dry Contact 1		off	Dry Contact	QLL7800040	Port 1, Chain Position 2, Channel 1	✓
10	Dry Contact 2		off	Dry Contact	QLL7800040	Port 1, Chain Position 2, Channel 2	✓

Note: On and Off buttons only appear when dry contacts are selected.

- Go to an individual sensor's or dry contact's data/setup page by clicking its name.



PERIPHERAL DEVICES

# ▲	Name
1	Temperature 1
2	Relative Humidity 1
3	Hall Effect 1
4	On/Off 1
5	On/Off 2

If desired, you can sort the list by clicking the desired column header. See ***Sorting a List*** (on page 28).

Sensor/dry contact overview on this page:

If any sensor enters the alarmed state, it is highlighted in yellow or red. See ***Yellow- or Red-Highlighted Sensors*** (on page 63). An dry contact is never highlighted.

Column	Description
Name	By default the PDU assigns a name comprising the following two elements to a newly managed sensor/dry contact. • Sensor type, such as "Temperature". • Sequential number of the same sensor/dry contact type, like 1, 2, 3 and so on. You can customize the name. See ***Individual Sensor/Dry Contact Pages*** (on page 67).
Reading	Only managed 'numeric' sensors show this data, such as temperature and humidity sensors.
State	The data is available for all sensors and dry contacts. See ***Sensor/Dry Contact States*** (on page 64).
Type	Sensor or dry contact type.
Serial Number	This is the serial number printed on the sensor package's label. It helps to identify your sensors/dry contacts. See ***Finding the Sensor's Serial Number*** (on page 66).
Position	The data indicates where this sensor or dry contact is located in the sensor chain. See ***Identifying the Sensor Position and Channel*** (on page 66).
Actuator	Indicates whether this sensor package is an actuator or not. If yes, the symbol ☑ is shown.

To release sensors/dry contacts:

When the total of managed sensors/dry contacts reaches the maximum (32), you cannot manage additional ones. The only way to manage any sensor/dry contact is to release or replace any managed ones. To replace a managed sensor/dry contact, see ***Managing One Sensor or*** (on page 67). To release them, follow this procedure.

1. Click Peripherals > ☑ to make checkboxes appear in front of sensors/actuators.

   Tip: To perform the desired action on only one sensor/actuator, simply click that sensor/actuator without making the checkboxes appear.

2. Select multiple sensors/actuators.

   Tip: To select ALL sensors/actuators, select the topmost checkbox in the header row.

3. Select "managed" sensors/actuators. See **Sensor/Dry Contact States** (on page 64).
4. Click ⋮ > Release.
5. Now released sensors/actuators become "unmanaged."

Managing One Sensor or Dry Contact

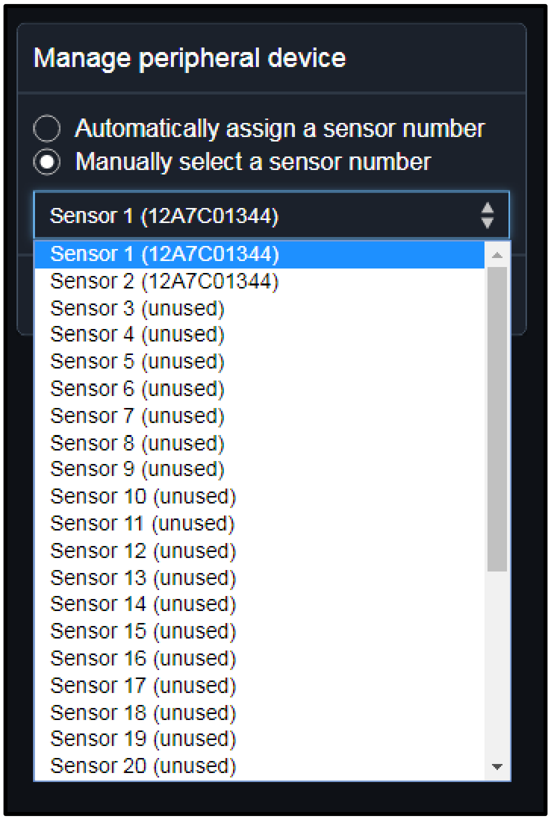
If you are managing only one sensor or dry contact, you can assign the desired ID number to it. Note that you cannot assign ID numbers when you are managing multiple sensors/dry contacts at a time.

Tip: When the total of managed sensors/dry contacts reaches the maximum (32), you cannot manage additional ones. The only way to manage any sensor/dry contact is to release or replace any managed ones. To replace a managed one, assign an ID number to it by following this procedure. To release any one, see ***Peripherals*** *(on page 57).*

▶ To manage only one sensor/dry contact:

1. Click Peripherals.
2. From the list of "unmanaged" sensors/dry contacts, click the one you want to manage.

   The "Manage peripheral device" dialog appears.



Manage peripheral device

○ Automatically assign a sensor number
● Manually select a sensor number

Sensor 1 (12A7C01344)

- To let the PDU randomly assign an ID number to it, select "Automatically assign a sensor number."

  This method does not release any managed sensor or dry contact.

- To assign the desired ID number to it, select "Manually select a sensor number." Then click ⬍ to select an ID number.

  This method may release a managed sensor/dry contact if the number you selected has been assigned to a specific sensor/dry contact.

Tip: The information in parentheses following each ID number indicates whether the number has been assigned to a sensor or dry contact. If it has been assigned to a sensor or dry contact, it shows its serial number. Otherwise, it shows the word "unused."

3. Click Manage.

Managing Multiple Sensors/Dry Contacts

▶ To manage multiple sensors/dry contacts:

When the total of managed sensors/dry contacts reaches the maximum (32), you cannot manage additional ones. The only way to manage any sensor/dry contact is to release or replace any managed ones. To replace a managed sensor/dry contact, see ***Managing One Sensor or*** (on page 67). To manage them, follow this procedure.

1. Click Peripherals > ☑ to make checkboxes appear in front of sensors/actuators.

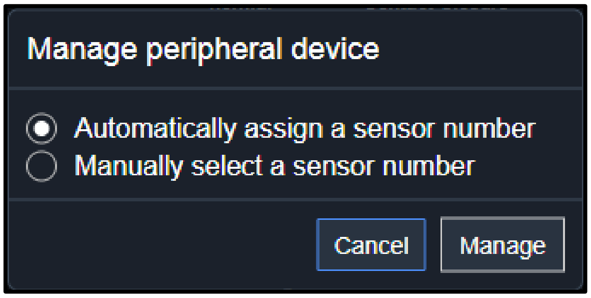
   Tip: To perform the desired action on only one sensor/actuator, simply click that sensor/actuator without making the checkboxes appear.

2. Select multiple sensors/actuators.

   Tip: To select ALL sensors/actuators, select the topmost checkbox in the header row.

3. Select "unmanaged" sensors/actuators.

4. Click Peripherals > ⋮ > Manage.
   - The management action triggers a "Manage peripheral device" dialog. Simply click Manage if you are managing *multiple* sensors/actuators.



Manage peripheral device

● Automatically assign a sensor number
○ Manually select a sensor number

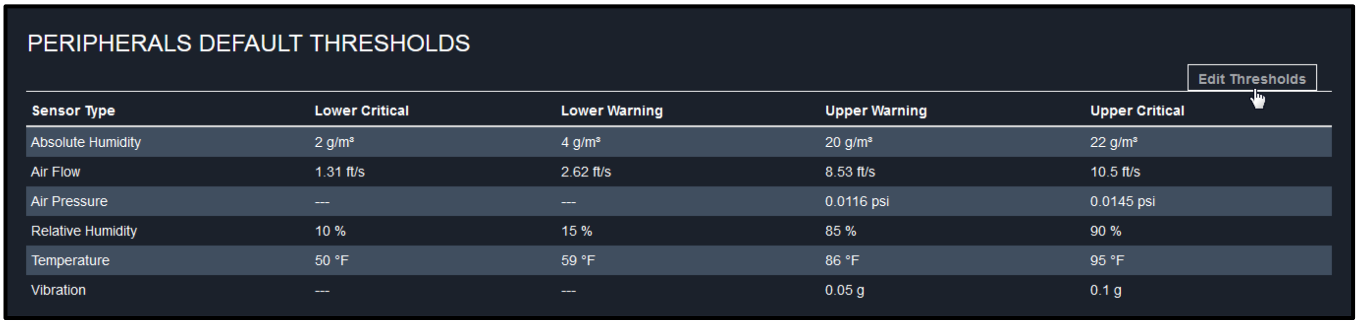
   - If you are managing only *one* sensor/actuator, you can choose to assign an ID number by selecting "Manually select a sensor number." See ***Managing One Sensor or*** (on page 67).
5. Managed sensors/dry contacts show one of the managed states.

Configuring Default Threshold Settings

▶ To configure default threshold settings:

Any changes made to default threshold settings not only re-determine the initial threshold values applying to newly added sensors but also the threshold values of the already-managed sensors where default thresholds are being used. See ***Individual Sensor/Dry Contact Pages*** (on page 67).

1. Click Peripherals > ⋮ > Default Threshold Setup.
2. Click the desired sensor type (required), and then click Edit Thresholds.



PERIPHERALS DEFAULT THRESHOLDS

Sensor Type	Lower Critical	Lower Warning	Upper Warning	Upper Critical
Absolute Humidity	2 g/m^3	4 g/m^3	20 g/m^3	22 g/m^3
Air Flow	1.31 ft/s	2.62 ft/s	8.53 ft/s	10.5 ft/s
Air Pressure	---	---	0.0116 psi	0.0145 psi
Relative Humidity	10 %	15 %	85 %	90 %
Temperature	50 °F	59 °F	86 °F	95 °F
Vibration	---	---	0.05 g	0.1 g

3. Make changes as needed.
4. To enable any threshold, select the corresponding checkbox.
5. Type a new value in the accompanying text box.

   For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** (on page 51).

6. Click Save.

*Tip: To customize the threshold settings on a per-sensor basis, see **Individual Sensor/Dry Contact Pages** (on page 67).*

Turning ON or OFF Dry Contacts

▶ To turn on or off dry contact(s):

1. Click Peripherals.
2. Select one or multiple dry contacts which are *in the same status*; meaning, on or off.
3. To select multiple dry contacts, click ☑ to make checkboxes appear and then select desired dry contacts.
4. Click the desired button.
   - ⏻ On: Turn ON.
   - ⏻ Off: Turn OFF.
5. Confirm the operation when prompted.

Yellow- or Red-Highlighted Sensors

The PDU highlights the sensors entering the abnormal state with a yellow or red color. Note that numeric sensors can change colors only after you have enabled their thresholds.

Tip: When an dry contact is turned ON, it is also highlighted in red for drawing attention.

For concepts of thresholds, deassertion hysteresis, assertion timeout, and coloring see ***Sensor Threshold Settings*** (on page 51).

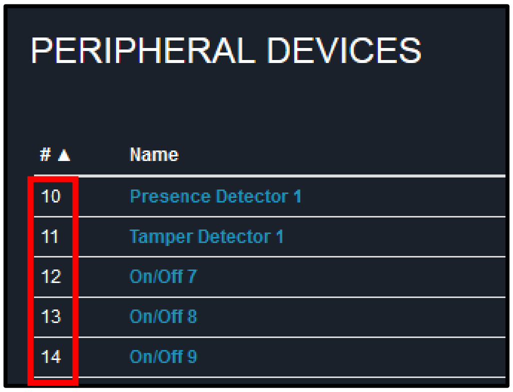
Managed vs. Unmanaged Sensors/Dry Contacts

To manually manage or unmanage/release a sensor or dry contact, see ***Peripherals*** (on page 57).

▶ Managed sensors/dry contacts:

- The PDU communicates with managed sensors/dry contacts and retrieves their data.
- Managed sensors/dry contacts are always listed on the Peripheral Devices page no matter they are physically connected or not.

- They have an ID number as illustrated below.



PERIPHERAL DEVICES

# ▲	Name
10	Presence Detector 1
11	Tamper Detector 1
12	On/Off 7
13	On/Off 8
14	On/Off 9

- They show one of the managed states. See ***Sensor/Dry Contact States*** (on page 64).
- For managed 'numeric' sensors, their readings are retrieved and displayed. If any numeric sensor is disconnected or its reading cannot be retrieved, it shows "unavailable" for its reading.

Understanding Unmanaged Sensors/Dry Contacts

▶ **Unmanaged sensors/dry contacts:**

- The PDU neither communicates with unmanaged sensors/dry contacts nor retrieves their data.
- Unmanaged sensors/dry contacts are listed only when they are physically connected to the PDU. They disappear when they are no longer connected.
- They do *not* have an ID number.
- They show the "unmanaged" state.

Sensor/Dry Contact States

An environmental sensor or dry contact shows its real-time state after being managed.

Available sensor states depend on the sensor type -- numeric or state sensors. For example, a contact closure sensor is a state sensor so it switches between three states only -- *unavailable*, *alarmed* and *normal*.

Sensors will be highlighted in yellow or red when they enter abnormal states. See ***Yellow- or Red-Highlighted Sensors*** (on page 63).

An dry contact's state is marked in red when it is turned on.

Managed sensor states:

In the following table, "R" represents any numeric sensor's reading. The symbol <= means "less than" or "equal to."

State	Description
normal	• For numeric sensors, it means the readings are within the normal range. • For state sensors, it means they enter the normal state.
below lower critical	"R" < Lower Critical threshold
below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
above upper critical	Upper Critical threshold < "R"
alarmed	The state sensor enters the abnormal state.
unavailable	• The communication with the managed sensor is lost. -- OR -- • Sensor packages are upgrading their sensor firmware.

Note: On contact closure sensors, the normal state depends on the normal setting you have configured. For more information, refer to the Premium+ PDU With RackLink Environmental Sensors User Manual at www.middleatlantic.com .

Managed dry contact states:

State	Description
on	The dry contact is turned on.
off	The dry contact is turned off.
unavailable	• The communication with the managed dry contact is lost. -- OR -- • Sensor packages are upgrading their sensor firmware.

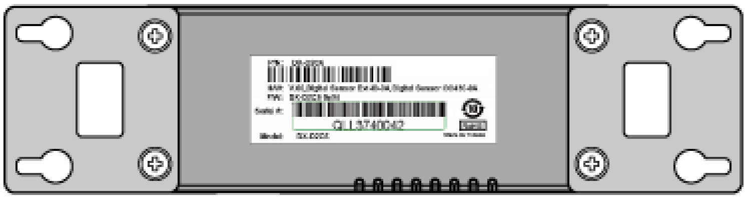
Unmanaged sensor/dry contact states:

State	Description
unmanaged	Sensors or dry contacts are physically connected to the PDU but not managed yet.

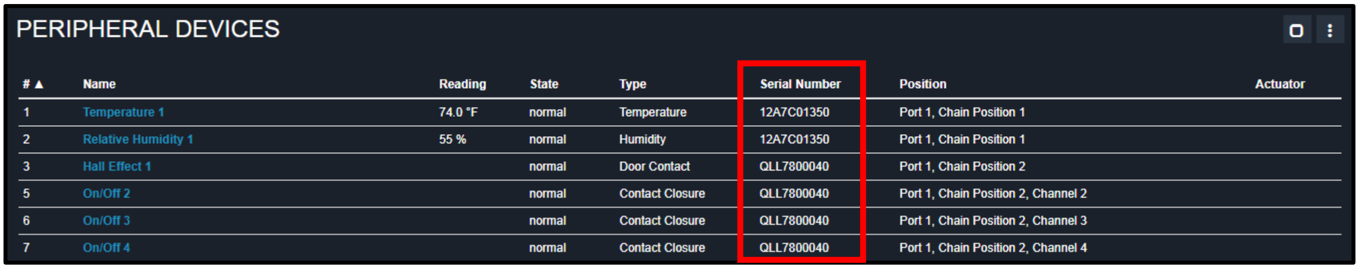
Note: Unmanaged sensors or dry contacts will disappear from the web interface after they are no longer physically *connected to the PDU. To manage a sensor/dry contact, see* ***Peripherals*** *(on page 57).*

Finding the Sensor's Serial Number

A RLNK-TEMP or RLNK-CONT sensor package has a serial number tag attached to its underside.



The serial number for each sensor or actuator appears listed in the web interface after each sensor or actuator is detected by the PDU. Match the serial number from the tag to those listed in the sensor table.

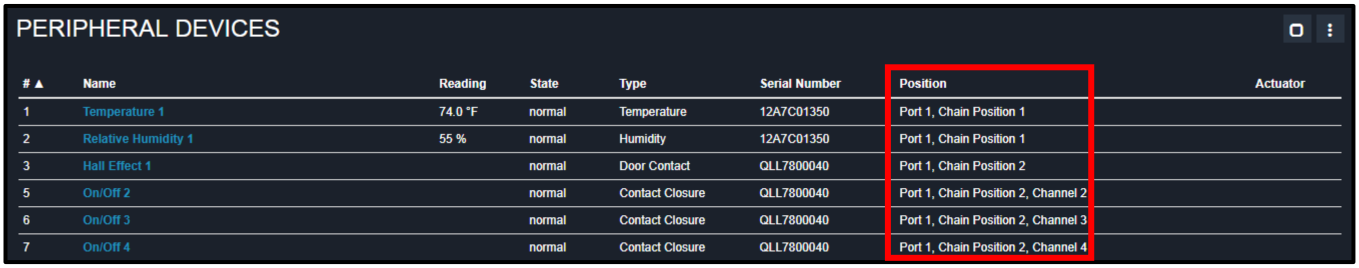


PERIPHERAL DEVICES

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	Temperature 1	74.0 °F	normal	Temperature	12A7C01350	Port 1, Chain Position 1	
2	Relative Humidity 1	55 %	normal	Humidity	12A7C01350	Port 1, Chain Position 1	
3	Hall Effect 1		normal	Door Contact	QLL7800040	Port 1, Chain Position 2	
5	On/Off 2		normal	Contact Closure	QLL7800040	Port 1, Chain Position 2, Channel 2	
6	On/Off 3		normal	Contact Closure	QLL7800040	Port 1, Chain Position 2, Channel 3	
7	On/Off 4		normal	Contact Closure	QLL7800040	Port 1, Chain Position 2, Channel 4	

Identifying the Sensor Position and Channel

The PDU can indicate where each sensor or actuator is connected on the Peripheral Devices page.



PERIPHERAL DEVICES

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	Temperature 1	74.0 °F	normal	Temperature	12A7C01350	Port 1, Chain Position 1	
2	Relative Humidity 1	55 %	normal	Humidity	12A7C01350	Port 1, Chain Position 1	
3	Hall Effect 1		normal	Door Contact	QLL7800040	Port 1, Chain Position 2	
5	On/Off 2		normal	Contact Closure	QLL7800040	Port 1, Chain Position 2, Channel 2	
6	On/Off 3		normal	Contact Closure	QLL7800040	Port 1, Chain Position 2, Channel 3	
7	On/Off 4		normal	Contact Closure	QLL7800040	Port 1, Chain Position 2, Channel 4	

- Both the sensor port number and its position in a sensor chain appears.

  For example, *Port 1, Chain Position 2*.

- If a sensor/actuator contains channels, such as a contact closure or dry contact sensor, the channel information is included in the position information.

  For example, *Channel 1*.

Understanding Sensor/Dry Contact Position

Sensor/dry contact position examples:

Example	Physical position
Port 1	Connected to the sensor port #1.
Port 1, Channel 2	• Connected to the sensor port #1. • The sensor/dry contact is the 2nd channel of the sensor package.
Port 1, Chain Position 4	• Connected to the sensor port #1. • The sensor/dry contact is located in the 4th sensor package of the sensor chain.
Port 1, Chain Position 3, Channel 2	• Connected to the sensor port #1. • The sensor/dry contact is located in the 3rd sensor package of the sensor chain. • It is the 2nd channel of the sensor package.

Individual Sensor/Dry Contact Pages

A sensor's or dry contact's data/setup page is opened after clicking any sensor or dry contact name on the Peripheral Devices page. See *Peripherals* (on page 57).

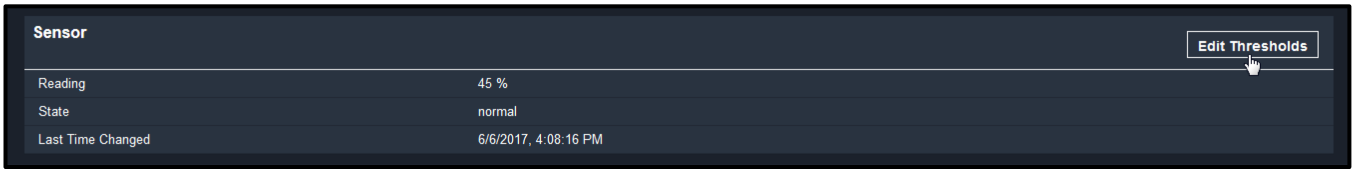
Note that only a numeric sensor has threshold settings, while a state sensor or dry contact has no thresholds.

Threshold settings, if enabled, help you identify whether any numeric sensor enters the warning or critical level. See *Yellow- or Red-Highlighted Sensors* (on page 63). In addition, you can have the PDU automatically generate alert notifications for any warning or critical status. See *Event Rules and Actions* (on page 120).

Configuring a Numeric Sensor's Threshold Settings

To configure a numeric sensor's threshold settings:

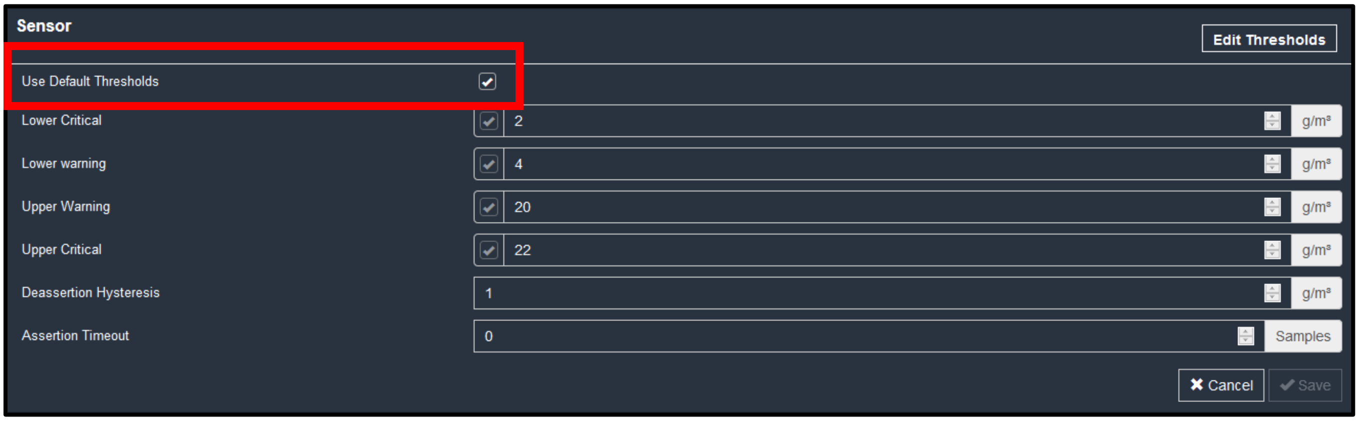
1. Click Edit Thresholds.



Sensor

Reading	45 %
State	normal
Last Time Changed	6/6/2017, 4:08:16 PM

2. Select or deselect Use Default Thresholds according to your needs.



Sensor

Use Default Thresholds	☑	
Lower Critical	☑ 2	g/m³
Lower warning	☑ 4	g/m³
Upper Warning	☑ 20	g/m³
Upper Critical	☑ 22	g/m³
Deassertion Hysteresis	1	g/m³
Assertion Timeout	0	Samples

- To have this sensor follow the default threshold settings configured for its sensor type, select the Use Default Thresholds checkbox.

  The default threshold settings are configured on the page of ***Peripherals*** (on page 57).

- To customize the threshold settings for this particular sensor, deselect the Use Default Thresholds checkbox, and then modify the threshold fields below it.

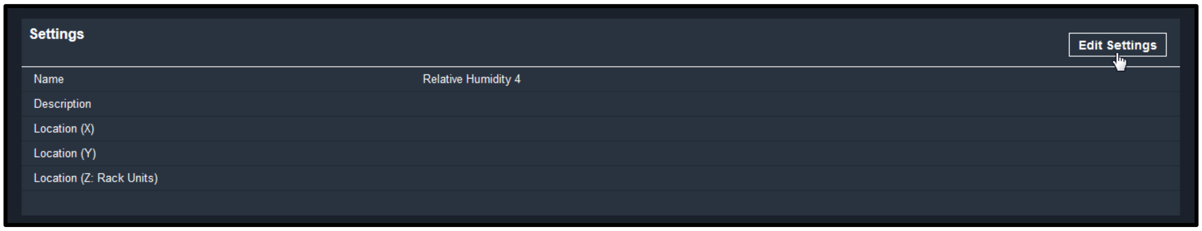
Note: For concepts of thresholds, deassertion hysteresis and assertion timeout, see ***Sensor Threshold Settings*** *(on page 51).*

3. Click Save.

Setting Up a Sensor's or Dry Contact's Physical Location and Additional Settings

▶ To set up a sensor's or dry contact's physical location and additional settings:

1. Click Edit Settings.



Settings

Name	Relative Humidity 4
Description	
Location (X)	
Location (Y)	
Location (Z: Rack Units)	

2. Make changes to available fields, and then click Save.

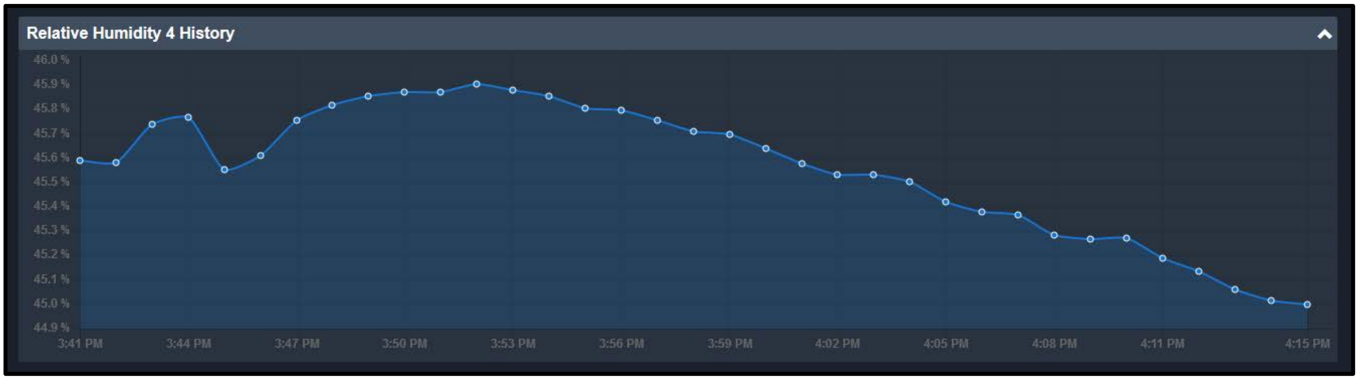
Fields	Description
Binary Sensor Subtype	This field is available for a contact closure sensor only. Determine the sensor type of your contact closure detector. • *Contact Closure* detects the door lock or door open/closed status. • *Smoke Detection* detects the appearance of smoke. • *Water Detection* detects the appearance of water on the floor. • *Vibration* detects the vibration of the floor.
Name	A name for the sensor or dry contact.
Description	Any descriptive text you want.
Location (X, Y and Z)	Describe the sensor's or dry contact's location in the data center by typing alphanumeric values for the X, Y and Z coordinates. See ***Sensor/Dry Contact Location Example*** (on page 71). If the term "Rack Units" appears in parentheses in the Z location, you must type an integer number. Note that the Z coordinate's format is determined on the page of ***PDU*** (on page 183).

3. Click Save.

Viewing a Numeric Sensor's Readings History Waveform

▶ To view a numeric sensor's readings history waveform:

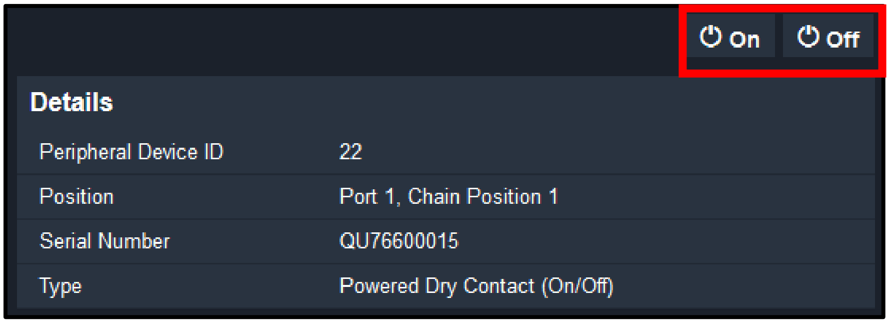
This sensor's data within the past tens of minutes is shown in the waveform diagram. Note that only a numeric sensor has this diagram. State sensors and dry contacts do not show this data.



Turning On or Off an Dry Contact From the Sensor/Dry Contact Page

To turn on or off a dry conctact from the sensor/dry contact page:

1. Click the desired control button.



Details

Peripheral Device ID	22
Position	Port 1, Chain Position 1
Serial Number	QU76600015
Type	Powered Dry Contact (On/Off)

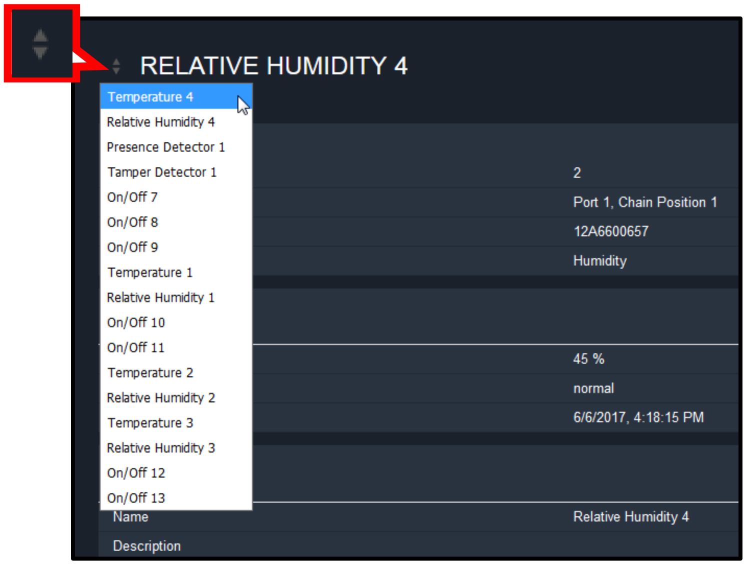
- ⏻ On: Turn ON.
- ⏻ Off: Turn OFF.

2. Confirm the operation on the confirmation message. An dry contact's state is marked in red when it is turned on.

Using Other Sensor or Dry Contact Operations

Other operations:

You can go to another sensor's or dry contacts's data/setup page by clicking the selector ⇕ on the top-left corner.



RELATIVE HUMIDITY 4

2

Port 1, Chain Position 1

12A6600657

Humidity

45 %

normal

6/6/2017, 4:18:15 PM

Name	Relative Humidity 4
Description	

Sensor/Dry Contact Location Example

Use the X, Y and Z coordinates to describe each sensor's or dry contact's physical location in the data center. See ***Individual Sensor/Dry Contact Pages*** (on page 67).

The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. Therefore, you can use non-measurement values.

▶ Example:

X = `Brown Cabinet Row`

Y = `Third Rack`

Z = `Top of Cabinet`

▶ Values of the X, Y and Z coordinates:

- X and Y: They can be any alphanumeric values comprising 0 to 24 characters.
- Z: When the Z coordinate format is set to *Rack Units*, it can be any number ranging from 0 to 60. When its format is set to *Free-Form*, it can be any alphanumeric value comprising 0 to 24 characters. See ***PDU*** (on page 183).

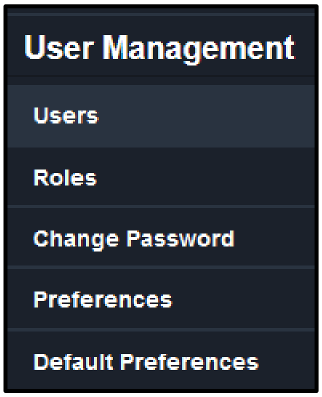
User Management

User Management menu deals with user accounts, permissions, and preferred measurement units on a per-user basis.

The PDU is shipped with one built-in administrator account: **admin**, which is ideal for initial login and system administrator. You can neither delete 'admin' nor change its permissions. For more information about login defaults, see ***Login, Logout, and Password Change*** (on page 22).

A "role" determines the tasks/actions a user is permitted to perform on the PDU, so you must assign one or multiple roles to each user.

Click 'User Management' in the ***Menu*** (on page 27), and the following submenu appears.

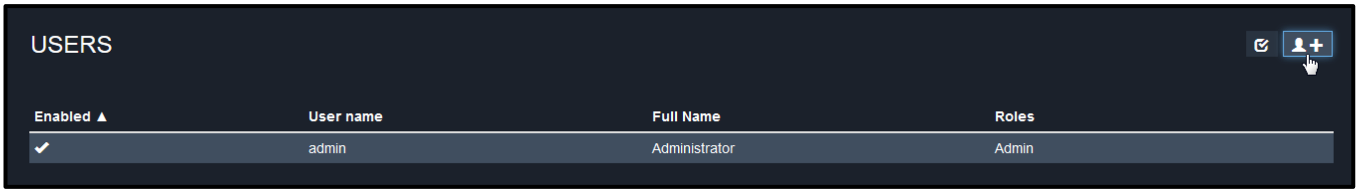


Creating Users

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

▶ To create users:

1. Select User Management > Users > .



USERS

Enabled ▲	User name	Full Name	Roles
✓	admin	Administrator	Admin

The New User page appears.

2. Provide information in the following fields or settings in the User section of the New User page as follows:

Note: You must enter information in the fields showing the message 'required.'

required

Field or Setting	Description
User Name	The name the user enters to log in to the PDU. • 4 to 32 characters • Case sensitive • Spaces are NOT permitted.
Full Name	The user's first and last names.
Password, Confirm Password	• 4 to 64 characters • Case sensitive • Spaces are permitted.
Telephone Number	The user's telephone number
eMail Address	The user's email address • Up to 64 characters • Case sensitive
Enable	When selected, the user can log in to the PDU.

3. You need to enter the SSH public key only if the public key authentication for SSH is enabled. See ***Changing SSH Settings*** (on page 95).
4. Open the SSH public key with a text editor.
5. Copy and paste all content in the text editor into the SSH Public Key field.
6. The SNMPv3 access permission is disabled by default.

Field or Setting	Description
Enable SNMPv3	Select this checkbox when intending to permit the SNMPv3 access by this user. *Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See* ***Configuring SNMP Settings*** *(on page 92).*
Security Level	Click the field to select a preferred security level from the list: • None: No authentication and no privacy. This is the default. • Authentication: Authentication and no privacy. • Authentication & Privacy: Authentication and privacy.

7. The Authentication Password section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

Field or Setting	Description
Same as User Password	Select this checkbox if the authentication password is identical to the user's password. To specify a different authentication password, disable the checkbox.
Password, Confirm Password	Type the authentication password if the 'Same as User Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

8. The Privacy Password section is configurable only when SNMPv3 is enabled and 'Authentication & Privacy' is selected as the Security Level above.

Field or Setting	Description
Same as Authentication Password	Select this checkbox if the privacy password is identical to the authentication password. To specify a different privacy password, disable the checkbox.
Password, Confirm Password	Type the privacy password if the 'Same as Authentication Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

9. The Protocol section and its fields or settings is only configurable when 'Authentication' or 'Authentication & Privacy' is selected.

Field or Setting	Description
Authentication	Click this field to select the desired authentication protocol. Two protocols are available: • MD5 • SHA-1 (default)
Privacy	Click this field to select the desired privacy protocol. Two protocols are available: • DES (default) • AES-128

10. The Preferences section determines the measurement units displayed in the web interface and command line interface for this user.

Field	Description
Temperature Unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length Unit	Preferred units for length or height -- Meter or Feet.
Pressure Unit	Preferred units for pressure -- Pascal or Psi. • Pascal = one newton per square meter • Psi = pounds per square inch

Note: Users can change the measurement units at any time by setting their own preferences. See ***Setting Your Preferred Measurement Units*** *(on page 79).*

11. In the Roles section, select one or multiple roles to determine the user's permissions.

Tip: To select all roles, select the top-most checkbox in the header row..

If the built-in roles do not satisfy your needs, add new roles by clicking 👤+ New Role. See ***Creating Roles*** (on page 76).

The Operator role is assigned to a newly created user account by default.

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently used permissions, including: • Acknowledge Alarms • Change Own Password • Change PDU, Inlet, Outlet & Overcurrent Protector Configuration • Switch Outlets • View Event Settings • View Local Event Log

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

12. Click Save.

Viewing Enabled or Disabled Users

► To view enabled or disabled user accounts:

1. Select User Management > Users to open the Users page, which lists all user accounts.
2. View one of the following icons for each user listed in the Enabled column:
   - ✓: The user is enabled.
   - ✖: The user is disabled.

*Tip: If desired, you can sort the list by clicking the desired column header. See **Sorting a List** (on page 28).*

Editing or Deleting Users

▶ To edit or delete a user account:

1. Select User Management > Users to open the Users page, which lists all user accounts.
2. Click the desired user.

   The Edit User page for that user appears.
3. Make changes as desired.
   - For information on each field, see ***Creating Users*** (on page 72).
   - To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password remains unchanged.
   - To delete this user, click 🗑, and confirm the operation.
4. Click Save.

Deleting Multiple User Accounts

▶ To delete multiple user accounts:

1. Select User Management > Users to open the Users page, which lists all user accounts.
2. On the Users page, click ☑ to make checkboxes appear in front of user names.

Tip: To delete only one user, you can simply click that user without making the checkboxes appear. See the previous procedure.

3. Select one or multiple users.
   - To select all roles, except for the admin role, select the top-most checkbox in the header row.
4. Click 🗑.
5. Click Delete on the confirmation message.

Creating Roles

A role is a combination of permissions. Each user must have at least one role.

The PDU provides two built-in roles. The Operator role is assigned to a newly created user account per default. See ***Creating Users*** (on page 72).

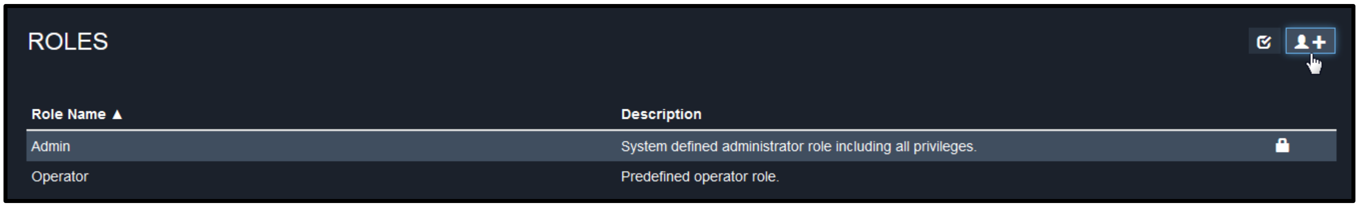
Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently used permissions, including: • Acknowledge Alarms • Change Own Password • Change PDU, Inlet, Outlet & Overcurrent Protector Configuration • Switch Outlets • View Event Settings • View Local Event Log

If the two do not satisfy your needs, add new roles.

To create a role:

1. Select User Management > Roles > 👤+.

   The Roles page appears.

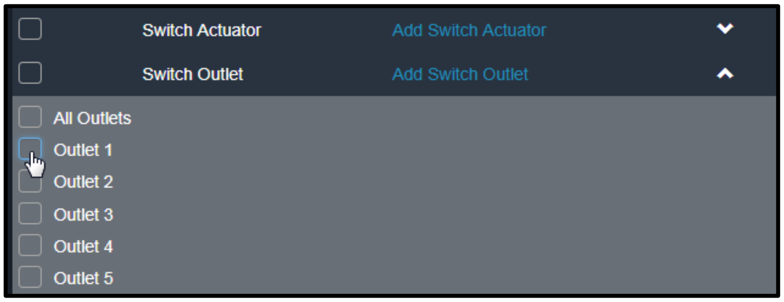


ROLES

Role Name ▲	Description
Admin	System defined administrator role including all privileges.
Operator	Predefined operator role.

2. Assign a role name.
   - 1 to 32 characters long
   - Case sensitive
   - Spaces are permitted
3. Type a description for the role in the Description field.
4. Select the desired privilege(s).
   - The 'Administrator Privileges' includes all privileges.
   - The 'Unrestricted View Privileges' includes all 'View' privileges.
5. To select any privilege requiring the argument setting, click + to select the desired arguments.

- For example, on an outlet-switching capable model, you can specify the outlets that are allowed to be switched on/off for the 'Switch Outlet' privilege as shown below.



□ Switch Actuator Add Switch Actuator

□ Switch Outlet Add Switch Outlet

□ All Outlets
□ Outlet 1
□ Outlet 2
□ Outlet 3
□ Outlet 4
□ Outlet 5

6. Click Save.

Now you can assign the role to any user. See ***Creating Users*** (on page 72) or ***Editing or Deleting Users*** (on page 76).

Editing or Deleting Roles

Select User Management > Roles to open the Roles page, which lists all defined roles.

If desired, you can sort the list by clicking the desired column header. See ***Sorting a List*** (on page 28).

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

Editing a Role

► **To edit a role:**

1. Select User Management > Roles.

   The Roles page appears and lists all the defined roles.

2. Click the desired role.

   The Edit Role page appears.

3. Make changes as desired.

Note: The role name cannot be changed.

Tip: To delete a role, click 🗑*, and confirm the operation.*

4. Click Save.

Deleting Roles

▶ To delete any roles:

1. Select User Management > Roles.

   The Roles page appears and lists all the defined roles.

2. Click ☑ to make checkboxes appear in front of roles.

Tip: To delete only one role, you can simply click that user without making the checkboxes appear. See the above procedure.

---

3. Select one or multiple roles.
4. To select all roles, except for the Admin role, select the top-most checkbox in the header row.
5. Click 🗑 on the top-right corner.
6. Click Delete on the confirmation message.

Changing Your Password

You must have the Change Own Password permission to change your own password. See ***Creating Roles*** (on page 76).

You must have Administrator Privileges to change other users' passwords. See ***Editing or Deleting Users*** (on page 76).

For more information about changing your password on your first login, see ***Changing Your Password on First Login*** (on page 23).

▶ To change your password via the Change Password command:

1. Select User Management > Change Password.

   The Change Password page appears.

2. First type the current password (listed as ‘old password’), and then the new password twice. Passwords are case sensitive.
3. A password must be within 4 to 64 characters.

Setting Your Preferred Measurement Units in User Preferences

You can change the measurement units shown in the interface according to your own preferences regardless of the permissions you have.

---

*Tip: User Preferences can also be changed by administrators for specific users on the Edit User page. See **Editing or Deleting Users** (on page 76).*

Measurement unit changes only apply to the web interface and command line interface.

Setting your own preferences does not change the default measurement units. See ***Setting Default Measurement Units*** (on page 80).

▶ To select your preferred measurement units in User Preferences:

1. Select User Management > User Preferences.

   The User Preferences page appears.

2. Make changes as desired.

Field	Description
Temperature Unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length Unit	Preferred units for length or height -- Meter or Feet.
Pressure Unit	Preferred units for pressure -- Pascal or Psi. • Pascal = one newton per square meter • Psi = pounds per square inch

3. Click Save.

Setting Default Measurement Units

Default measurement units are applied to all PDU user interfaces across all users, including users accessing the PDU via external authentication servers. For a list of affected user interfaces, see ***User Interfaces Showing Default Units*** (on page 81). The front panel display also shows the default measurement units.

*Note: The preferred measurement units set by any individual user or by the administrator on a per-user basis will override the default units in the web interface and command line interface. See **Setting Your Preferred Measurement Units** (on page 79) or **Creating Users** (on page 72).*

▶ To set up default user preferences:

1. Select User Management > Default Preferences.

   The Default Preferences page appears.

2. Make changes as desired.

Field	Description
Temperature Unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length Unit	Preferred units for length or height -- Meter or Feet.

Field	Description
Pressure Unit	Preferred units for pressure -- Pascal or Psi. • Pascal = one newton per square meter • Psi = pounds per square inch

3. Click Save.

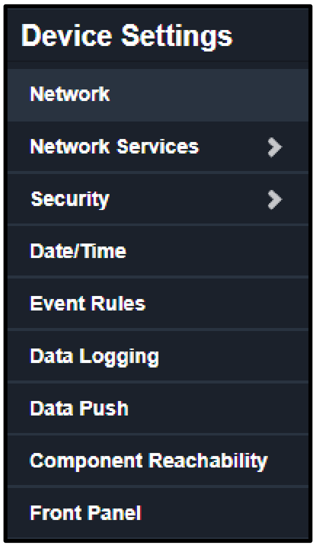
User Interfaces Showing Default Units

Default measurement units will apply to the following user interfaces or information:

- Web interface for "newly created" local users when they have not configured their own preferred measurement units. See *Creating Users* (on page 72).
- The sensor report sent because of the "Send Sensor Report" action. See *Send Sensor Report* (on page 138).
- Front panel display.

Device Settings

Click 'Device Settings' in the *Menu* (on page 27), and the following submenu appears.



Configuring Network Settings

Configure common, ETH1, ETH2, and wireless settings on the Network page after connecting the PDU to your network. For more information, see *Connecting the PDU to Your Network* (on page 20).

You can enable both wired and wireless networking on the PDU so that it has multiple IP addresses -- wired and wireless IP. For example, you can obtain one IPv4 and/or IPv6 address by enabling one Ethernet interface, and obtain one more IPv4 and/or IPv6 address by enabling/configuring the wireless interface. This also applies when the PDU enters port forwarding mode so that the PDU can have more than one IPv4 or IPv6 address while in that mode.

▶ To set up the network settings:

1. Choose Device Settings > Network.
2. The Network page appears. Choose from the following network configuration options:
   - To use DHCP-assigned DNS servers and gateway instead of static ones, see step 3. To manually specify DNS servers and default gateway, configure the Common Network Settings section. See ***Common Network Settings*** (on page 84).
   - To use DHCP-assigned DNS servers and gateway instead of static ones, see step 3. To manually specify DNS servers and default gateway, configure the Common Network Settings section.
   - To configure IPv4/IPv6 settings for a *wired* network, select Wired from the Network Interface drop-down. See ***Wired Network Settings*** (on page 83).
   - To configure IPv4/IPv6 settings for a *wireless* network, select Wireless from the Network Interface drop-down. See ***Wireless Network Settings*** (on page 87).

Note: You must connect a USB wireless LAN adapter to the PDU for wireless networking.

- To configure the ETHERNET interface settings, see Configuring Network Settings (on page 81).

Note: After enabling IPv4 and/or IPv6, all but not limited to the following protocols will be compliant with the selected Internet protocol(s):

- *NTP*
- *SMTP*
- *SSH*
- *Telnet*
- *FTP*
- *SSL/TLS*
- *SNMP*
- *SysLog*

The PDU supports TLS 1.0, 1.1 and 1.2.

Configuring Wired Network Settings

▶ **To configure wired network settings:**

1. Select Device Settings > Network.

   The Network page appears.

2. Select Wired from the Network Interface drop-down to configure IPv4/IPv6 settings.
3. Configure IPv4 or IPv6 settings as follows:

▶ **IPv4 settings:**

Field or Setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP Auto Configuration	Select the method to configure IPv4 settings. • DHCP: Auto-configure IPv4 settings via DHCP servers. • Static: Manually configure the IPv4 settings.

- **DHCP settings:** Optionally specify the preferred hostname, which must meet the following requirements:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols
- **Static settings:** Assign a static IPv4 address, which follows this syntax "IP address/prefix length".

  Example: 192.168.84.99/24

▶ **IPv6 settings:**

Field or Setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP Auto Configuration	Select the method to configure IPv6 settings. • Automatic: Auto-configure IPv6 settings via DHCPv6. • Static: Manually configure the IPv6 settings.

4. **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
5. **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

Example: fd07:2fa:6cff:1111::0/128

Common Network Settings

DNS Settings are OPTIONAL, not required. Therefore, leave them unchanged if there are no specific local networking requirements.

1. Select Device Settings > Network.

   The Network page appears.

2. Click the Common Network Settings title bar as shown.

3. Configure settings as follows:

Field	Description
IP Protocol	Specify from the following protocols: • IPv4 Address: Use the IPv4 addresses. • IPv6 Address: Use the IPv6 addresses. • IPv4 and IPv6: Use both addresses.
DNS Resolver Preference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. • IPv4 Address: Use the IPv4 addresses. • IPv6 Address: Use the IPv6 addresses.
DNS Suffixes (optional)	Specify a DNS suffix name if needed.
First, Second, and Third DNS Server	Manually specify static DNS server(s). • If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. • If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, the PDU will use DHCP-assigned DNS servers.

4. Configure IPv4 Route settings as follows:
   a. In the Default Gateway text box, provide a default gateway address for your IPv4 routes.
   b. Click Add Route.
   c. In the Destination text box, enter a valid destination address.

d. Select Gateway or Interface from the drop-down and provide the following additional information:

- If you select Gateway, enter a gateway address in the adjacent text box.
- If you select Interface, select from BRIDGE, ETH1, ETH2, and WIRELESS options in the adjacent drop-down field.

e. Use the ⬆ and ⬇ buttons to arrange the order of the routes.

f. Click 🗑 to delete a created route.

5. Configure IPv6 Route settings as follows:

a. In the Default Gateway text box, provide a default gateway address for your IPv6 routes.

b. Click Add Route.

c. In the Destination text box, enter a valid destination address.

d. Select Gateway or Interface from the drop-down and provide the following additional information:

- If you select Gateway, enter a gateway address in the adjacent text box.
- If you select Interface, select from BRIDGE, ETH1, ETH2, and WIRELESS options in the adjacent drop-down field.

e. Use the ⬆ and ⬇ buttons to arrange the order of the routes.

f. Click 🗑 to delete a created route.

Ethernet Interface Settings

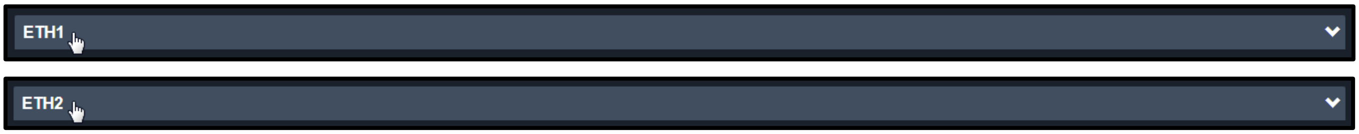
By default the ETH1/ETH2 interfaces for your PDU are enabled.

▶ Ethernet interface settings:

1. Select Device Settings > Network.

   The Network page appears.

2. Click the ETH1 or ETH2 title bar as shown.



Note: ETH1 and ETH2 sections of the Network page have the same configuration settings available for each port. Therefore, they are covered in this single topic for the sake of space.

3. Configure settings as follows:

Field	Description
Speed	Select a LAN speed. • Auto: System determines the optimum LAN speed through auto-negotiation. • 10 MBit/s: Speed is always 10 Mbps. • 100 MBit/s: Speed is always 100 Mbps.
Duplex	Select a duplex mode. • Auto: The PDU selects the optimum transmission mode through auto-negotiation. • Full: Data is transmitted in both directions simultaneously. • Half: Data is transmitted in one direction (to or from the PDU) at a time.
Current State	Show the LAN's current status, including the current speed and duplex mode.

Note: Auto-negotiation is disabled after setting both the speed and duplex settings of the PDU to NON-Auto values, which may result in a duplex mismatch.

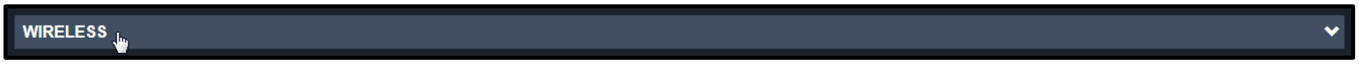
4. Configure IPv4 settings as follows:
   a. Select the Enable IPv4 checkbox to enable the interface. This checkbox is selected by default.
   b. In the IP Auto Configuration drop-down select DHCP or Static and provide the following additional information:
      - If you selected DHCP, enter a Preferred Hostname in the text box provided.
      - DHCP hostnames must meet the following requirements:
        - Consists of alphanumeric characters and/or hyphens
        - Cannot begin or end with a hyphen
        - Cannot contain more than 63 characters
        - Cannot contain punctuation marks, spaces, and other symbols
      - If you selected Static, enter a valid IPv4 address in the text box provided.
      - If you selected Static, enter a corresponding subnet mask or prefix length for your IPv4 address in the text box provided.
        - Subnet Mask Example: 255.255.255.254

          OR
        - Prefix Length Example: /23

5. Configure IPv6 settings as follows:
   a. Select the Enable IPv6 checkbox to enable the interface. This checkbox is selected by default.
   b. In the IP Auto Configuration drop-down select DHCP or Static and provide the following additional information:
      - If you selected DHCP, enter a Preferred Hostname in the text box provided.
      - DHCP hostnames must meet the following requirements:
        - Consists of alphanumeric characters and/or hyphens
        - Cannot begin or end with a hyphen
        - Cannot contain more than 63 characters
        - Cannot contain punctuation marks, spaces, and other symbols
      - If you selected Static, enter a valid IPv6 address with a prefix length in the text box provided. The address follows an “IP address/prefix length” syntax.
        - Example: fd07:2fa:6cff:1111::0/128

Wireless Network Settings

1. Choose Device Settings > Network.
2. Click the WIRELESS title bar as shown.



Note: By default the wireless interface is disabled. You should enable it if wireless networking is desired.

3. Configure as follows:

Interface Settings:

Field or Setting	Description
Hardware State	Look in this display field to ensure that the PDU has detected a wireless USB LAN adapter. If not, verify whether the USB LAN adapter is firmly connected or whether it is supported.
SSID	Type the name of the wireless access point (AP)
Force AP BSSID	If the BSSID is available, select this checkbox
BSSID	Type the MAC address of an access point

Field or Setting	Description
Authentication	Select an authentication method. • No Authentication: No authentication data is required. • PSK: A Pre-Shared Key is required. • EAP - PEAP: Use Protected Extensible Authentication Protocol. Only MSCHAPv2 is supported. Enter required authentication data in the fields that appear.
Pre-Shared Key	This field appears only when PSK is selected. Type the PSK string
Identity	This field appears only when 'EAP - PEAP' is selected. Type your user name.
Password	This field appears only when 'EAP - PEAP' is selected. Type your password.
CA Certificate	This field appears only when 'EAP - PEAP' is selected. A third-party CA certificate may or may not be needed. If needed, follow the steps below.

4. Available settings for the CA Certificate:

Field or Setting	Description
Enable verification of TLS certificate chain	Select this checkbox for the PDU to verify the validity of the TLS certificate that will be installed. • For example, the PDU will check the certificate's validity period against the system time.
Browse…	Click this button to install a certificate file. Then you can: • Click Show to view the certificate's content. • Click Remove to delete the installed certificate if it is inappropriate.

Field or Setting	Description
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period. • After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Allow wireless connection if system clock is incorrect	When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail. When this checkbox is selected, it will make the wireless network connection successful when the PDU system time is earlier than the firmware build before synchronizing with any NTP server. • The incorrect system time issue may occur when the PDU has been powered off for a long time.

5. Configure wireless IPv4 settings as follows:
    a. Select the Enable IPv4 checkbox to enable the interface. This checkbox is selected by default.
    b. In the IP Auto Configuration drop-down select DHCP or Static and provide the following additional information:
        - If you selected DHCP, enter a Preferred Hostname in the text box provided.
        - DHCP hostnames must meet the following requirements:
            - Consists of alphanumeric characters and/or hyphens
            - Cannot begin or end with a hyphen
            - Cannot contain more than 63 characters
            - Cannot contain punctuation marks, spaces, and other symbols
        - If you selected Static, enter a valid IPv4 address with a prefix length in the text box provided. The address follows an “IP address/prefix length” syntax.
            - Example: 192.168.84.99/24
6. Configure wireless IPv6 settings as follows:
    a. Select the Enable IPv6 checkbox to enable the interface. This checkbox is selected by default.
    b. In the IP Auto Configuration drop-down select DHCP or Static and provide the following additional information:
        - If you selected DHCP, enter a Preferred Hostname in the text box provided.
        - DHCP hostnames must meet the following requirements:
            - Consists of alphanumeric characters and/or hyphens

  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

- If you selected Static, enter a valid IPv6 address with a prefix length in the text box provided. The address follows an "IP address/prefix length" syntax.
  - Example: fd07:2fa:6cff:1111::0/128

7. Click Save.

Wireless LAN Diagnostic Log

The PDU provides a diagnostic log for inspecting connection errors that occurred over the wireless network interface. The information is useful for technical support.

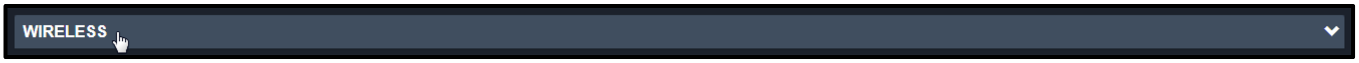
Note that the WLAN Diagnostic Log shows data only after the Network Interface is set to Wireless.

Each entry in the log consists of:

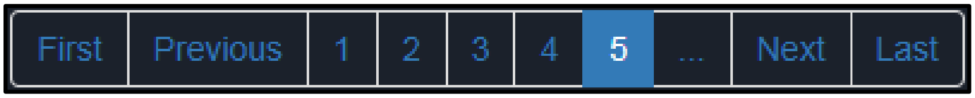
- ID number
- Date and time
- Description

To view the log:

1. Choose Device Settings > Network.
2. Click the WIRELESS title bar as shown.



3. Click Show WLAN Diagnostic Log.
4. To go to other pages of the log, click the pagination bar at the bottom of the page.
5. If there are more than 5 pages and the page numbers displayed in the bar does not show the desired one, click ... to have it show the next or previous five page numbers, if available.



6. To refresh the diagnostic, click Refresh on the top-right corner.
7. If desired, you can sort the list by clicking the desired column header. See *Sorting a List* (on page 28).

8. If desired, you can cliear the diagnostic log by clicking ⋮ > Clear Log in the top-right corner.
9. Click Clear Log in the confirmation message.

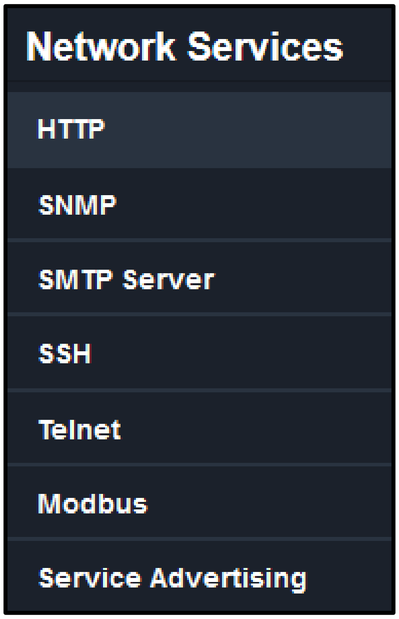
Configuring Network Services

The PDU supports all of the network communication services contained in this portion of the interface.

HTTPS and HTTP enable the access to the web interface. Telnet and SSH enable the access to the command line interface. Refer to ***Using the Command Line Interface*** in the Premium+ PDU With RackLink Avanced User Manual at www.middleatlantic.com.

By default, SSH is enabled, Telnet is disabled, and all TCP ports for supported services are set to standard ports. You can change default settings if necessary.

Note: Telnet access is disabled by default because it communicates openly and is therefore insecure.



Important: The PDU uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as mail services, uses TLS rather than SSL 3.0.

Changing HTTP(S) Settings

HTTPS uses Transport Layer Security (TLS) technology to encrypt all traffic to and from the PDU so it is a more secure protocol than HTTP. The PDU supports TLS *1.0*, *1.1* and *1.2*.

By default, any access to the PDU via HTTP is automatically redirected to HTTPS. You can disable this redirection if needed.

► To change HTTP or HTTPS port settings:

1. Choose Device Settings > Network Services > HTTP.
2. Enable either or both protocols by selecting the corresponding 'Enable' checkbox.
3. To use a different port for HTTP or HTTPS, type a new port number.

Important: Different network services cannot share the same TCP port.

4. To redirect the HTTP access to the PDU to HTTPS, select the "Redirect HTTP connections to HTTPS."
   - The redirection checkbox is configurable only when both HTTP and HTTPS have been enabled.

Special note for AES ciphers:

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

Tip: If intending to force the PDU to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings. For example, you can enable a cipher and disable the other in the Firefox via the "about:config" command.

Configuring SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the PDU. Enabling SNMP communication allows the manager to retrieve and even control the power status of each outlet.

You may need to configure the SNMP destination(s) if the built-in "System SNMP Notification Rule" is enabled and the SNMP destination has not been set yet. See ***Event Rules and Actions*** (on page 120).

► To configure SNMP communication:

1. Choose Device Settings > Network Services > SNMP.
2. Enable or disable "SNMP v1 / v2c" and/or "SNMP v3" by clicking the corresponding checkbox.
   - The SNMP v1/v2c read-only access is enabled by default. The default Read Community String is 'public.'
   - To enable read-write access, type the Write Community String. Usually the string is 'private.'
3. Enter the MIB-II system group information, if applicable.
   - sysContact - the contact person in charge of the system
   - sysName - the name assigned to the system

- sysLocation - the location of the system

4. To configure SNMP notifications:

   c. Select the Enable SNMP Notifications checkbox.

   d. Select a notification type -- SNMPv2c Trap, SNMPv2c Inform, SNMPv3 Trap, and SNMPv3 Inform.

   e. Specify the SNMP notification destinations and enter necessary information. For more information, see:

      - ***SNMPv2c Notifications*** (on page 195).
      - ***SNMPv3 Notifications*** (on page 195).

*Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See **Available Actions** (on page 132). To add more than three SNMP destinations, you can create new SNMP notification actions. See **Send an SNMP Notification** (on page 142).*

5. You must download the SNMP MIB for your PDU to use with your SNMP manager.

   a. Click the Download MIBs title bar to show the download links.

   b. Click the PDU2-MIB download link. See ***Downloading SNMP MIB*** (on page 196).

6. Click Save.

Configuring SMTP Settings

The PDU can be configured to send alerts or event messages to a specific administrator by email. See ***Event Rules and Actions*** (on page 120).

To send emails, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

If any email messages fail to be sent successfully, the failure event and reason are available in the event log. See ***Viewing or Clearing the Local Event Log*** (on page 167).

▶ To set SMTP server settings:

1. Choose Device Settings > Network Services > SMTP Server.
2. Enter the information needed.

Field	Description
IP Address/Host Name	Type the name or IP address of the mail server.

Field	Description
Port	Type the port number. • Default is 25
Sender Email Address	Type an email address for the sender.
Number of Sending Retries	Type the number of email retries. • Default is 2 retries
Time Between Sending Retries	Type the interval between email retries in minutes. • Default is 2 minutes.
Server Requires Authentication	Select this checkbox if your SMTP server requires password authentication.
User Name, Password	Type a user name and password for authentication after selecting the above checkbox. • The length of user name and password ranges between 4 and 64. Case sensitive. • Spaces are not allowed for the user name, but allowed for the password.
Enable SMTP over TLS (StartTLS)	If your SMTP server supports the Transport Layer Security (TLS), select this checkbox.

3. Settings for the CA Certificate:

Field or Setting	Description
	Click this button to install a certificate file. Then you can: • Click Show to view the certificate's content. • Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period. • After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.

4. Now that you have set the SMTP settings, you can test it to ensure it works properly.
   a. Type the recipient's email address in the Recipient Email Addresses field. Use a comma to separate multiple email addresses.
   b. Click Send Test Email.
   c. Check if the recipient(s) receives the email successfully.

5. Click Save.

▶ Regarding AES ciphers:

The PDU's SSL/TLS-based protocols, including SMTP over StartTLS, support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between the PDU and the client (such as a web browser), which is impacted by the cipher priority of the PDU and the client's cipher availability/settings.

Tip: If intending to force the PDU to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Changing SSH Settings

You can enable or disable the SSH access to the command line interface, change the TCP port, or set a password or public key for login over the SSH connection.

▶ To change SSH settings:

1. Choose Device Settings > Network Services > SSH.
2. To enable or disable the SSH access, select or deselect the checkbox.
3. To use a different port, type a port number.
4. Select one of the authentication methods.
   - Password authentication only: Enables the password-based login only.
   - Public key authentication only: Enables the public key-based login only.
   - Password and public key authentication: Enables both the password- and public key-based login. This is the default.
5. Click Save.

If the public key authentication is selected, you must enter a valid SSH public key for each user profile to log in over the SSH connection. See ***Creating Users*** (on page 72).

Changing Telnet Settings

You can enable or disable the Telnet access to the command line interface, or change the TCP port.

▶ To change Telnet settings:

1. Choose Device Settings > Network Services > Telnet.
2. To enable the Telnet access, select the checkbox.
3. To use a different port, type a new port number.

4. Click Save.

Changing Modbus Settings

You can enable or disable the Modbus/TCP access to your PDU, set it to the read-only mode, or change the TCP port.

▶ To change the Modbus/TCP settings:

1. Choose Device Settings > Network Services > Modbus.
2. To enable the Modbus/TCP access, select the "Modbus/TCP Access" checkbox.
3. To use a different port, type a new port number.
4. To enable the Modbus read-only mode, select the checkbox of the "Read-only mode" field. To enable the read-write mode, deselect it.
5. Click Save.

Changing Service Advertising

For more information about service advertising, refer to ***Enabling Service Advertising*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.

▶ To enable or disable service advertising:

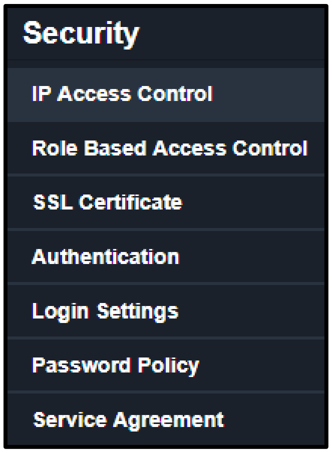
1. Choose Device Settings > Network Services > Service Advertising.
2. To enable the service advertising, select either or both checkboxes.
   - To advertise via MDNS, select the Multicast DNS (MDNS) checkbox.
   - To advertise via LLMNR, select the Link-Local Multicast Name Resolution (LLMNR) checkbox.
3. Click Save.

Configuring Security Settings

The PDU provides tools to control access. You can enable the internal firewall, create firewall rules, and set login limitations. In addition, you can create and install the certificate or set up external authentication servers for access control.

This product supports the SHA-2 certificate.

*Tip: To force all HTTP accesses to the PDU to be redirected to HTTPS, see **Changing HTTP(S) Settings** (on page 91).*



Creating IP Access Control Rules

IP access control rules (firewall rules) determine whether to accept or discard traffic to/from the PDU, based on the IP address of the host sending or receiving the traffic. When creating rules, keep these principles in mind:

- Rule order is important.

  When traffic reaches or is sent from the PDU, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored.

- Subnet mask is required.

  When typing the IP address, you must specify BOTH the address and a subnet mask. For example, to specify a single address in a Class C network, use this format:

  x.x.x.x/24

  where */24* = a subnet mask of 255.255.255.0.

  To specify an entire subnet or range of addresses, change the subnet mask accordingly.

  Note: Valid IPv4 addresses range from 0.0.0.0 through 255.255.255.255.

▶ To configure IPv4 access control rules:

1. Choose Device Settings > Security > IP Access Control.
2. Select the Enable IPv4 Access Control checkbox to enable IPv4 access control rules.
3. Go to the Inbound Rules section or the Outbound Rules section according to your needs.

- Inbound rules control the data sent to the PDU.
- Outbound rules control the data sent from the PDU.

4. Determine the IPv4 default policy.
    - Accept: Accepts traffic from all IPv4 addresses.
    - Drop: Discards traffic from all IPv4 addresses, without sending any failure notification to the source host.
    - Reject: Discards traffic from all IPv4 addresses, and an ICMP message is sent to the source host for failure notification.
5. Create rules. See the tables for different operations.

ADD a rule to the end of the list

- Click Append.
- Type an IP address and subnet mask in the IP/Mask field.
- Select an option in the Policy field.
    - Accept: Accepts traffic from/to the specified IP address(es).
    - Drop: Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
    - Reject: Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

INSERT a rule between two rules

- Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4.
- Click Insert Above.
- Type an IP address and subnet mask in the IP/Mask field.
- Select Accept, Drop or Reject in the Policy field. See the above for their descriptions.

The system automatically numbers the rule.

6. When finished, the rules are listed.
    a. Use the ⬆ and ⬇ buttons to arrange the order of the rules.
    b. Click 🗑 to delete a created rule.
7. Click Save.
8. The rules are applied.

▶ To configure IPv6 access control rules:

1. On the same page, select the Enable IPv6 Access Control checkbox to enable IPv6 access control rules.
2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.
3. Make sure you click the Save button in the IPv6 section, or the changes made to IPv6 rules will not be saved.

Editing or Deleting IP Access Control Rules

When an existing IP access control rule requires updates of IP address range and/or policy, modify them accordingly. Or you can delete any unnecessary rules.

▶ To modify or delete a rule:

1. Choose Device Settings > Security > IP Access Control.
2. Go to the IPv4 or IPv6 section.
3. Select the desired rule in the list.
    - Ensure the IPv4 or IPv6 checkbox has been selected, or you cannot edit or delete any rule.
4. Perform the desired action.
    - Make changes to the selected rule, and then click Save. For information on each field, see ***Creating IP Access Control Rules*** (on page 97).
    - Use the ⬆ and ⬇ buttons to arrange the order of the rules.
    - Click 🗑 to delete a created rule.
5. Click Save.
    - IPv4 rules: Make sure you click the Save button in the IPv4 section, or the changes made to IPv4 rules are not saved.
    - IPv6 rules: Make sure you click the Save button in the IPv6 section, or the changes made to IPv6 rules are not saved.

Creating Role Based Access Control Rules

Role-based access control rules are similar to IP access control rules, except they are applied to members of a specific role. This enables you to grant system permissions to a specific role, based on their IP addresses.

Same as IP access control rules, the order of role-based access control rules is important, since the rules are executed in numerical order.

► To create IPv4 role-based access control rules:

1. Choose Device Settings > Security > Role Access Control.
2. Select the "Enable Role Based Access Control for IPv4" checkbox to enable IPv4 access control rules.
3. Determine the IPv4 default policy.
    - Accept: Accepts traffic from all IPv4 addresses regardless of the user's role.
    - Deny: Drops traffic from all IPv4 addresses regardless of the user's role.
4. Create rules. See the tables for different operations.

ADD a rule to the end of the list

- Click Append.
- Type a starting IP address in the Start IP field.
- Type an ending IP address in the End IP field.
- Select a role in the Role field. This rule applies to members of this role only.
- Select an option in the Policy field.
    - Accept: Accepts traffic from the specified IP address range when the user is a member of the specified role
    - Deny: Drops traffic from the specified IP address range when the user is a member of the specified role

INSERT a rule between two rules

- Select the rule above where you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4.
- Click Insert Above.
- Type a starting IP address in the Start IP field.
- Type an ending IP address in the End IP field.
- Select a role in the Role field. This rule applies to members of this role only.
- Select Allow or Deny in the Policy field. See previous steps for their descriptions.

The system automatically numbers the rule.

5. When finished, the rules are listed on this page.
    a. Use the ⬆ and ⬇ buttons to arrange the order of the rules.
    b. Click 🗑 to delete a created rule.
6. Click Save.

7. The rules are applied.

► To configure IPv6 access control rules:

1. On the same page, select the "Enable Role Based Access Control for IPv6" checkbox to enable IPv6 access control rules.
2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.
3. Make sure you click the Save button in the IPv6 section, or the changes made to IPv6 rules are not saved.

Editing or Deleting Role Access Control Rules

You can modify existing rules to update their roles/IP addresses, or or delete them when they are no longer needed.

► To modify a role-based access control rule:

1. Choose Device Settings > Security > Role Based Access Control.
2. Go to the IPv4 or IPv6 section.
3. Select the desired rule in the list.
   - Ensure the IPv4 or IPv6 checkbox has been selected, or you cannot select any rule.
4. Perform the desired action.
   - Make changes to the selected rule, and then click Save. For information on each field, see *Creating Role Based Access Control* Rules (on page 99).
   - Use the ↑ and ↓ buttons to arrange the order of the rules.
   - Click 🗑 to delete a created rule.
5. Click Save.
   - IPv4 rules: Make sure you click the Save button in the IPv4 section, or the changes made to IPv4 rules are not saved.
   - IPv6 rules: Make sure you click the Save button in the IPv6 section, or the changes made to IPv6 rules are not saved.

Setting Up an SSL/TLS Certificate

Important: The PDU uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as mail services, uses TLS rather than SSL 3.0.

Having an X.509 digital certificate ensures that both parties in an SSL/TLS connection are who they say they are.

To obtain a new CA-signed SSL certificate:

1. Create a Certificate Signing Request (CSR) on the PDU. See ***Creating a New SSL Certificate Signing Request (CSR)*** (on page 102).
2. Submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with a certificate.
3. Install the CA-signed certificate onto the PDU. See ***Uploading a CA-Signed Key*** and Certificate (on page 104).

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

A CSR is not required in either scenario below:

- If you make the PDU create a *self-signed* certificate. See ***Creating a Self-Signed Certificate*** (on page 105).
- If appropriate, valid certificate and key files are already available, and you just need to install them. See ***Installing or Downloading Existing Certificate and Key*** (on page 106).

Creating a New SSL Certificate Signing Request (CSR)

Follow this procedure to create the CSR for your PDU.

Note: You must enter information in the fields showing the message 'required.'

required

To create a new SSL certificate signing request (CSR):

1. Choose Device Settings > Security > SSL Certificate.
2. Provide the information requested.
3. Subject:

Field	Description
Country	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** at http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm.
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.

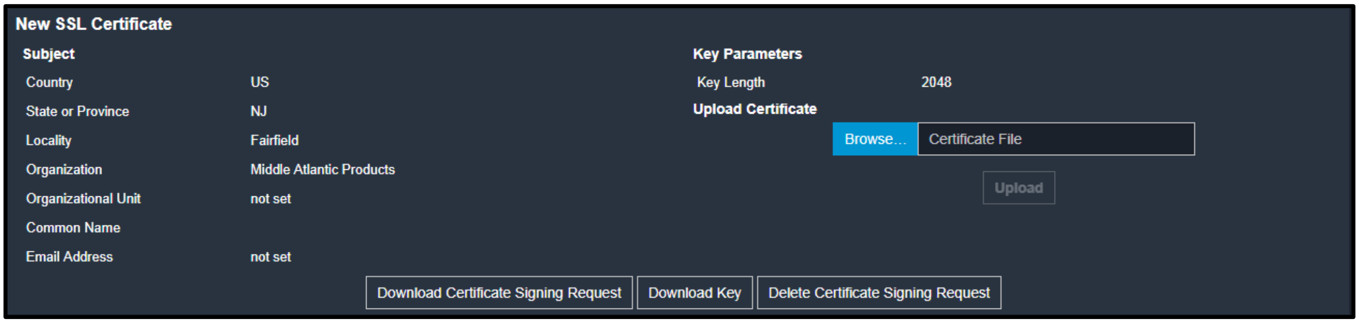
Field	Description
Common Name	The fully qualified domain name (FQDN) of your PDU.
Email Address	An email address where you or another administrative user can be reached.

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

4. In the Subject Alternative Names section, enter the host names or IP addresses for which the certificate will be valid.
    - Click Add Name to include multiple host names or IP addresses for the certificate.
    - Click − to remove a specific host name or IP address for the certificate
5. Key Creation Parameters:

Field	Do this
Key Length	Select an available key length (bits). A larger key length enhances the security, but slows down the PDU's response. • Only 2048 is available now.
Self Sign	**For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.**
Challenge, Confirm Challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional. The value should be 4 to 64 characters long. Case sensitive.

6. Click Create New SSL Key to create both the CSR and private key. This may take several minutes to complete.



New SSL Certificate

Subject

Country	US
State or Province	NJ
Locality	Fairfield
Organization	Middle Atlantic Products
Organizational Unit	not set
Common Name	
Email Address	not set

Key Parameters

Key Length	2048

Upload Certificate

Browse...
Certificate File
Upload
Download Certificate Signing Request
Download Key
Delete Certificate Signing Request

7. Click Download Certificate Signing Request to download the CSR to your computer.
    a. You are prompted to open or save the file. Click Save to save it onto your computer.
    b. Submit it to a CA to obtain the digital certificate.
    c. If the CSR contains incorrect data, click Delete Certificate Signing Request to remove it, and then repeat the above steps to re-create it.

8. To store the newly created private key on your computer, click Download Key in the New SSL Certificate section.

Note: The Download Key button in the Active SSL Certificate section is for downloading the private key of the currently installed certificate rather than the newly created one.

- You are prompted to open or save the file. Click Save to save it onto your computer.

9. After getting the CA-signed certificate, install it. See ***Uploading a CA-Signed Key and Certificate*** (on page 104).

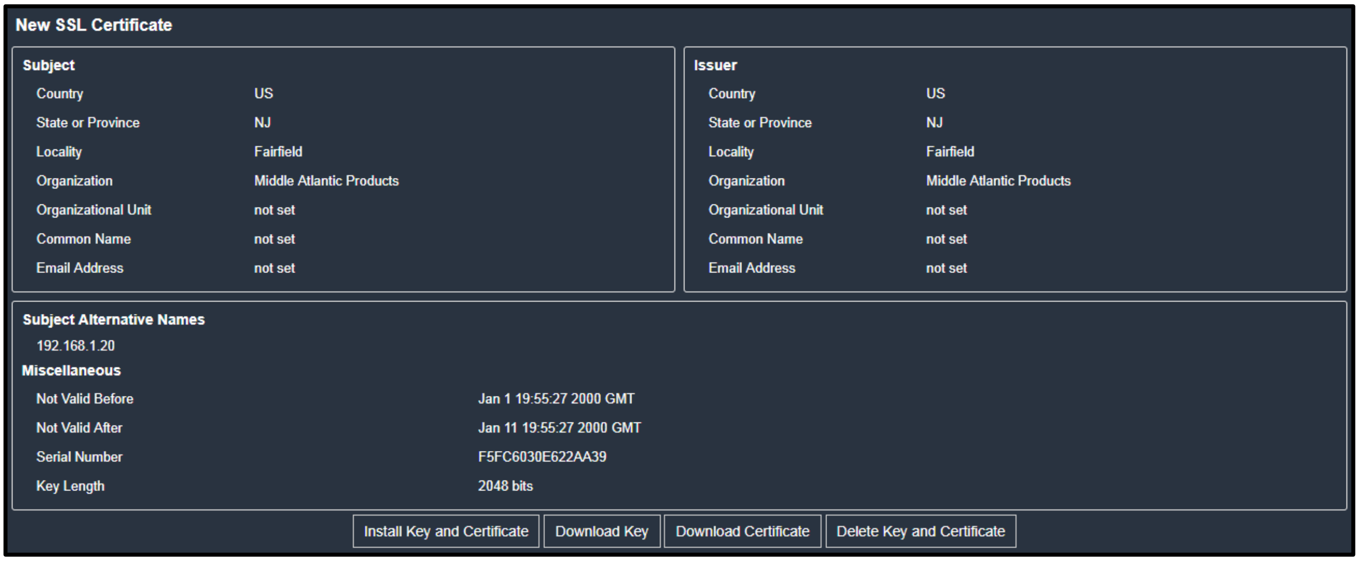
Uploading a CA-Signed Key and Certificate

To get a certificate from a certificate authority (CA), first create a CSR and send it to the CA. See ***Creating a New SSL Certificate Signing Request (CSR)*** (on page 102).

After receiving the CA-signed certificate, install it onto the PDU.

▶ To install the CA-signed certificate:

1. Choose Device Settings > Security > SSL Certificate.
2. Select the Upload Key and Certificate checkbox.
3. Click Browse... to navigate to the Key File.
4. Click Browse... to navigate to the CA-signed Certificate File.
5. Click Upload to install it.
6. To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.



New SSL Certificate

Subject

Country	US
State or Province	NJ
Locality	Fairfield
Organization	Middle Atlantic Products
Organizational Unit	not set
Common Name	not set
Email Address	not set

Issuer

Country	US
State or Province	NJ
Locality	Fairfield
Organization	Middle Atlantic Products
Organizational Unit	not set
Common Name	not set
Email Address	not set

Subject Alternative Names

192.168.1.20

Miscellaneous

Not Valid Before	Jan 1 19:55:27 2000 GMT
Not Valid After	Jan 11 19:55:27 2000 GMT
Serial Number	F5FC6030E622AA39
Key Length	2048 bits

Creating a Self-Signed Certificate

When appropriate certificate and key files for the PDU are unavailable, the alternative, other than submitting a CSR to the CA, is to generate a self-signed certificate.

Note: You must enter information in the fields showing the message 'required.'

required

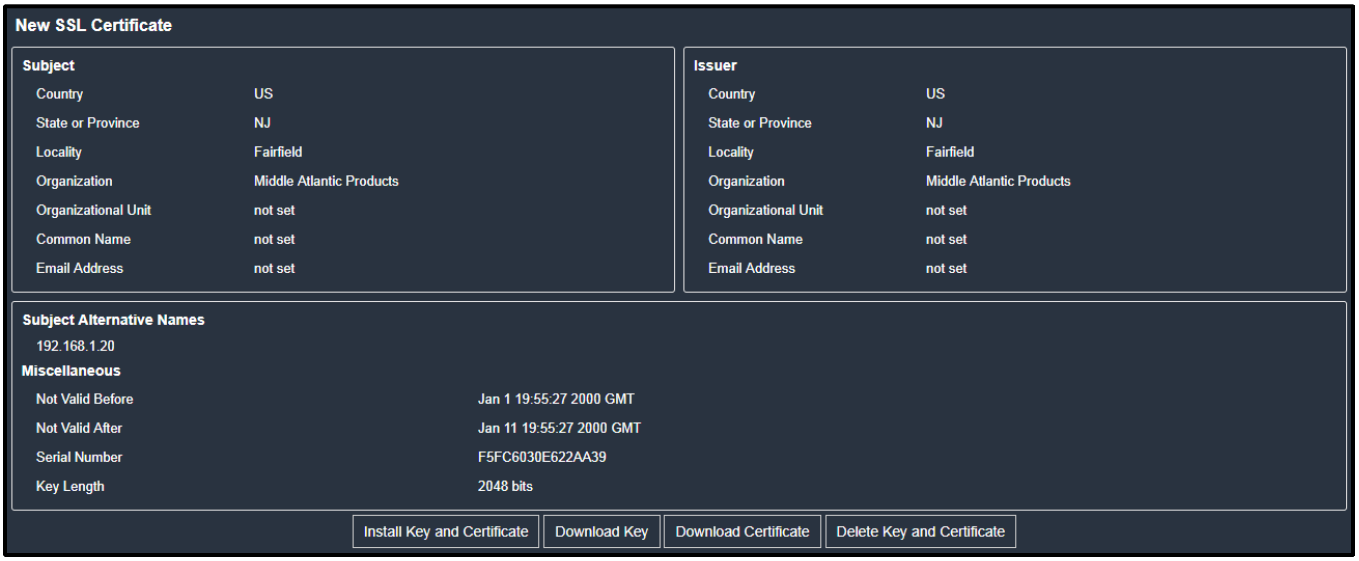
To create and install a self-signed certificate:

1. Choose Device Settings > Security > SSL Certificate.
2. Enter information.

Field	Description
Country	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** at http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm.
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your PDU.
Email Address	An email address where you or another administrative user can be reached.
Key Length	Select an available key length (bits). A larger key length enhances the security, but slows down the PDU's response. • Only 2048 is available now.
Self Sign	**Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.**
Validity in days	This field appears after the Self Sign checkbox is selected. Type the number of days for which the self-signed certificate will be valid.

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

3. Click Create New SSL Key to create both the self-signed certificate and private key. This may take several minutes to complete.



New SSL Certificate

Subject		Issuer	
Country	US	Country	US
State or Province	NJ	State or Province	NJ
Locality	Fairfield	Locality	Fairfield
Organization	Middle Atlantic Products	Organization	Middle Atlantic Products
Organizational Unit	not set	Organizational Unit	not set
Common Name	not set	Common Name	not set
Email Address	not set	Email Address	not set

Subject Alternative Names

192.168.1.20

Miscellaneous

Not Valid Before	Jan 1 19:55:27 2000 GMT
Not Valid After	Jan 11 19:55:27 2000 GMT
Serial Number	F5FC6030E622AA39
Key Length	2048 bits

4. Once complete, do the following:

   a. Double check the data shown in the New SSL Certificate section.

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

Tip: To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.

      - If incorrect, click "Delete Key and Certificate" to remove the self-signed certificate and private key, and then repeat the above steps to re-create them.

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

   - You are prompted to open or save the file. Click Save to save it onto your computer.

Note: The Download Key button in the Active SSL Certificate section is for downloading the private key of the currently installed certificate rather than the newly created one.

Installing or Downloading Existing Certificate and Key

You can download the already-installed certificate and private key from any PDU for backup or file transfer. For example, you can install the files onto a replacement PDU, add the certificate to your browser and so on.

If a valid certificate and private key files are already available, you can install them on the PDU without going through the process of creating a CSR or a self-signed certificate.

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

To download active key and certificate files from the PDU:

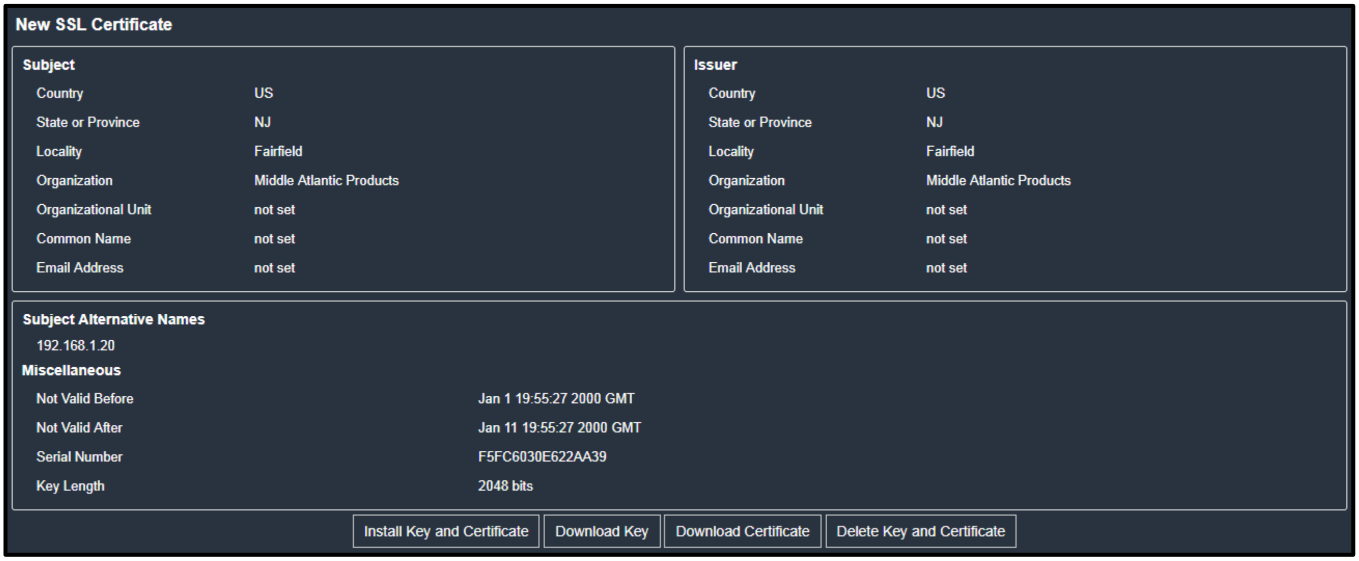
1. Choose Device Settings > Security > SSL Certificate.
2. In the *Active SSL Certificate* section, click Download Key and Download Certificate respectively.

Note: The Download Key button in the New SSL Certificate section, if present, is for downloading the newly created private key rather than the one of the currently installed certificate.

3. You are prompted to open or save the file. Click Save to save it onto your computer.

To install available key and certificate files onto the PDU:

1. Choose Device Settings > Security > SSL Certificate.
2. Select the "Upload Key and Certificate" checkbox at the bottom of the New SSL Certificate section of the page.
3. The Key File and Certificate File fields appear. Click Browse... to select the key and/or certificate file.
4. Click Upload. The selected files are installed.
5. To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.



New SSL Certificate

Subject		Issuer	
Country	US	Country	US
State or Province	NJ	State or Province	NJ
Locality	Fairfield	Locality	Fairfield
Organization	Middle Atlantic Products	Organization	Middle Atlantic Products
Organizational Unit	not set	Organizational Unit	not set
Common Name	not set	Common Name	not set
Email Address	not set	Email Address	not set

Subject Alternative Names

192.168.1.20

Miscellaneous

Not Valid Before	Jan 1 19:55:27 2000 GMT
Not Valid After	Jan 11 19:55:27 2000 GMT
Serial Number	F5FC6030E622AA39
Key Length	2048 bits

Configuring Authentication

Important: The PDU uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

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

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

By default, the PDU is configured for local authentication. If you stay with this method, you only need to create user accounts. See ***Creating Users*** (on page 72).

If you prefer external authentication, you must provide the PDU with information about the external Authentication, Authorization, and Accounting (AAA) server.

If both local and external authentication is needed, create user accounts on the PDU in addition to providing the external AAA server data.

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

If the external authentication fails, an "Authentication failed" message is displayed. Details regarding the authentication failure are available in the event log. See ***Viewing or Clearing the Local Event Log*** (on page 167).

Note that only users who have both the "Change Authentication Settings" and "Change Security Settings" permissions can configure or modify the authentication settings.

▶ To enable external authentication:

1. Collect external AAA server information. See ***Gathering LDAP/Radius Information*** (on page 109).
2. Enter required data for external AAA server(s) on the PDU. See ***Adding LDAP Servers*** (on page 110) or ***Adding RADIUS Servers*** (on page 113).
3. If both the external and local authentication is needed, or you have to return to the local authentication only, see ***Managing External Authentication Settings*** (on page 114).

▶ Special note about the AES cipher:

The PDU's SSL/TLS-based protocols, including LDAPS, support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between the PDU and the client (such as a web browser), which is impacted by the cipher priority of the PDU and the client's cipher availability/settings.

Tip: If intending to force the PDU to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Gathering LDAP/Radius Information

It requires knowledge of your AAA server settings to configure the PDU for external authentication. If you are not familiar with these settings, consult your AAA server administrator for help.

► Information needed for LDAP authentication:

- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over TLS) is being used
  - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- The type of the LDAP server, usually one of the following options:
  - *OpenLDAP*

    If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
  - *Microsoft Active Directory® (AD)*

    If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.
- Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)

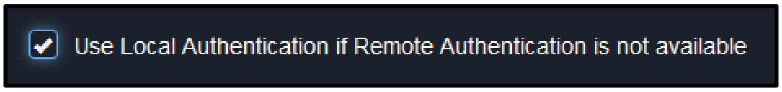
► Information needed for Radius authentication:

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

Configuring Authentication Settings

To configure authentication settings:

1. Choose Device Settings > Security > Authentication.
2. In the Authentication Type drop-down, select one of the following options:
   - Local (selecting Local disables external authentication)
   - LDAP
   - Radius
3. Select the Use Local Authentication if Remote Authentication is not available checkbox if desired.



☑ Use Local Authentication if Remote Authentication is not available

Note: This enables both external and local authentication. When selected, the PDU always tries external authentication first. Whenever the external authentication fails, the PDU then switches to local authentication.

4. Click Save.

Adding LDAP Servers

To add an LDAP server:

1. Choose Device Settings > Security > Authentication.
2. Click New in the LDAP Servers section.
3. Enter information.

Note: You must enter information in the fields showing the message 'required.'

required

Field or Setting	Description
IP Address / Hostname	The IP address or hostname of your LDAP/LDAPS server. • Important: Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.
Copy settings from existing LDAP server	This checkbox appears only when there are existing AAA server settings on the PDU. To duplicate any existing AAA server's settings, refer to the duplicating procedure below.

Field or Setting	Description
Type of LDAP Server	Choose one of the following options: • OpenLDAP • Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
Security	Determine whether you would like to use Transport Layer Security (TLS) encryption, which allows the PDU to communicate securely with the LDAPS server. Three options are available: • StartTLS • TLS • None
Port (None/StartTLS)	The default Port is 389. Either use the standard LDAP TCP port or specify another port.
Port (TLS)	**Configurable only when "TLS" is selected in the Security field.** The default is 636. Either use the default port or specify another one.
Enable verification of LDAP Server Certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the PDU prior to the connection. If the certificate validation fails, the connection is refused.
CA Certificate	• Consult your AAA server administrator to get the CA certificate file for the LDAPS server. • Click Browse... to select and install the certificate file. • Click Show to view the installed certificate's content. • Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	• Select this checkbox to make the authentication succeed regardless of the certificate's validity period. • After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Anonymous Bind	Use this checkbox to enable or disable anonymous bind. • To use anonymous bind, select this checkbox. • When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.

Field or Setting	Description
Bind DN	**Required after deselecting the Anonymous Bind checkbox.** Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base.
Bind Password, Confirm Bind Password	**Required after deselecting the Anonymous Bind checkbox.** Enter the Bind password.
Base DN for Search	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search. • Example: `ou=dev,dc=example,dc=com`
Login Name Attribute	The attribute of the LDAP user class which denotes the login name. • Usually it is the `uid.`
User Entry Object Class	The object class for user entries. • Usually it is `inetOrgPerson`.
User Search Subfilter	Search criteria for finding LDAP user objects within the directory tree.
Active Directory Domain	The name of the Active Directory Domain. • Example: `testradius.com`

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

   *Tip: You can also test the connection on the Authentication page after finishing adding servers. See **Managing External Authentication Settings** (on page 114).*

5. Click Add Server. The new LDAP server is listed on the Authentication page.
6. To add more servers, repeat the same steps.
7. In the Authentication Type field, select LDAP. Otherwise, the LDAP authentication does not work.
8. Click Save. The LDAP authentication is now in place.

Duplicating LDAP Server Settings

If you have added any LDAP/LDAPS server to the PDU, and the server you will add shares identical settings with an existing one, the most convenient way is to duplicate that LDAP/LDAPS server's data and then revise the IP address/host name.

1. Repeat Steps 1 to 2 in the above procedure.
2. Select the "Copy settings from existing LDAP server" checkbox.
3. Click the "Select LDAP Server" field to select the LDAP/LDAPS server whose settings you want to copy.

Note: The Copy settings from existing LDAP server and Select LDAP Server fields only appear after at least one LDAP server is already created.

4. Modify the IP Address/Hostname field.
5. Click Add Server.

Note: If the PDU clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, may be considered expired. To ensure proper synchronization, administrators should configure the PDU and the LDAP server to use the same NTP server(s).

Adding RADIUS Servers

▶ To add a RADIUS server:

1. Choose Device Settings > Security > Authentication.
2. Click New in the Radius section.
3. Enter information.

Note: You must enter information in the fields showing the message 'required.'

Field or Setting	Description
IP Address / Hostname	The IP address or hostname of your Radius server.
Type of RADIUS Authentication	Select an authentication protocol. • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) • MS-CHAPv2 (Microsoft version of the Challenge-Handshake Authentication Protocol) CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear.

Field or Setting	Description
Authentication Port, Accounting Port	The default are standard ports -- 1812 and 1813. To use non-standard ports, type a new port number.
Timeout	This sets the maximum amount of time to establish contact with the Radius server before timing out. Type the timeout period in seconds.
Retries	Type the number of retries.
Shared Secret, Confirm Shared Secret	The shared secret is necessary to protect communication with the Radius server.

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

> *Tip: You can also test the connection on the Authentication page after finishing adding servers. See **Managing External Authentication Settings** (on page 114).*

5. Click Add Server. The new Radius server is listed on the Authentication page.
6. To add more servers, repeat the same steps.
7. In the Authentication Type field, select Radius. Otherwise, the Radius authentication does not work.
8. Click Save. Radius authentication is now in place.

Managing External Authentication Settings

Choose Device Settings > Security > Authentication to open the Authentication page, where you can:

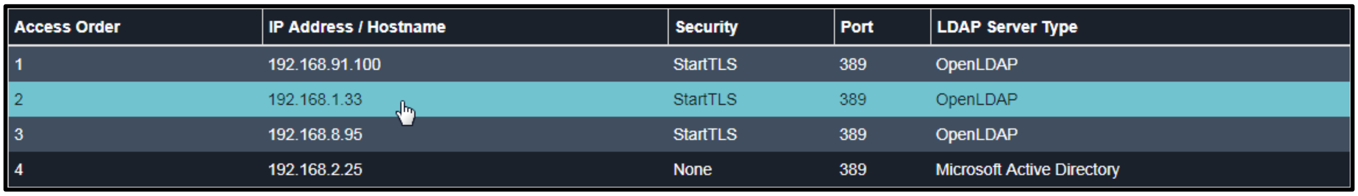
- Enable both the external and local authentication
- Edit or delete a server
- Sort the access order of servers
- Test the connection to a server
- Disable external authentication without removing servers

Testing, Editing, or Deleting a Server, or Sorting a Server List

▶ To test, edit or delete a server, or sort the server list:

1. Choose Device Settings > Security > Authentication.

2. Select a server from either LDAP or RADIUS lists.



Access Order	IP Address / Hostname	Security	Port	LDAP Server Type
1	192.168.91.100	StartTLS	389	OpenLDAP
2	192.168.1.33	StartTLS	389	OpenLDAP
3	192.168.8.95	StartTLS	389	OpenLDAP
4	192.168.2.25	None	389	Microsoft Active Directory

3. Perform the desired action.
   - Click Edit to edit its settings, and click Modify Server to save changes. For information on each field, see ***Adding LDAP Servers*** (on page 110) or ***Adding RADIUS Servers*** (on page 113).
   - Click Delete to delete the server, and then confirm the operation.
   - Click Test Connection to test the connection to the selected server. User credentials may be required.
   - Click ⌃ or ⌄ to change the server order, which determines the access priority, and click Save Order to save the new sequence.

Note: Whenever the PDU is successfully connected to one external authentication server, it STOPS trying to access the remaining servers in the authentication list regardless of the user authentication result.

Configuring Login Settings

Choose Device Settings > Security > Login Settings to open the Login Settings page, where you can:

- Configure the user blocking feature.

Note: The user blocking function applies only to local authentication instead of external authentication through AAA servers.

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

▸ To configure user blocking:

1. Choose Device Settings > Security > Login Settings.
2. To enable the user blocking feature, select the "Block user on login failure" checkbox.
3. In the "Block timeout" field, type a value or click ▲▼ to select a time option. This setting determines how long the user is blocked.
   - If you type a value, the value must be followed by a time unit, such as '4 min.' See ***Time Units*** (on page 188).

4. In the "Maximum number of failed logins" field, type a number. This is the maximum number of login failure the user is permitted before the user is blocked from accessing the PDU.
5. Click Save.

Tip: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command over a local connection. Refer to ***Unblocking a User*** *in the Premium+ PDU With RackLink Advanced User Manual at* ***www.middleatlantic.com****.*

▶ To set limitations for login timeout and use of identical login names:

1. Choose Device Settings > Security > Login Settings.
2. In the "Idle timeout period" field, type a value or click ▲▼ to select a time option. This setting determines how long users are permitted to stay idle before being forced to log out.
   - If you type a value, the value must be followed by a time unit, such as '4 min.' See ***Time Units*** (on page 188).
   - Keep the idle timeout to 20 minutes or less if possible. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to the PDU.
3. Select the "Prevent concurrent login with same username" checkbox if intending to prevent multiple persons from using the same login name simultaneously.
4. Click Save.

Configuring Password Policy

1. Choose Device Settings > Security > Password Policy
2. The Password Policy page appears.
3. Configure the following:
   - Force users to change passwords at a regular interval using the password aging setting.
   - Force users to use strong passwords.

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

Configuring Password Aging

▶ To configure password aging:

1. Choose Device Settings > Security > Password Policy
2. The Password Policy page appears.
3. Select the 'Enabled' checkbox of Password Aging.

4. In the Password Aging Interval field, type a value or click ⬍ to select a time option. This setting determines how often users are requested to change their passwords.
   - If you type a value, the value must be followed by a time unit, such as '10 d.' See *Time Units* (on page 188).
5. Click Save.

Configuring Strong Password Settings

▶ To force users to create strong passwords:

1. Choose Device Settings > Security > Password Policy
2. The Password Policy page appears.
3. Select the 'Enabled' checkbox of Strong Passwords to activate the strong password feature.
4. Configure the following fields from their default settings as desired:

Field	Description
Minimum Password Length	The default is 8 characters. Change the minimum password character length as desired.
Maximum Password Length	The default is 32 characters. Change the maximum password character length as desired. *Note: The maximum password length accepted by the PDU is 64 characters.*
Enforce at least one lower case character	This field is selected by default.
Enforce at least one upper case character	This field is selected by default.
Enforce at least one numeric character	This field is selected by default.
Enforce at least one special character	This field is selected by default.
Password History Size	The default is 5 previous passwords allowed. Change the history size as desired.

5. Click Save.

Enabling the Restricted Service Agreement

The restricted service agreement feature, if enabled, forces users to read a security agreement when they log in to the PDU.

Users must accept the agreement, or they cannot log in.

An event notifying you if a user has accepted or declined the agreement can be generated. See ***Default Log Messages*** (on page 125).

▶ To enable the service agreement:

1. Click Device Settings > Security > Service Agreement.
2. Select the Enforce Restricted Service Agreement checkbox.
3. Edit or paste the content as needed.
    - A maximum of 10,000 characters can be entered.
4. Click Save.

Understanding the Login Manner After Enabling the Service Agreement

▶ Login manner after enabling the service agreement:

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed in the login screen.

Do either of the following, or the login fails:

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."

Tip: To select the agreement checkbox using the keyboard, first press Tab to go to the checkbox and then Enter.

- In the CLI, type y when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Setting the Date and Time

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

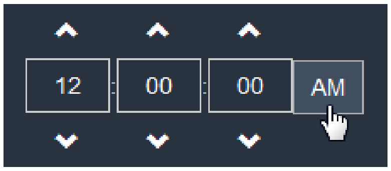
▶ To set the date and time:

1. Choose Device Settings > Date/Time.
2. Click the Time Zone field to select your time zone from the list.
3. If the daylight saving time applies to your time zone, verify the Automatic Daylight Saving Time Adjustment checkbox is selected.
    - If the daylight saving time rules are not available for the selected time zone, the checkbox is not configurable.

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

Customize the date and time

- Select User Specified Time.
- Type values in the Date field using the yyyy-mm-dd format, or click 📅 to select a date.
  - Use arrows to switch between months.
  - Click on a calendar day (0-31) to select the specific day.
  - Click the Today button to select the current date.
  - Click the Clear button to remove any existing date entry in the Date field.
  - Click Close to close the calendar and return to the Date field.
- Type values in the Time field using the hh:mm:ss format, or click ▲ ▼ to adjust values.
  - The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM or PM button.



Use the NTP server

- Select "Synchronize with NTP Server."
- There are two ways to assign the NTP servers:
  - To use the DHCP-assigned NTP servers, DO NOT enter any NTP servers for the First and Second NTP Server.

  DHCP-assigned NTP servers are available only when either IPv4 or IPv6 DHCP is enabled.

  - To use the manually specified NTP servers, specify the primary NTP server in the First Time Server field. A secondary NTP server is optional.

  Click Check NTP Servers to verify the validity and accessibility of the manually specified NTP servers.

5. Click Save.

The PDU follows the NTP server sanity check per the IETF RFC. If your PDU has problems synchronizing with a Windows NTP server, refer to ***Windows NTP Server Synchronization Solution*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.

Event Rules and Actions

A benefit of the product's intelligence is its ability to notify you of or react to a change in conditions. This event notification or reaction is an "event rule."

An event rule consists of two parts:

- Event: This is the situation where the PDU or a device connected to it meets a certain condition. For example, the inlet's voltage reaches the warning level.
- Action: This is the response to the event. For example, the PDU notifies the system administrator of the event via email.

If you want the PDU to perform one action at a regular interval instead of waiting until an event occurs, you can schedule that action. For example, you can make the PDU email the temperature report every hour.

Note that you need the Administrator Privileges to configure event rules.

Creating an Event Rule With an Action

▶ **To create an event rule with an action:**

1. Choose Device Settings > Event Rules.
2. If the needed action is not available yet, create it by clicking **+ New Action**.
   a. Assign a name to this action.
   b. Select the desired action and configure it as needed.
   c. Click Create.

   For details, see ***Available Actions*** (on page 132).
3. Click **+ New Rule** to create a new rule.
   a. Assign a name to this rule.
   b. Make sure the Enabled checkbox is selected, or the new event rule does not work.
   c. In the Event field, select the event to which you want the PDU to react.
   d. In the Available Actions field, select the desired action(s) to respond to the selected event.
   e. Click Create.

   For details, see ***Built-in Rules and Rule Configuration*** (on page 121).

Creating a Scheduled Action

▶ **To create a scheduled action:**

1. If the needed action is not available yet, create it by clicking + New Action. See above.

Note: When creating scheduled actions, available actions are less than usual because it is meaningless to schedule certain actions like "Alarm," "Log event message," "Send email," "Syslog message" and the like.

---

2. Click + New Scheduled Action to schedule the desired action.
   a. Assign a name to this scheduled action.
   b. Make sure the Enabled checkbox is selected, or the PDU does not perform this scheduled action.
   c. Set the interval time, which ranges from every minute to yearly.
   d. In the Available Actions field, select the desired action(s).
   e. Click Create.

   For details, see ***Scheduling an Action*** (on page 148).

Built-in Rules and Rule Configuration

The PDU is shipped with four built-in event rules, which cannot be deleted. If the built-in event rules do not satisfy your needs, you can always create new rules.

▶ **Built-in rules:**

- *System Event Log Rule:*

  This causes ANY event occurred to the PDU to be recorded in the internal log. It is enabled by default.

---

*Note: For the default log messages generated for each event, see **Default Log Messages** (on page 125).*

- *System SNMP Notification Rule:*

  This causes SNMP traps or informs to be sent to specified IP addresses or hosts when ANY event occurs to the PDU. It is disabled by default.

An Event Rule Configuration Example

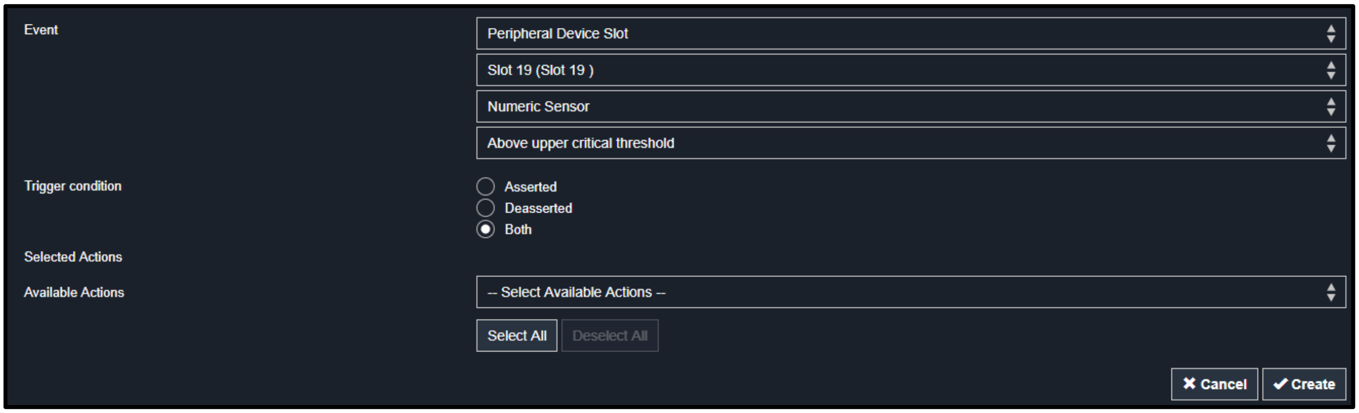
▶ **Event rule configuration example:**

1. Choose Device Settings > Event Rules > + New Rule.
2. Click the Event field to select an event type.
   - <Any sub-event> means all events shown on the list.

- <Any Numeric Sensor> means all numeric sensors of the PDU, including internal and environmental sensors.

  <Any Numeric Sensor> is especially useful if you want to receive the notifications when any numeric sensor's readings pass through a specific threshold.

3. In this example, the Peripheral Device Slot is selected, which is related to the environmental sensor packages. Then a sensor ID field for this event type appears. Click this additional field to specify which sensor should be the subject of this event.
4. In this example, sensor ID 2 (Slot 2) is selected, which is a temperature sensor. Then a new field for this sensor appears. Click this field to specify the type of event(s) you want.
5. In this example, Numeric Sensor is selected because we want to select numeric-sensor-related event(s). Then a field for numeric-sensor-related events appears. Click this field to select one of the numeric-sensor-related events from the list.
6. In this example, 'Above upper critical threshold' is selected because we want the PDU to react only when the selected temperature sensor's reading enters the upper critical range. A "Trigger condition" field appears, requiring you to define the "exact" condition related to the "upper critical" event.



Event: Peripheral Device Slot
Slot 19 (Slot 19)
Numeric Sensor
Above upper critical threshold

Trigger condition: ○ Asserted ○ Deasserted ● Both

Selected Actions

Available Actions: -- Select Available Actions --

7. Select the desired radio button to finish the event configuration. Refer to the following table for different types of radio buttons.
   - If needed, you may refer to event rule examples in the section titled ***Sample Event Rules*** (on page 154).
8. To select any action(s), select them one by one from the Available Actions list.
   - To select all available actions, click Select All.
9. To remove any action(s) from the Selected Actions field, click that action's ✖.
   - To remove all actions, click Deselect All.

Understanding Radio Button Selections for Different Events

► Radio buttons for different events:

According to the event you select, the "Trigger condition" field containing three radio buttons may or may not appear.

Event types	Radio buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	Available radio buttons include "Asserted," "Deasserted" and "Both." • Asserted: The PDU takes the action only when the selected event occurs. That is, the status of the event transits from FALSE to TRUE. • Deasserted: The PDU takes the action only when the selected event disappears or stops. That is, the status of the selected event transits from TRUE to FALSE. • Both: The PDU takes the action both when the event occurs (asserts) and when the event stops/disappears (deasserts).
State sensor state change	Available radio buttons include "Alarmed/Open/On," "No longer alarmed/Closed/Off" and "Both." • Alarmed/Open/On: The PDU takes the action only when the chosen sensor enters the alarmed, open or on state. • No longer alarmed/Closed/Off: The PDU takes the action only when the chosen sensor returns to the normal, closed, or off state. • Both: The PDU takes the action whenever the chosen sensor switches its state.
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." • Unavailable: The PDU takes the action only when the chosen sensor is NOT detected and becomes unavailable. • Available: The PDU takes the action only when the chosen sensor is detected and becomes available. • Both: The PDU takes the action both when the chosen sensor becomes unavailable or available.
Network interface link state	• Link state is up: The PDU takes the action only when the network link state changes from down to up. • Link state is down: The PDU takes the action only when the network link state changes from up to down. • Both: The PDU takes the action whenever the network link state changes.

Event types	Radio buttons
Function enabled or disabled	• Enabled: The PDU takes the action only when the chosen function is enabled. • Disabled: The PDU takes the action only when the chosen function is disabled. • Both: The PDU takes the action when the chosen function is either enabled or disabled.
Restricted service agreement	• Accepted: The PDU takes the action only when the specified user accepts the restricted service agreement. • Declined: The PDU takes the action only when the specified user rejects the restricted service agreement. • Both: The PDU takes the action both when the specified user accepts or rejects the restricted service agreement.
Component monitoring event	• Monitoring started: The PDU takes the action only when the monitoring of any specified component starts. • Monitoring stopped: The PDU takes the action only when the monitoring of any specified component stops. • Both: The PDU takes the action when the monitoring of any specified component starts or stops.
Component reachability	• Unreachable: The PDU takes the action only when any specified component becomes inaccessible. • Reachable: The PDU takes the action only when any specified component becomes accessible. • Both: The PDU takes the action when any specified component becomes either inaccessible or accessible.
+12V Supply 1 Status	Available radio buttons include "Fault," "Ok" and "Both." • Fault: The PDU takes the action only when the selected 12V power supply to the controller enters the fault state. • Ok: The PDU takes the action only when when the selected 12V power supply to the controller enters the OK state. • Both: The PDU takes the action whenever the selected 12 power supply's status changes.

Default Log Messages

Following are default log messages recorded internally and emailed to specified recipients when PDU events occur (are TRUE) or, in some cases, stop or become unavailable (are FALSE). See ***Send Email*** (on page 137) for information configuring email messages to be sent when specified events occur.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Device > System started	System started.	
Device > System reset	System reset performed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware validation failed	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update started	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update completed	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update failed	Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Hardware failure present	Failure '[FAILURETYPESTR]' asserted for component '[COMPONENTID]'.	Failure '[FAILURETYPESTR]' deasserted for component '[COMPONENTID]'.
Device > Device identification changed	Config parameter '[PARAMETER]' changed to '[VALUE]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device settings saved	Device settings saved from host '[USERIP]'	
Device > Device settings restored	Device settings restored from host '[USERIP]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Device > Data push failed	Data push to URL [DATAPUSH_URL] failed. [ERRORDESC].	
Device > Event log cleared	Event log cleared by user '[USERNAME]' from host '[USERIP]'.	
Device > Bulk configuration saved	Bulk configuration saved from host '[USERIP]'.	
Device > Bulk configuration copied	Bulk configuration copied from host '[USERIP]'.	
Device > Network interface link state is up	The [IFNAME] network interface link is now up.	The [IFNAME] network interface link is now down.
Device > Peripheral Device Firmware Update	Firmware update for peripheral device [EXTSENSORSERIAL] from [OLDVERSION] to [VERSION] [SENSORSTATENAME].	
Device > Sending SMTP message failed	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed.	
Device > Sending SNMP inform failed or no response	Sending SNMP inform to manager [SNMPMANAGER]:[SNMPMANAGERPORT] failed or no response. [ERRORDESC].	
Device > Sending Syslog message failed	Sending Syslog message to server [SYSLOGSERVER]:[SYSLOGPORT] ([SYSLOGTRANSPORTPROTO]) failed. [ERRORDESC].	
Device > Sending SMS message failed	Sending SMS message to '[PHONENUMBER]' failed.	
Device > Unknown peripheral device attached	An unknown peripheral device with rom code '[ROMCODE]' was attached at position '[PERIPHDEVPOSITION]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Device > USB slave connected	USB slave connected.	USB slave disconnected.
Device > WLAN authentication over TLS with incorrect system clock	Established connection to wireless network '[SSID]' via Access Point with BSSID '[BSSID]' using '[AUTHPROTO]' authentication with incorrrect system clock.	
Peripheral Device Slot > * > Numeric Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > Numeric Sensor > Above upper critical threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Above upper warning threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Below lower warning threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Below lower critical threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower critical' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical' at [READING].
Peripheral Device Slot > * > State Sensor/Dry Contact > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Peripheral Device Slot > * > State Sensor/Dry Contact > Alarmed/Open/On	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].
Inlet > * > Enabled	Inlet '[INLET]' has been enabled by user '[USERNAME]' from host '[USERIP]'.	Inlet '[INLET]' has been disabled by user '[USERNAME]' from host '[USERIP]'.
Inlet > * > Sensor > * > Unavailable	Sensor '[INLETSENSOR]' on inlet '[INLET]' unavailable.	Sensor '[INLETSENSOR]' on inlet '[INLET]' available.
Inlet > * > Sensor > * > Above upper critical threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper critical'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper critical'.
Inlet > * > Sensor > * > Above upper warning threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper warning'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper warning'.
Inlet > * > Sensor > * > Below lower warning threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower warning'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower warning'.
Inlet > * > Sensor > * > Below lower critical threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower critical'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower critical'.
Inlet > * > Sensor > Active Energy > Reset	Sensor '[INLETSENSOR]' on inlet '[INLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Power control > Powered on	Outlet '[OUTLET]' has been powered on by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Power control > Powered off	Outlet '[OUTLET]' has been powered off by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Power control > Power cycled	Outlet '[OUTLET]' power cycle initiated by user '[USERNAME]' from host '[USERIP]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Outlet > * > Sensor > * > Unavailable	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' unavailable.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' available.
Outlet > * > Sensor > * > Above upper critical threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper critical'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper critical'.
Outlet > * > Sensor > * > Above upper warning threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper warning'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper warning'.
Outlet > * > Sensor > * > Below lower warning threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'below lower warning'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'below lower warning'.
Outlet > * > Sensor > * > Below lower critical threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'below lower critical'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'below lower critical'.
Outlet > * > Sensor > Active Energy > Reset	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' has been reset by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Sensor > Outlet State > On	Outlet '[OUTLET]' state changed to on.	Outlet '[OUTLET]' state changed to off.
Outlet > * > Pole > * > Sensor > Unavailable	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' unavailable.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' available.
Outlet > * > Pole > * > Sensor > Above upper critical threshold	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'above upper critical'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'above upper critical'.
Outlet > * > Pole > * > Sensor > Above upper warning threshold	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'above upper warning'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'above upper warning'.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Outlet > * > Pole > * > Sensor > Below lower warning threshold	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower warning'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below lower warning'.
Outlet > * > Pole > * > Sensor > Below lower critical threshold	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower critical'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below lower critical'.
PDU > Load Shedding > Started	PX placed in Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.	PX removed from Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.
PDU > Sensor > +12V Supply 1 Status > fault	Global sensor 'powerSupplyStatus1' entered fault state.	PDU > Sensor > +12V Supply 1 Status > fault
PDU > Sensor > +12V Supply 1 Status > Unavailable	Global sensor 'powerSupplyStatus1' unavailable.	Global sensor 'powerSupplyStatus1' available.
Component Monitoring > * > Error	Error monitoring component '[MONITOREDHOST]': [ERRORDESC]	
Component Monitoring > * > Monitored	Component '[COMPONENT]' is now being monitored.	Component '[COMPONENT]' is no longer being monitored.
Component Monitoring > * > Unreachable	Component '[COMPONENT]' is unreachable.	Component '[COMPONENT]' is reachable.
Component Monitoring > * > Unrecoverable	Connection to component '[MONITOREDHOST]' could not be restored.	
User Activity > * > User logon state	User '[USERNAME]' from host '[USERIP]' logged in.	User '[USERNAME]' from host '[USERIP]' logged out.
User Activity > * > Authentication failure	Authentication failed for user '[USERNAME]' from host '[USERIP]'.	
User Activity > * > User accepted the Restricted Service Agreement	User '[USERNAME]' from host '[USERIP]" accepted the Restricted Service Agreement.	User '[USERNAME]' from host '[USERIP]" declined the Restricted Service Agreement.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
User Activity > * > User blocked	User '[USERNAME]' from host '[USERIP]' was blocked.	
User Activity > * > Session timeout	Session of user '[USERNAME]' from host '[USERIP]' timed out.	
User Administration > User added	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User modified	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User deleted	User '[TARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password changed	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password settings changed	Password settings changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role added	Role '[TARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role modified	Role '[TARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role deleted	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.	
Surge Event > Surge Occurred	Surge protection status: [SURGESTATUS]	
Timer Event > Timer Event Occurred	Timer event '[EVENTRULENAME]' occurred.	

The asterisk symbol (*) represents anything you select for the 'trigger' events.

Available Actions

The PDU comes with four built-in actions, which cannot be deleted. You can create additional actions for responding to different events.

Built-in actions:

- *System Event Log Action:*

  This action records the selected event in the internal log when the event occurs.

- *System SNMP Notification Action:*

  This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.

  Note: No IP addresses are specified for this notification action by default so you must enter IP addresses before applying this action to any event rule. See ***Editing or Deleting a Rule/Action*** *(on page 153). Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See* ***Configuring SNMP Settings*** *(on page 92).*

Actions you can create:

1. Choose Device Settings > Event Rules > + New Action.
2. Click the Action field to select an action type from the list.
3. Below is the list of available actions.

Note: The "Change load shedding state" and "Switch outlets" options are only available for outlet-switching capable models.

Action	Function
Alarm	Requires the user to acknowledge the alert after it is generated. If needed, you can have the alert notifications regularly generated until a person takes the acknowledgment action. See ***Alarm*** (on page 133).
Change load shedding state	Enters or quits the load shedding mode. See ***Change Load Shedding State*** (on page 135).
Execute an action group	Creates a group of actions comprising existing actions. See ***Executing an*** Action Group (on page 135).
Log event message	Records the selected events in the internal log. See ***Log an Event Message*** (on page 136).

Action	Function
Push out sensor readings	Sends internal sensor log, environmental sensor log or asset management strip data to a remote server using HTTP POST requests. See ***Push Out Sensor Readings*** (on page 136).
Send email	Emails a textual message. See ***Send Email*** (on page 137).
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See ***Send Sensor Report*** (on page 138).
Send SMS message	Sends a message to a mobile phone. See ***Send SMS Message*** (on page 141).
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See ***Send an SNMP Notification*** (on page 142).
Switch outlets	Switches on, off or cycles the power to the specified outlet(s). See ***Switch Outlets*** (on page 144).
Switch peripheral dry contact	Switches on or off the mechanism or system connected to the specified dry contact. See ***Switch Peripheral*** (on page 145).
Syslog message	Makes the PDU automatically forward event messages to the specified syslog server. See ***Syslog Message*** (on page 146).

4. Enter the information as needed and click Create.
5. Then you can assign the newly created action to an event rule or schedule it. See ***Event Rules and Actions*** (on page 120).

Alarm

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

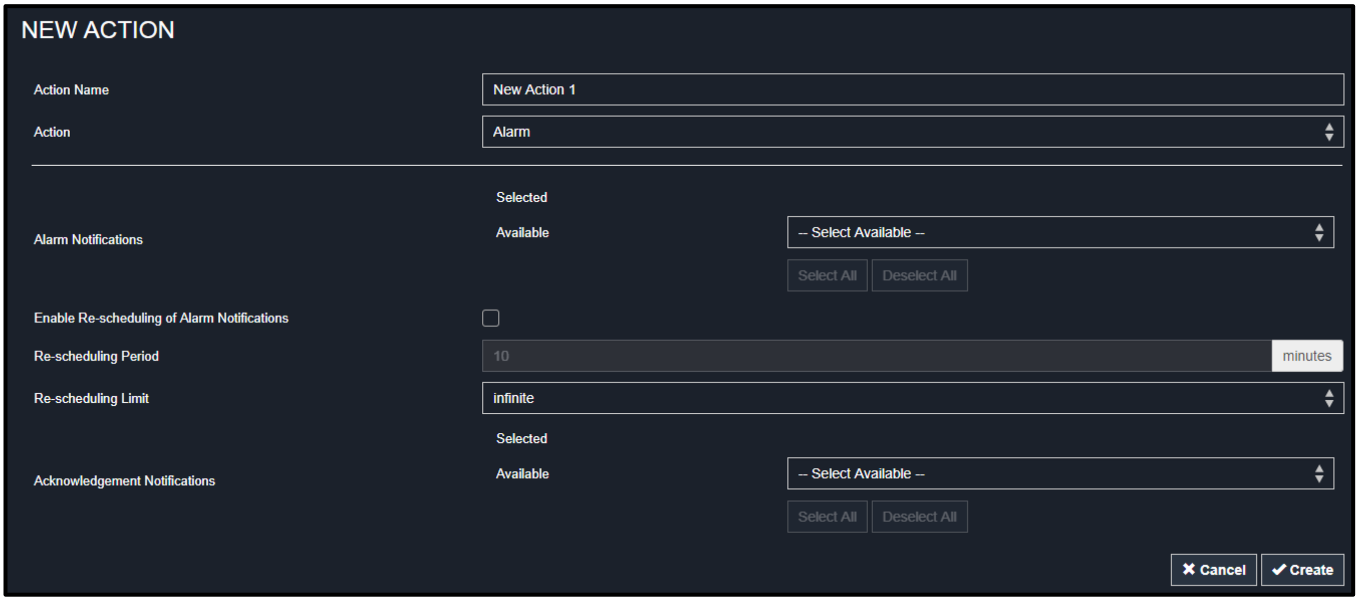
If the Alarm action has been included in a specific event rule and no one acknowledges that alert after it occurs, the PDU resends or regenerates an alert notification regularly until the alert is acknowledged or the maximum number of alert notifications is sent.

For information on acknowledging an alert, see ***Dashboard*** (on page 29).

▶ To create an alarm action:

1. Choose Device Settings > Event Rules > .

2. Select Alarm from the Action list.



NEW ACTION

Action Name	New Action 1
Action	Alarm
Alarm Notifications	Selected Available: -- Select Available --
Enable Re-scheduling of Alarm Notifications	□
Re-scheduling Period	10 minutes
Re-scheduling Limit	infinite
Acknowledgement Notifications	Selected Available: -- Select Available --

3. In the Alarm Notifications list box, specify one or multiple ways to issue the alert notifications. Available methods vary, depending on how many notification-based actions have been created. Notification-based action types include:

   - Syslog message
   - Send email
   - Send SMS message

   If no appropriate actions are available, create them first.

   a. To select any methods, select them one by one in the Available field.

      To add all available methods, simply click Select All.

   b. To delete any methods, click a method's ✖ in the Selected field.

      To remove all methods, simply click Deselect All.

4. To enable the notification-resending feature, select the "Enable Re-scheduling of Alarm Notifications" checkbox.
5. In the "Re-scheduling Period" field, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly.
6. In the "Re-scheduling Limit" field, specify the maximum number of times the alert notification is resent. Values range from 1 to infinite.
7. **(Optional)** You can instruct the PDU to send the acknowledgment notification after the alarm is acknowledged in the Acknowledgment Notifications field. Available methods are identical to those for generating alarm notifications.

   a. In the Available field, select desired methods one by one, or click Select All. See step 3 for details.

b. In the Selected field, click any method's ✖ to remove unnecessary ones, or click Deselect All.

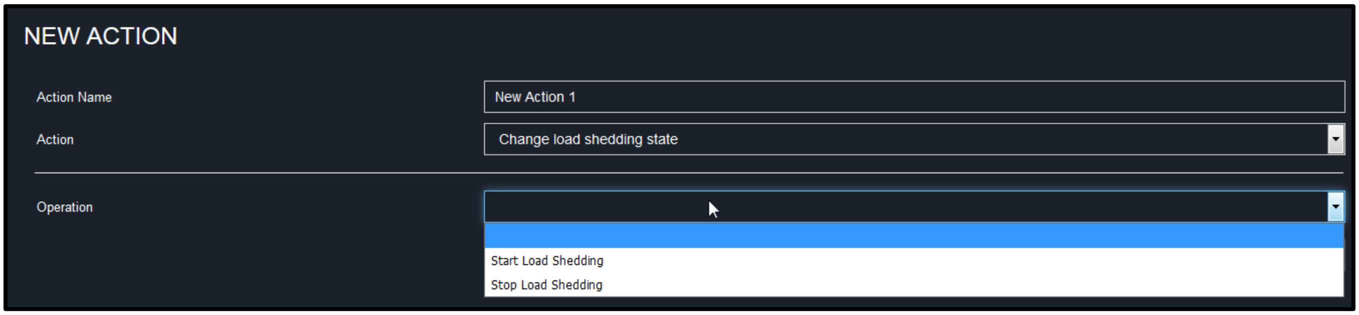
8. Click Create.

Change Load Shedding State

The "Change load shedding state" action is available only when your PDU is able to control outlet power. Use this action to activate or deactivate the load shedding mode for responding to a specific event. For additional informtion, see ***Load Shedding Mode*** (on page 37).

▶ To create a change load shedding state action:

1. Choose Device Settings > Event Rules > + New Action.
2. Select "Change load shedding state" from the Action list.



NEW ACTION

Action Name: New Action 1

Action: Change load shedding state

Operation:

3. In the Operation field, select either one below:
   - Start Load Shedding: Enters the load shedding mode when the specified event occurs.
   - Stop Load Shedding: Quits the load shedding mode when the specified event occurs.
4. Click Create.

Executing an Action Group

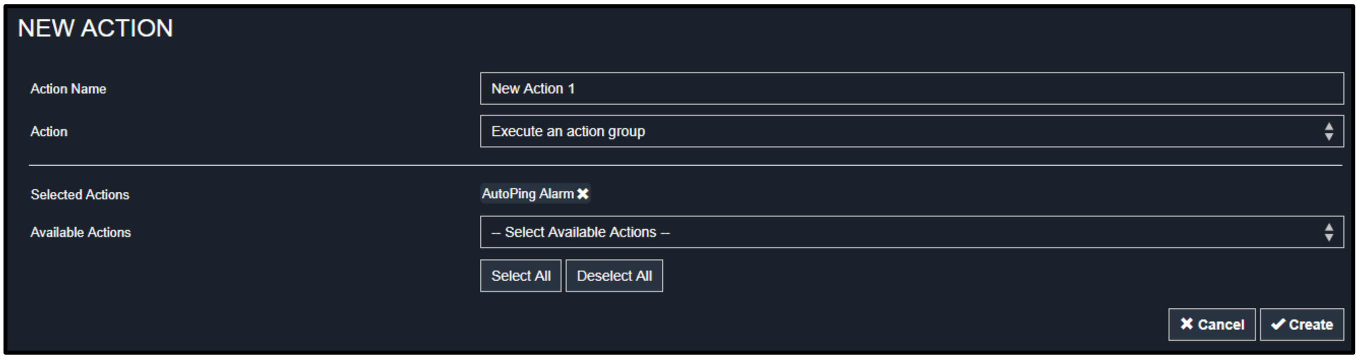
You can create an action group that performs up to 32 actions. After creating such an action group, you can easily assign this set of actions to any event rule rather than selecting all needed actions one by one per rule.

If the needed action is not available yet, create it first. See ***Available Actions*** (on page 132).

▶ To execute an action group:

1. Choose Device Settings > Event Rules > + New Action.

2. Select "Execute an action group" from the Action list.



NEW ACTION

Action Name: New Action 1

Action: Execute an action group

Selected Actions: AutoPing Alarm ✖

Available Actions: -- Select Available Actions --

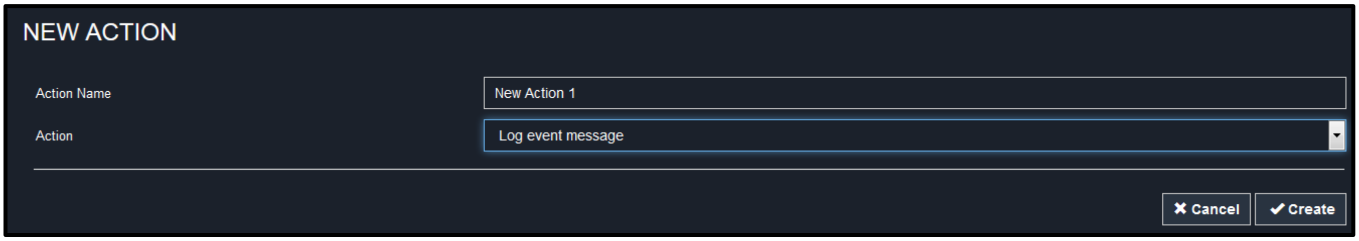
3. To select any action(s), select them one by one from the Available Actions list.
    - To select all available actions, click Select All.
4. To remove any action(s) from the Selected Actions field, click that action's ✖.
    - To remove all actions, click Deselect All.
5. Click Create.

Log an Event Message

▶ To create a log event message action:

1. Choose Device Settings > Event Rules > + New Action.
2. Select "Log event message" from the Action list.

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



NEW ACTION

Action Name: New Action 1

Action: Log event message

The default log message generated for each type of event is available in the section titled ***Default Log Messages*** (on page 125).

3. Click Create.

Push Out Sensor Readings

You can configure the PDU to push sensor log to a remote server after a certain event occurs, including logs of internal sensors, environmental sensors and dry contacts.

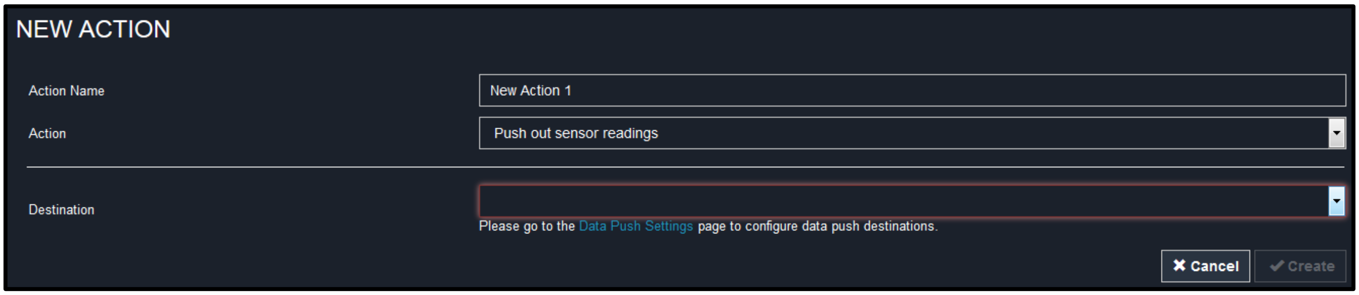
Before creating this action, make sure that you have properly defined the destination servers and the data to be sent on the Data Push page. See ***Configuring Data Push Settings*** (on page 158).

---

*Tip: To send the data at a regular interval, schedule this action. See **Scheduling an Action** (on page 148).*

▶ To create a push out sensor reading action:

1. Choose Device Settings > Event Rules > **+ New Action**.
2. Select "Push out sensor readings" from the Action list.



NEW ACTION

Action Name: New Action 1

Action: Push out sensor readings

Destination:

Please go to the Data Push Settings page to configure data push destinations.

3. Select a server or host which receives the sensor log in the Destination field.
   - If the desired destination is not available yet, see the Data Push page to specify it. See ***Configuring Data Push Settings*** (on page 158).
4. Click Create.

Send Email

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

Messages consist of a combination of free text and PDU placeholders. The placeholders represent information is pulled from the PDU and inserted into the message.

For example:

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

translates to

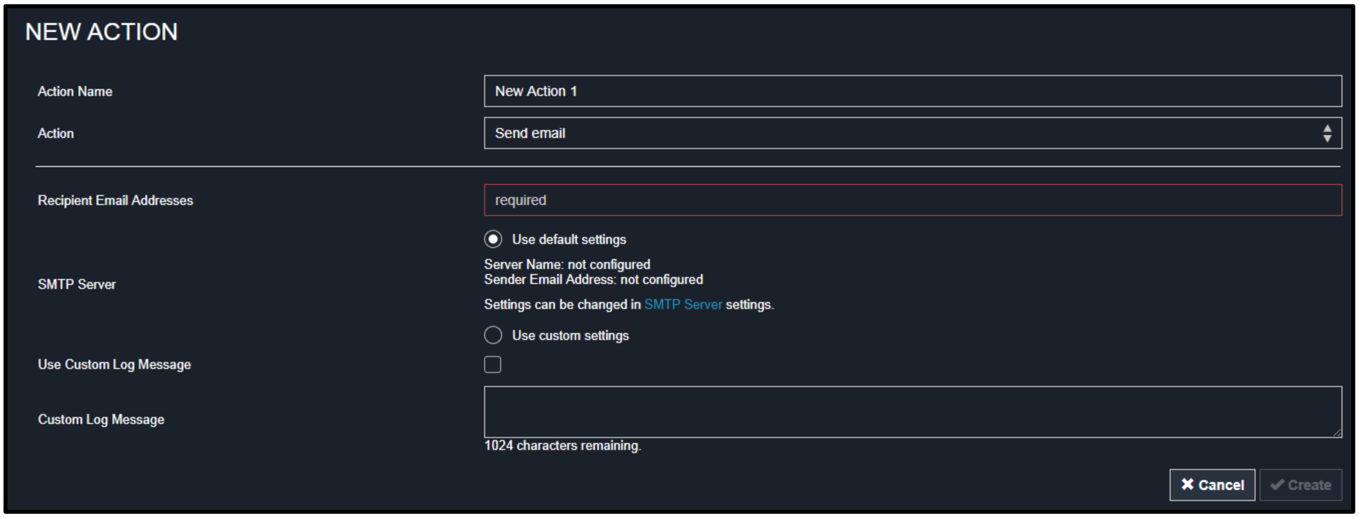
```
JQPublic logged into the device on 2012-January-30 21:00
```

For a list and definition of available variables, see ***Email and SMS Message Placeholders*** (on page 150).

▶ To create a send email action:

1. Choose Device Settings > Event Rules > **+ New Action**.

2. Select "Send email" from the Action list.



NEW ACTION

Action Name: New Action 1

Action: Send email

Recipient Email Addresses: required

SMTP Server:
● Use default settings
Server Name: not configured
Sender Email Address: not configured
Settings can be changed in SMTP Server settings.
○ Use custom settings

Use Custom Log Message □

Custom Log Message:
1024 characters remaining.

3. In the "Recipient Email Addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
4. To use the SMTP server specified on the SMTP Server page, make sure the "Use custom SMTP Server" radio button is NOT selected.

   To use a different SMTP server, select this radio button. The fields for customized SMTP settings appear. For information on each field, see ***Configuring SMTP Settings*** (on page 93).

   Default messages are sent based on the event. For a list of default log messages and events that trigger them, see ***Default Log Messages*** (on page 125).
5. If needed, select the Use Custom Log Message checkbox, and then create a custom message up to 1024 characters in the provided field.
6. When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just click the desired placeholder. For details, see ***Email and SMS Message Placeholders*** (on page 150).
7. To start a new line in the text box, press Enter.
8. If needed, you can resize the text box by dragging the bottom-right corner.
9. Click Create.

Send Sensor Report

You may set the PDU so that it automatically reports the latest readings or states of one or multiple sensors by sending a message or email or simply recording the report in a log. These sensors can be either internal or environmental sensors as listed below.

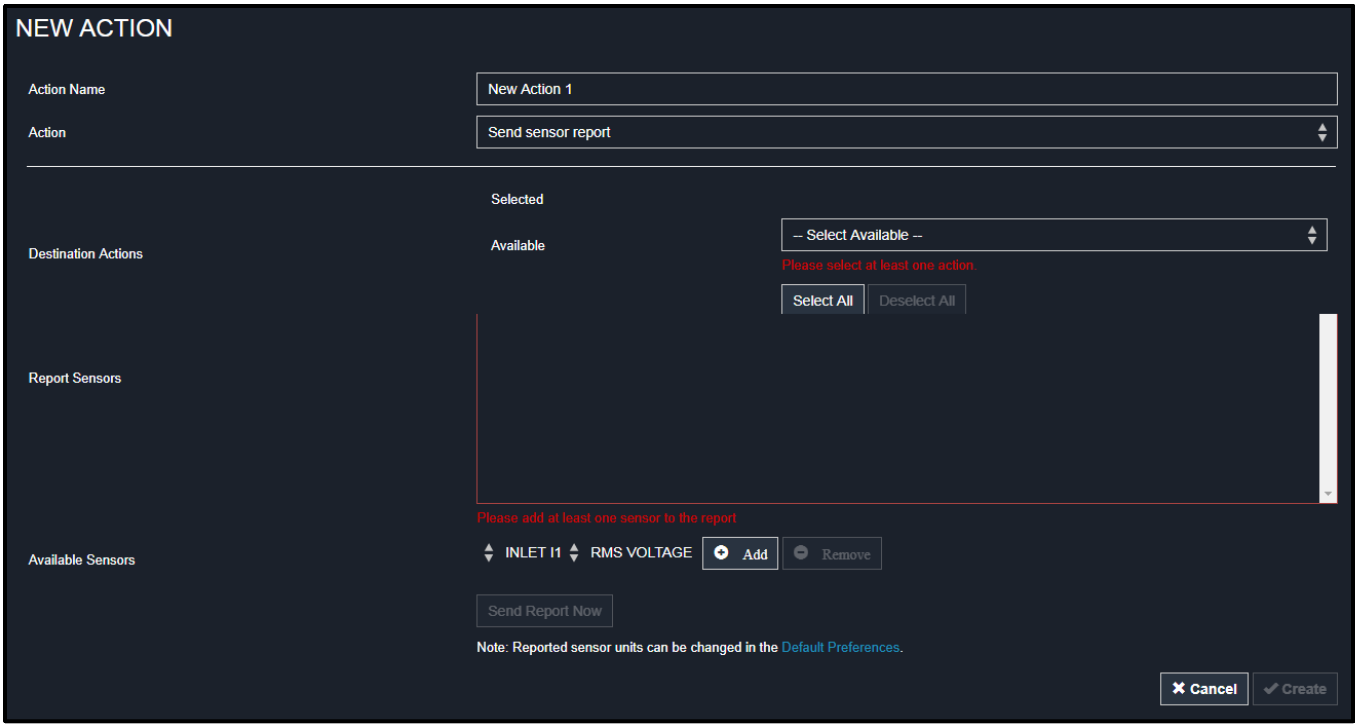
- Inlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor and active energy.

- Outlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor, active energy and outlet state (for outlet-switching capable PDUs only).
- Overcurrent protector sensors, including RMS current and tripping state.
- Peripheral device sensors, which can be any environmental sensor packages connected to the PDU, such as temperature or humidity sensors.

An example of this action is available in the section titled ***Send Sensor Report Example*** (on page 149).

▶ To create a send sensor report action:

1. Choose Device Settings > Event Rules > + New Action.
2. Select "Send sensor report" from the Action list.



NEW ACTION

Action Name: New Action 1

Action: Send sensor report

Destination Actions: Selected / Available: -- Select Available --

Please select at least one action.

Report Sensors

Please add at least one sensor to the report

Available Sensors: INLET I1 RMS VOLTAGE

Note: Reported sensor units can be changed in the Default Preferences.

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

   The messaging action types include:

4. Log event message
5. Syslog message
6. Send email
7. Send SMS message

a. If no messaging actions are available, create them now. See ***Available Actions*** (on page 132).

b. To select any methods, select them one by one in the Available field.

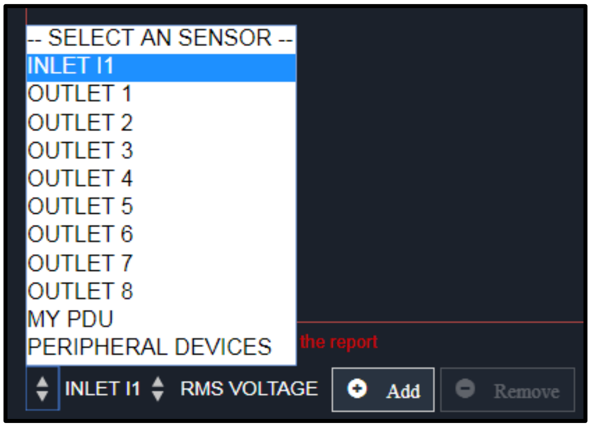
To add all available methods, simply click Select All.

c. To delete any methods, click a method's ✖ in the Selected field.

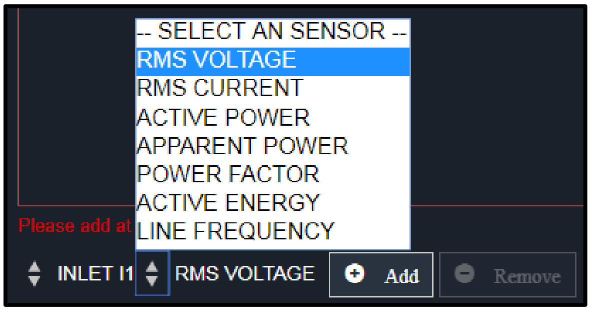
To remove all methods, simply click Deselect All.

8. In the Available Sensors field, select the desired target's sensor.

a. Click the first ⬍ to select a target sensor from the list.



b. Click the second ⬍ to select the specific sensor for the target from the list.



c. Click ⊕ Add to add the selected sensor to the Report Sensors list box.

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

9. To report additional sensors simultaneously, repeat the above step to add more sensors.

10. To remove any sensor from the Report Sensors list box, select it and click ⊖ Remove. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
11. To immediately send out the sensor report, click Send Report Now.

---

*Tip: When intending to send a sensor report using custom messages, use the placeholder [SENSORREPORT] to report sensor readings. See **Email and SMS Message Placeholders** (on page 150).*

---

12. Click Create.

Send SMS Message

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

Messages consist of a combination of free text and PDU placeholders. The placeholders represent information which is pulled from the PDU and inserted into the message.

Note: The PDU cannot receive SMS messages.

For example:

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

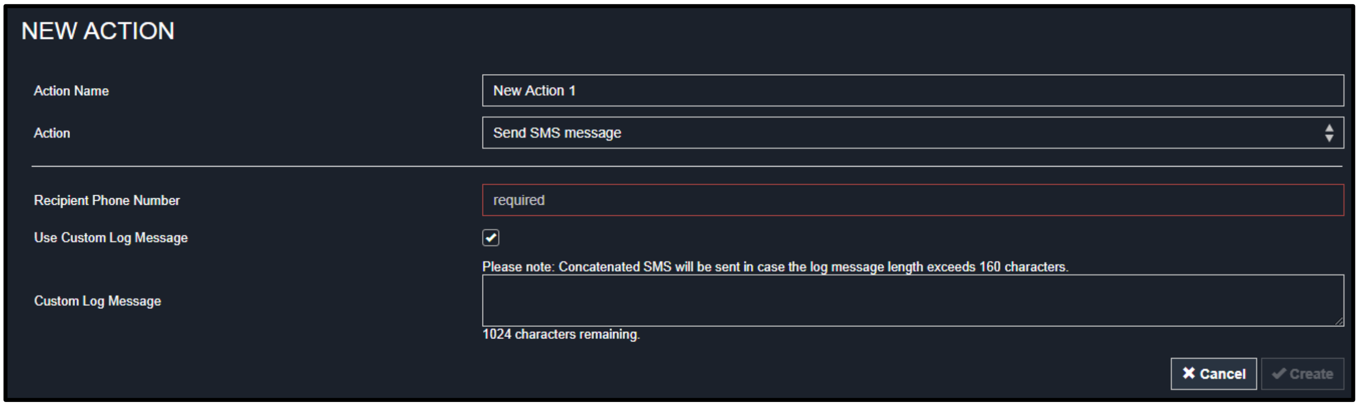
translates to

```
JQPublic logged into the device on 2012-January-30 21:00
```

For a list and definition of available variables, see ***Email and SMS Message Placeholders*** (on page 150).

▶ To create a send SMS message action:

1. Choose Device Settings > Event Rules > + New Action.
2. Select "Send SMS message" from the Action list.



NEW ACTION

Action Name	New Action 1
Action	Send SMS message
Recipient Phone Number	required
Use Custom Log Message	☑
Custom Log Message	Please note: Concatenated SMS will be sent in case the log message length exceeds 160 characters. 1024 characters remaining.

3. In the Recipient Phone Number field, specify the phone number of the recipient.

4. Select the Use Custom Log Message checkbox, and then create a custom message in the provided text box.
5. When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just click the desired placeholder. For details, see ***Email and SMS Message Placeholders*** (on page 150).
6. To start a new line in the text box, press Enter.
7. If needed, you can resize the text box by dragging the bottom-right corner.

Note: Only the 7-bit ASCII charset is supported for SMS messages.

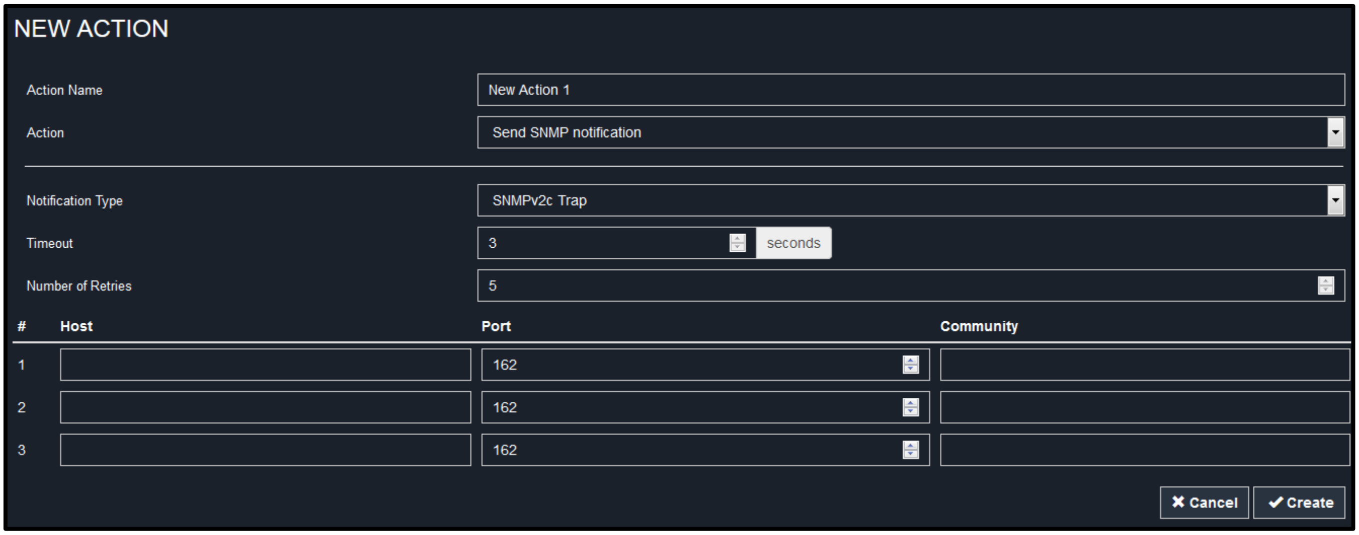
8. Click Create.

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

▶ To create a send SNMP v2c notifications action:

1. Choose Device Settings > Event Rules > + New Action.
2. Select "Send SNMP notification" from the Action list.
3. In the Notification Type field, select SNMPv2c Trap or SNMPv2c Inform.



NEW ACTION

Action Name	New Action 1
Action	Send SNMP notification
Notification Type	SNMPv2c Trap
Timeout	3 seconds
Number of Retries	5

#	Host	Port	Community
1		162	
2		162	
3		162	

4. For SNMP INFORM communications, leave the resend settings at their default or do the following:
   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.

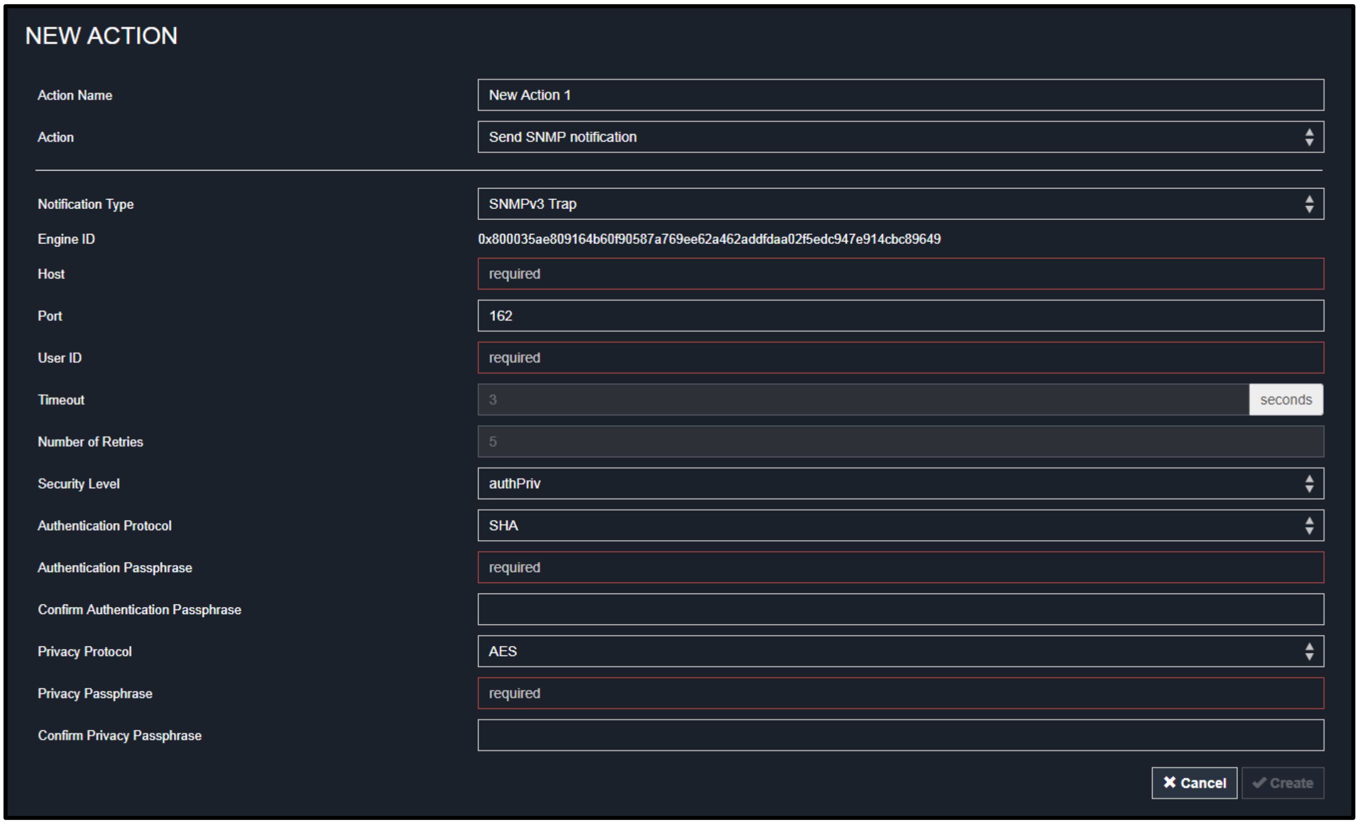
5. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.
6. In the Port fields, enter the port number used to access the device(s).
7. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the PDU and all SNMP management stations.

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

8. Click Create.

To create a send SNMP v3 notification action:

1. Choose Device Settings > Event Rules > + New Action.
2. Select "Send SNMP notification" from the Action list.
3. In the Notification Type field, select SNMPv3 Trap or SNMPv3 Inform.



NEW ACTION

Action Name	New Action 1
Action	Send SNMP notification
Notification Type	SNMPv3 Trap
Engine ID	0x800035ae809164b60f90587a769ee62a462addfdaa02f5edc947e914cbc89649
Host	required
Port	162
User ID	required
Timeout	3 seconds
Number of Retries	5
Security Level	authPriv
Authentication Protocol	SHA
Authentication Passphrase	required
Confirm Authentication Passphrase	
Privacy Protocol	AES
Privacy Passphrase	required
Confirm Privacy Passphrase	

4. For SNMP TRAPs, the engine ID is prepopulated.

5. For SNMP INFORM communications, leave the resend settings at their default or do the following:
   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
6. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:
   a. Host name
   b. Port number
   c. User ID for accessing the host -- make sure the User ID has the SNMPv3 permission.
   d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

7. Click Create.

Switch Outlets

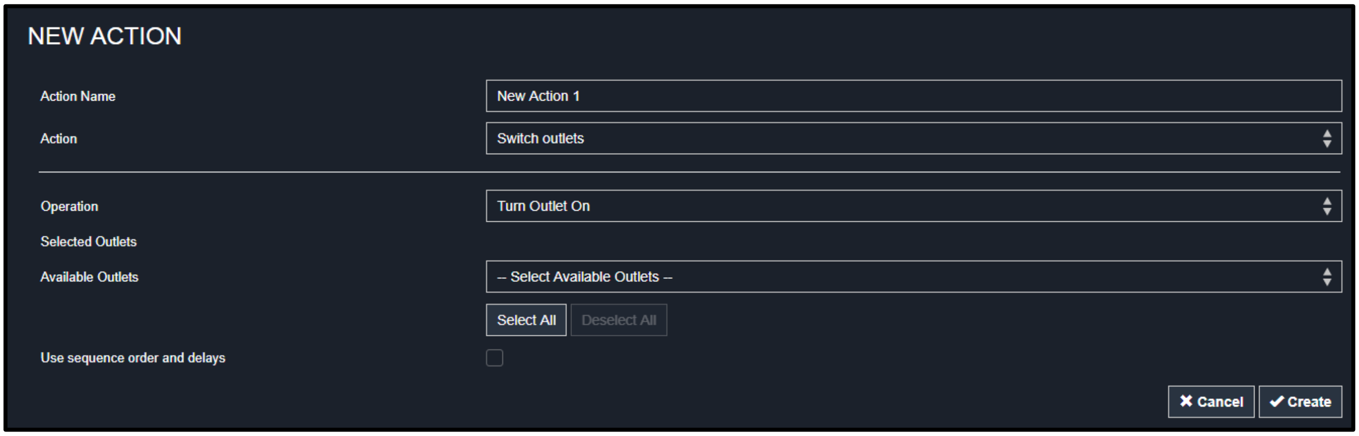
This action turns on, off or power cycles a specific outlet.

▶ To create a switch outlets action:

1. Choose Device Settings > Event Rules >

.

2. Select "Switch outlets" from the Action list.



NEW ACTION

Action Name: New Action 1

Action: Switch outlets

Operation: Turn Outlet On

Selected Outlets

Available Outlets: -- Select Available Outlets --

Use sequence order and delays ☐

3. In the Operation field, select an operation for the selected outlet(s).
4. Turn Outlet On: Turns on the selected outlet(s).
5. Turn Outlet Off: Turns off the selected outlet(s).
6. Cycle Outlet: Cycles power to the selected outlet(s).
7. To specify the outlet(s) where this action will be applied, select them one by one from the Available Outlets list.
8. To add all outlets, click Select All.
9. To remove any outlets from the Selected Outlets field, click that outlet's ✖.
10. To remove all outlets, click Deselect All.
11. If "Turn Outlet On" or "Cycle Outlet" is selected in step 3, you can choose to select the "Use sequence order and delays" checkbox so that all selected outlets will follow the power-on sequence defined on the page of ***Outlets*** (on page 33).

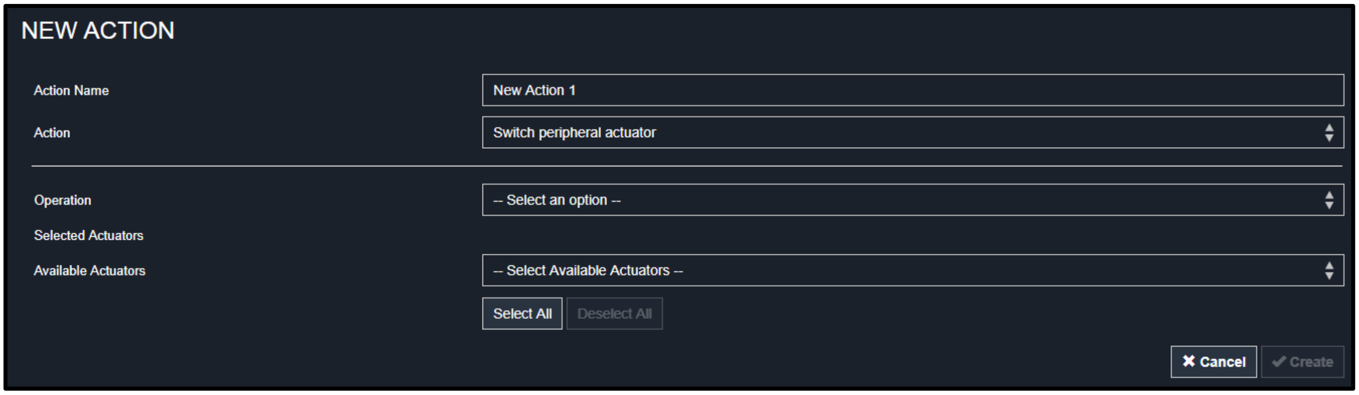
Switch Peripheral Dry Contact

If you have any dry contact connected to the PDU, it can be configured so it automatically turns on or off the system controlled by the dry contact when a specific event occurs.

Note: For information on connecting dry contacts, refer to ***Contact Closure Sensor Series*** *in the Premium+ PDU with RackLink Environmental Sensors User Manual at* ***www.middleatlantic.com****.*

▶ To create a switch peripheral dry contact action:

1. Choose Device Settings > Event Rules > + New Action.
2. Select "Switch peripheral actuator" from the Action list.



NEW ACTION

Action Name: New Action 1

Action: Switch peripheral actuator

Operation: -- Select an option --

Selected Actuators

Available Actuators: -- Select Available Actuators --

3. In the Operation field, select an operation for the selected actuator(s).
4. Turn On: Turns on the selected actuator(s).
5. Turn Off: Turns off the selected actuator(s).
6. To select the actuator(s) where this action will be applied, select them one by one from the Available Actuators list.
7. To add all actuators, click Select All.
8. To remove any selected actuator from the Selected Actuators field, click that actuator's ✖.
9. To remove all actuators, click Deselect All.
10. Click Create.

Syslog Message

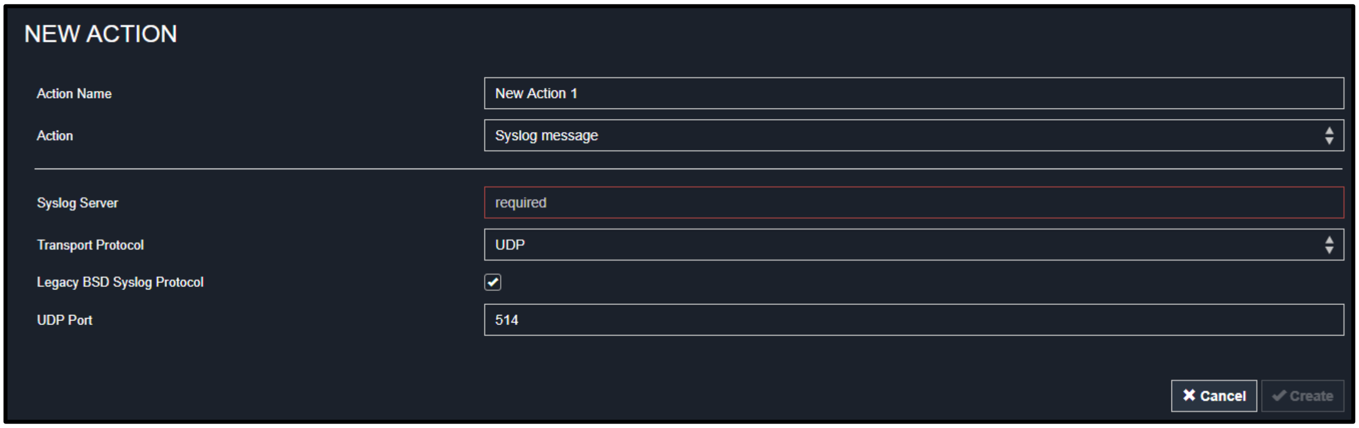
Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up - UDP, TCP or TLS over TCP.

The PDU may or may not detect the syslog message transmission failure. If yes, it will log this syslog failure as well as the failure reason in the event log. See ***Viewing or Clearing the Local Event Log*** (on page 167).

▶ To create a syslog message action:

1. Choose Device Settings > Event Rules > + New Action.

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



NEW ACTION

Action Name: New Action 1

Action: Syslog message

Syslog Server: required

Transport Protocol: UDP

Legacy BSD Syslog Protocol: ☑

UDP Port: 514

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

4. In the Transport Protocol field, select one of the syslog protocols: TCP, UDP or TCP+TLS. The default is UDP.

Transport protocols	Next steps
UDP	• In the UDP Port field, type an appropriate port number. Default is 514. • Select the "Legacy BSD Syslog Protocol" checkbox if applicable.
TCP	NO TLS certificate is required. Type an appropriate port number in the TCP Port field.
TCP+TLS	A TLS certificate is required. Do the following: a. Type an appropriate port number in the "TCP Port" field. Default is 6514. b. In the CA Certificate field, click Browse... to select a TLS certificate. After installing the certificate, you may: ▪ Click Show to view its contents. ▪ Click Remove to delete it if it is inappropriate. c. Determine whether to select the "Allow expired and not yet valid certificates" checkbox. ▪ To always send the event message to the specified syslog server as long as a TLS certificate is available, select this checkbox. ▪ To prevent the event message from being sent to the specified syslog server when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect this checkbox.

5. Click Create.

Scheduling an Action

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

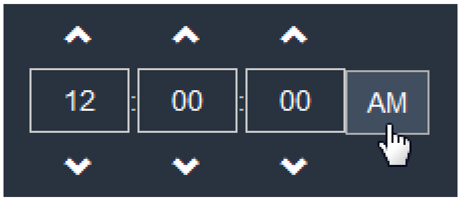
When scheduling an action, make sure you have a minimum of 1-minute buffer between this action's creation and first execution time. Otherwise, the scheduled action will NOT be performed at the specified time when the buffer time is too short. For example, if you want an action to be performed at 11:00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

If the needed action is not available yet, create it first. See ***Available Actions*** (on page 132).

▶ To schedule an action:

1. Choose Device Settings > Event Rules > + New Scheduled Action.
2. To select any action(s), select them one by one from the Available Actions list.
3. To select all available actions, click Select All.
4. To remove any action(s) from the Selected Actions field, click that action's ✖.
5. To remove all actions, click Deselect All.
6. Select the desired frequency in the Execution Time field, and then specify the time interval or a specific date and time in the field(s) that appear.

Execution time	Frequency settings
Minutes	Click the Frequency field to select an option. The frequency ranges from every minute, every 5 minutes, every 10 minutes and so on until every 30 minutes.
Hourly	Type a value in the Minute field, which is set to either of the following: • The Minute field is set to 0 (zero). Then the action is performed at 1:00 am, 2:00 am, 3:00 am and so on. • The Minute field is set to a non-zero value. For example, if it is set to 30, then the action is performed at 1:30 am, 2:30 am, 3:30 am and so on.

Execution time	Frequency settings
Daily	Type values or click ▲ ▼. The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. 12 : 00 : 00 AM For example, if you specify 01:30PM, the action is performed at 13:30 pm every day.
Weekly	Both the day and time must be specified for the weekly option. • Days range from Sunday to Saturday. • The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.
Monthly	Both the date and time must be specified for the monthly option. • The dates range from 1 to 31. • The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. Note that NOT every month has the date 31, and February in particular does not have the date 30 and probably even 29. Check the calendar when selecting 29, 30 or 31.
Yearly	This option requires three settings: • Month - January through December. • Day of month - 1 to 31. • Time - the value is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.

An example of the scheduled action is available in the section titled ***Send Sensor Report Example*** (on page 149).

Send Sensor Report Example

To create a scheduled action for emailing a temperature sensor report hourly, it requires:

- A 'Send email' action
- A 'Send sensor report' action
- A timer - that is, the scheduled action

▶ To create a send sensor report example:

1. Click **+ New Action** to create a 'Send email' action that sends an email to the desired recipient(s). For details, see ***Send Email*** (on page 137).
2. In this example, this action is named *Email a Sensor Report*.
3. If intended, you can customize the email messages in this action.
4. Click **+ New Action** to create a 'Send sensor report' action that includes the 'Email a Sensor Report' action as its destination action. For details, see ***Send Sensor Report*** (on page 138).
5. In this example, this action is named *Send Temperature Sensor Readings*.
6. You can specify more than one temperature sensor as needed in this action.
7. Click **+ New Scheduled Action** to create a timer for performing the 'Send Temperature Sensor Readings' action hourly. For details, see ***Scheduling an Action*** (on page 148).
8. In this example, the timer is named *Hourly Temperature Sensor Reports*.
9. To perform the specified action at 12:30 pm, 01:30 pm, 02:30 pm, and so on, select Hourly, and set the Minute to 30.

Then the PDU will send out an email containing the specified temperature sensor readings hourly every day.

Whenever you want the PDU to stop sending the temperature report, simply deselect the Enabled checkbox in the timer.

Email and SMS Message Placeholders

Actions of "Send email" and "Send SMS message" allow you to customize event messages. See ***Send Email*** (on page 137) or ***Send SMS Message*** (on page 141).

When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Simply drag the scroll bar and then click the desired placeholder to insert it into the custom message. Or you can type a keyword in the "search" box to quickly find the desired placeholder.

If desired, you can sort the list by clicking the desired column header. See ***Sorting a List*** (on page 28).

To make the Event Context Information disappear, click anywhere outside its window.

Following are placeholders that can be used in custom messages.

Placeholder	Definition
[ACTIVEINLET]	The label of the newly activated inlet
[CIRCUITCTRATING]	The circuit CT rating
[CIRCUITCURRENTRATING]	The circuit current rating

Placeholder	Definition
[CIRCUITNAME]	The circuit name
[CIRCUITPOLE]	The circuit power line identifier
[CIRCUITSENSOR]	The circuit sensor name
[CIRCUIT]	The circuit identifier
[CARDREADERPRODUCT]	The product name of a card reader
[CARDREADERSERIALNUMBER]	The serial number of a card reader
[COMPONENTID]	The ID of a hardware component
[CONFIGPARAM]	The name of a configuration parameter
[CONFIGVALUE]	The new value of a parameter
[DATETIME]	The human readable timestamp of the event occurrence
[DEVICEIP]	The IP address of the device, the event occurred on
[DEVICENAME]	The name of the device, the event occurred on
[DEVICESERIAL]	The unit serial number of the device the event occurred on
[ERRORDESC]	The error message
[EVENTRULENAME]	The name of the matching event rule
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSORSLOT]	The ID of a peripheral device slot
[FAILURETYPE]	The numeric hardware failure type
[FAILURETYPESTR]	The textual hardware failure type
[EXTSENSOR]	The peripheral device identifier
[IFNAME]	The human readable name of a network interface
[INLETPOLE]	The inlet power line identifier
[INLETSENSOR]	The inlet sensor name
[INLET]	The power inlet label
[ISASSERTED]	Boolean flag whether an event condition was entered (1) or left (0)

Placeholder	Definition
[LOGMESSAGE]	The original log message
[MONITOREDHOST]	The name or IP address of a monitored host
[OLDVERSION]	The firmware version the device is being upgraded from
[OUTLETNAME]	The outlet name *Note: If any outlet does not have a name, neither an outlet name nor an outlet number will be shown in the custom message for it. Therefore, it is recommended to check the availability of all outlet names if intending to use this placeholder.*
[OUTLETPOLE]	The outlet power line identifier
[OUTLETSENSOR]	The outlet sensor name
[OUTLET]	The outlet label
[PDUPOLESENSOR]	The sensor name for a certain power line
[PDUSENSOR]	The PDU sensor name
[PERIPHDEVPOSITION]	The position of an attached peripheral device
[PHONENUMBER]	The phone number an SMS was sent to
[PORTID]	The label of the external port, the event triggering device is connected to
[PORTTYPE]	The type of the external port (for example, 'feature' or 'auxiliary'), the event triggering device is connected to
[POWERMETERPOLE]	The PMC power meter line identifier
[POWERMETERSENSOR]	The PMC power meter sensor name
[POWERMETER]	The PMC power meter ID
[ROMCODE]	The rom code of an attached peripheral device
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREADING]	The value of a sensor reading
[SENSORREPORT]	The formatted sensor report contents

Placeholder	Definition
[SENSORSTATENAME]	The human readable state of a sensor
[SMTPRECIPIENTS]	The list of recipients, an SMTP message was sent to
[SMTPSERVER]	The name or IP address of an SMTP server
[SYSCONTACT]	SysContact as configured for SNMP
[SYSLOCATION]	SysLocation as configured for SNMP
[SYSNAME]	SysName as configured for SNMP
[TIMEREVENTID]	The id of a timer event
[TIMESTAMP]	The timestamp of the event occurrence
[TRANSFERSWITCHREASON]	The transfer reason
[TRANSFERSWITCHSENSOR]	The transfer switch sensor name
[TRANSFERSWITCH]	The transfer switch label
[UMTARGETROLE]	The name of a user management role, an action was applied on
[UMTARGETUSER]	The user, an action was triggered for
[USERIP]	The IP address, a user connected from
[USERNAME]	The user who triggered an action
[VERSION]	The firmware version the device is upgrading to
[SURGESTATUS]	Surge protection status

Editing or Deleting a Rule/Action

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

Exception: Some settings of the built-in event rules or actions are not user-configurable. Besides, you cannot delete built-in rules and actions. See ***Built-in Rules and Rule Configuration*** *(on page 121) or* ***Available Actions*** *(on page 132).*

► To edit or delete an event rule, action or scheduled action:

1. Choose Device Settings > Event Rules.
2. Click the desired one in the list of rules, actions or scheduled actions. Its setup page opens.
3. Perform the desired action.

4. To modify settings, make necessary changes and then click Save.
5. To delete it, click 🗑 Delete on the top-right corner. Then click Delete on the confirmation message.

Sample Event Rules

Sample PDU-Level Event Rule

In this example, we want the PDU to record the firmware upgrade failure in the internal log when it happens.

The event rule involves:

- Event: Device > Firmware update failed
- Action: System Event Log Action

▶ To create this PDU-level event rule:

1. For an event at the PDU level, select "Device" in the Event field.
2. Select "Firmware update failed" so that the PDU responds to the event related to firmware upgrade failure.
3. To make the PDU record the firmware update failure event in the internal log, select "System Event Log Action" in the Available Actions field.

Sample Outlet-Level Event Rule

In this example, we want the PDU to send SNMP notifications to the SNMP manager for any sensor change event of outlet 3.

The event rule involves:

- Event: Outlet > Outlet 3 > Sensor > Any sub-event
- Action: System SNMP Notification Action

▶ To create this outlet-level event rule:

1. For an event at the outlet level, select "Outlet" in the Event field.
2. Select "Outlet 3" because that is the desired outlet.
3. Select "Sensor" to refer to sensor-related events.
4. Select "Any sub-event" to include all events related to all sensors of this outlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
5. To make the PDU send SNMP notifications, select "System SNMP Notification Action" in the Available Actions field.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action. See ***Enabling and Configuring SNMP*** *(on page 194).*

Then the SNMP notifications are sent when:

6. Any numeric sensor's reading enters the warning or critical range.
7. Any sensor reading or state returns to normal.
8. Any sensor becomes unavailable.
9. The active energy sensor is reset.
10. Any state sensor changes its state.

For example, when the outlet 3's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

Sample Inlet-Level Event Rule

In this example, we want the PDU to send SNMP notifications to the SNMP manager for any sensor change event of the Inlet I1.

The event rule involves:

- Event: Inlet > Sensor > Any sub-event
- Action: System SNMP Notification Action

▸ To create the above event rule:

1. For an event at the inlet level, select "Inlet" in the Event field.
2. Select "Sensor" to refer to sensor-related events.
3. Select "Any sub-event" to include all events related to all sensors of this inlet and all thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
4. To make the PDU send SNMP notifications, select "System SNMP Notification Action" in the Available Actions box.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps/informs, depending on the settings for the System SNMP Notification Action. See ***Enabling and Configuring SNMP*** *(on page 194).*

Then the SNMP notifications are sent when:

5. Any numeric sensor's reading enters the warning or critical range.
6. Any sensor reading or state returns to normal.
7. Any sensor becomes unavailable.
8. The active energy sensor is reset.

For example, when the Inlet I1's voltage exceeds the upper warning threshold, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

Sample Environmental-Sensor-Level Event Rule

In this example, we want the PDU to activate the load shedding function when a contact closure sensor enters the alarmed state. This event rule requires creating a new action before creating the rule.

Step 1: create a new action for activating the load shedding

1. Choose Device Settings > Event Rules > + New Action.
2. In this illustration, assign the name "Activate Load Shedding" to the new action.
3. In the Action field, select "Change load shedding state."
4. In the Operation field, select Start Load Shedding.
5. Click Create to finish the creation.

After the new action is created, follow the procedure below to create an event rule that triggers the load shedding mode when the contact closure sensor enters the alarmed state. This event rule involves the following:

- Event: Peripheral Device Slot > Slot 1 > State Sensor/Actuator > Alarmed/Open/On
- Trigger condition: Alarmed
- Action: Activate Load Shedding

Step 2: create the contact closure-triggered load shedding event rule

1. Click + New Rule on the Event Rules page.
2. In this illustration, assign the name "Contact Closure Triggered Load Shedding" to the new rule.
3. In the Event field, select "Peripheral Device Slot" to indicate we are specifying an event related to the environmental sensor package.
4. Select the ID number of the desired contact closure sensor. In this illustration, the ID number of the desired contact closure sensor is 1, so select Slot 1.

---

*Note: ID numbers of all sensors/dry contacts are available on the Peripherals page. See **Peripherals** (on page 57).*

---

5. Select "State Sensor/Actuator" because the contact closure sensor is a state sensor.
6. Select "Alarmed" since we want the PDU to respond when the selected contact closure sensor changes its state related to the "alarmed" state.
7. In the "Trigger condition" field, select the Alarmed/Open/On radio button so that the action is taken only when the contact closure sensor enters the alarmed state.
8. Select "Activate Load Shedding" from the Available Actions list.

A Note about Infinite Loop

You should avoid building an infinite loop when creating event rules.

The infinite loop refers to a condition where the PDU keeps busy because the action or one of the actions taken for a certain event triggers an identical or similar event which will result in an action triggering one more event.

Example 1

This example illustrates an event rule which continuously causes the PDU to send out email messages.

Event selected	Action included
Device > Sending SMTP message failed	Send email

Example 2

This example illustrates an event rule which continuously causes the PDU to send out SMTP messages when one of the selected events listed on the Device menu occurs. Note that <Any sub-event> under the Device menu includes the event "Sending SMTP message failed."

Event selected	Action included
Device > Any sub-event	Send email

Example 3

This example illustrates a situation where two event rules combined regarding the outlet state changes causes the PDU to continuously power cycle outlets 1 and 2 in turn.

Event selected	Action included
Outlet > Outlet 1 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 2 (Switch outlets --> Cycle Outlet --> Outlet 2)
Outlet > Outlet 2 > Sensor > Outlet State > On/Off > Both (trigger condition)	Cycle Outlet 1 (Switch outlets --> Cycle Outlet --> Outlet 1)

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing the PDU to generate an alert. The measurement then returns to a value within the threshold, but the PDU does not generate an alert message for the Deassertion event. Such scenarios can occur due to the The PDU tracking the PDU uses. For more information, refer to ***"To De-assert" and Deassertion The PDU*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.

Setting Data Logging

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

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field.

Since the PDU's internal sensors are measured every second, specifying a value of 60, for example, would cause measurements to be written to the data log once every minute. Since there are 120 measurements of storage per sensor, specifying a value of 60 means the log can store the last two hours of measurements before the oldest one in the log gets overwritten.

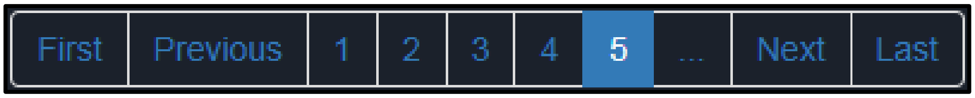
Whenever measurements are written to the log, three values for each sensor are written: the average, minimum and maximum values. For example, if measurements are written every minute, the average of all measurements that occurred during the preceding 60 seconds along with the minimum and maximum measurement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

Note: The PDU's SNMP agent must be enabled for this feature to work. See ***Enabling and Configuring SNMP*** *(on page 194). In addition, using an NTP time server ensures accurately time-stamped measurements.*

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

▶ To configure the data logging feature:

1. Choose Device Settings > Data Logging.
2. To enable the data logging feature, select the "Enable" checkbox in the General Settings section.
3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.
4. Verify that all sensor logging is enabled. Logging is divided into sections of the page based on sensor types. You can also click Enable All at the bottom of the page to have all sensors selected.
5. You can also click the topmost checkbox labeled "Logging Enabled" in the header row of each sensor type section to select all sensors of the same type.
6. If any section's number of sensors exceeds 35, the remaining sensors are listed on next page(s). If so, a pagination bar similar to the following diagram displays in this section, which you can click any button to switch between pages.



7. Click Save. This button is located at the bottom of the page.

Important: Although it is possible to selectively enable/disable logging for individual sensors on the PDU, it is NOT recommended to do so.

Configuring Data Push Settings

You can push the sensor data to a remote server for data synchronization. The data will be sent in JSON format using HTTP POST requests. You need to set up the destination and authentication for data push on the PDU.

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

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

See ***Event Rules and Actions*** (on page 120).

▶ To configure data push settings:

1. Choose Device Settings > Data Push.
2. To specify a destination, click + New Destination.
3. Do the following to set up the URL field.
   a. Click http:// ⬍ to select *http* or *https*.
   b. Type the URL or host name in the accompanying text box.
4. If selecting https, a CA certificate is required for making the connection. Click Browse... to install it. Then you can:
5. Click Show to view the certificate's content.
6. Click Remove to delete the installed certificate if it is inappropriate.
7. If the destination server requires authentication, select the Use Authentication checkbox, and enter the following data.
   - User name
   - Password
8. In the Entry Type field, determine the data that will be transmitted.
   - Sensor log: Transmit the record of all logged sensors, including their sensor readings and/or status. Logged sensors refer to all internal and/or environmental sensors/dry contacts that you have selected on the Data Logging page. See Setting Data Logging (on page 157).
9. Click Create.
10. Repeat the same steps for additional destinations.

▶ To modify or delete data push settings:

1. On the Data Push page, click the one you want in the list.
2. Perform either action below.

3. To modify settings, make necessary changes and then click Save.
4. To delete it, click Delete, and then confirm it on the confirmation message.

Monitoring Component Reachability

You can monitor whether specific devices are alive by having the PDU continuously ping them. A device's successful response to the ping commands indicates that the device is still alive and can be remotely accessed.

This function is especially useful when you are not located in an area with Internet connectivity.

The PDU can monitor the accessibility of any device, such as third-party control systems, televisions, power distribution units (PDUs), or routers.

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

*Tip: To make the PDU automatically log, send notifications or perform other actions for any component monitoring events, you can create event rules. See **Event Rules and Actions** (on page 120). An example is available in **Example: Ping Monitoring and SNMP Notifications** (on page 162).*

▶ To add IT equipment for ping monitoring:

1. Choose Device Settings > Component Reachability.
2. Click + Monitor New Component.
3. By default, the "Enable ping monitoring for this component" checkbox is selected. If not, select it to enable this feature.
4. Configure the following.

Field	Description
IP address/hostname	IP address or host name of the IT equipment which you want to monitor.
Enable ping monitoring for this component	Select the checkbox to enable ping monitoring.
Number of successful pings to enable feature	The number of successful pings required to declare that the monitored equipment is "Reachable." Valid range is 0 to 200.
Wait time after successful ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait time after unsuccessful ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).

Field	Description
Number of consecutive unsuccessful pings for failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.
Wait time before resuming pinging after failure	The wait time before the PDU resumes pinging after the monitored equipment is declared "Unreachable." Valid range is 1 to 1200 (seconds).
Number of consecutive failures before disabling feature (0 = unlimited)	The number of times the monitored equipment is declared "Unreachable" consecutively before the PDU disables the ping monitoring feature for it and shows "Waiting for reliable connection." Valid range is 0 to 100.

5. Click Create.
6. To add more IT devices, repeat the same steps.

Initially, the status of the added IT equipment shows "Waiting for reliable connection," which means the requested number of consecutive successful or unsuccessful pings has not been reached before the PDU can declare that the monitored device is reachable or unreachable.

▶ To check the component monitoring states and results:

1. After adding IT equipment for monitoring, all IT devices are listed on the Component Reachability page.
2. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.
3. The column labeled "Status" indicates the accessibility of each monitored equipment.

Status	Description
Reachable	The monitored equipment is accessible.
Unreachable	The monitored equipment is inaccessible.
Waiting for reliable connection	The connection between the PDU and the monitored equipment is not reliably established yet.

Editing or Deleting Ping Monitoring Settings

You can edit the ping monitoring settings of any IT device or delete it if it's no longer needed.

▶ **To modify or delete any monitored IT device:**

1. Choose Device Settings > Component Reachability.
2. Click the desired one in the list.
3. Perform the desired action.
4. To modify settings, make necessary changes and then click Save. For information on each field, see ***Monitoring Component*** (on page 160).
5. To delete it, click 🗑 on the top-right corner.

Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your PDU to make sure that PDU is properly operating all the time, and the PDU must send out SNMP notifications (trap or inform) if that PDU is declared unreachable due to power or network failure. The prerequisite for this example is that the power sources are different between your PDU and the monitored PDU.

This requires the following two steps.

▶ **Step 1: Set up the ping monitoring for the target PDU**

1. Choose Device Settings > Component Reachability.
2. Click + Monitor New Component.
3. Ensure the "Enable ping monitoring for this component" checkbox is selected.
4. Enter the data shown below.
5. Enter the component's data.

Field	Data entered
IP address/hostname	192.168.84.95

6. To make the PDU declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, enter the following data.

Field	Data entered
Number of successful pings to enable feature	3

Field	Data entered
Wait time after successful ping	5

7. To make the PDU declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 seconds * 3 pings), enter the following data.

Field	Data entered
Wait time after unsuccessful ping	4
Number of consecutive unsuccessful pings for failure	3

8. To make the PDU stop pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared. After 60 seconds, the PDU will re-ping the target PDU, enter the following data.

Field	Data entered
Wait time before resuming pinging after failure	60

9. The "Number of consecutive failures before disabling feature (0 = unlimited)" can be set to any value you want.
10. Click Create.

Step 2: Create an event rule to send SNMP notifications for the target PDU

1. Choose Device Settings > Event Rules.
2. Click + New Rule.
3. Select the Enabled checkbox to enable this new rule.
4. Configure the following.

Field or Setting	Data specified
Rule name	Send SNMP notifications for PDU (192.168.84.95) inaccessibility
Event	Choose Component Reachability > 192.168.84.95 > Unreachable
Trigger condition	Select the Unreachable radio button

This will make the PDU react only when the target PDU becomes inaccessible.

5. Select the System SNMP Notification Action.

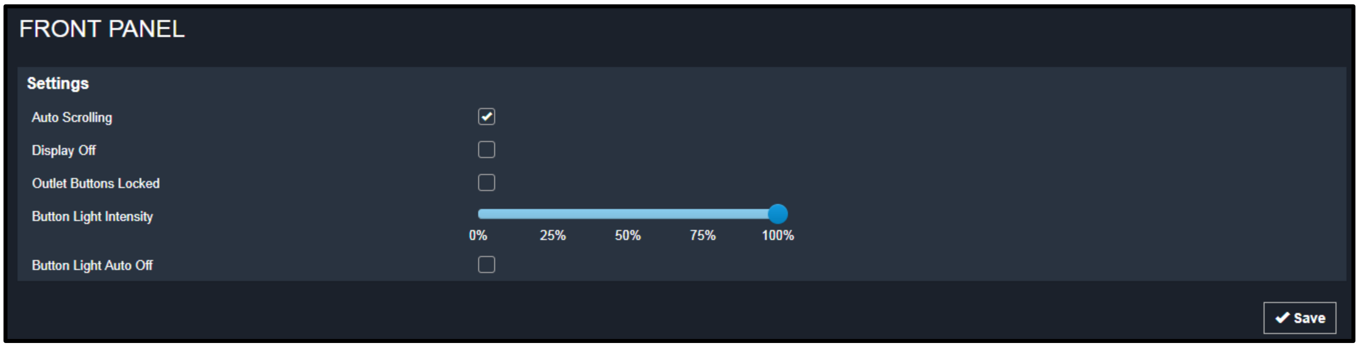
*Note: If you have not configured the System SNMP Notification Action to specify the SNMP destination(s), see **Editing or Deleting a Rule/Action** (on page 153).*

Front Panel Settings (Rackmount PDUs Only)

You can make various settings to the outlet buttons and front panel display area on the front panel of your Rackmount PDU.

▶ To configure the front panel settings:

1. Choose Device Settings > Front Panel.
2. The front panel page appears.



FRONT PANEL

Settings

Auto Scrolling ☑

Display Off □

Outlet Buttons Locked □

Button Light Intensity

Button Light Auto Off □

3. Configure the following fields:

- Auto Scrolling: Select this checkbox to enable the auto scrolling of information on the front panel display. For more information, see ***Front Panel (Rackmount PDUs Only)*** (on page 14).
- Display Off: Select this checkbox to turn off the front panel display text.

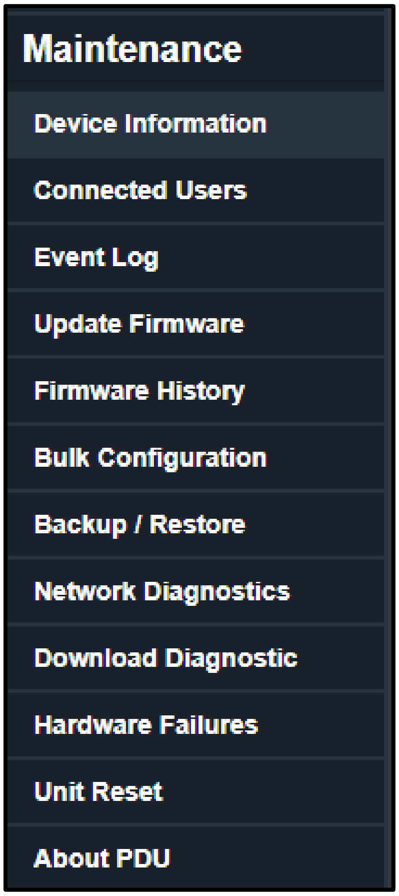
Note: Even with the Display Off checkbox selected, the outlet relays still remain active and responsive.

- Outlet Buttons Locked: Select this checkbox to lock the outlet buttons on the front panel. They will continue to indicate outlet status in the user interface, but will no longer toggle the outlet when touched from the front panel.
- Button Light Intensity: Slide along the percentage rule to select one of the five levels of light intensity for your outlet buttons on the front panel.
- Button Light Auto Off: Select this checkbox to have the outlet buttons on the front panel automatically turn off after approximately 10 seconds of inactivity.

4. Click Save.

Maintenance

Click 'Maintenance' in the *Menu* (on page 27), and the following submenu appears.



Device Information

Using the web interface, you can retrieve hardware and software information of components or peripheral devices connected to your PDU.

Tip: If the information shown on this page does not match the latest status, press F5 to reload it.

▶ **To display device information:**

1. Choose Maintenance > Device Information.
2. Click the desired section's title bar to show that section's information. For example, click the Network section.

The number of available sections is model dependent.

Section title	Information shown
Information	General device information, such as model name, serial number, firmware version, hardware revision, MIB download link(s) and so on.
Network	The network information, such as the current networking mode, IPv4 and/or IPv6 addresses.
Port Forwarding	Displays port forwarding settings for your network.
Outlets	Each outlet's label, receptacle type, operating voltage and rated current.
Controllers	Each inlet or outlet controller's serial number, board ID, firmware version, and hardware version.
Peripheral Devices	Serial numbers, model names, position and firmware-related information of connected environmental sensor packages.
Asset Management	Provides device information regarding type, number of components, device ID, hardware version, boot version, app version, and protocol state.

Viewing Connected Users

You can check which users have logged in to the PDU and their status. If you have administrator privileges, you can terminate any user's connection to the PDU.

▶ To view and manage connected users:

1. Choose Maintenance > Connected Users.

   The Connected Users page appears.

If desired, you can sort the list by clicking the desired column header. See ***Sorting a List*** (on page 28).

Column	Description
User name	The login name of each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (serial RS-232 or USB), <local> is displayed instead of an IP address.

Column	Description
Client Type	The interface through which the user is being connected to the PDU. • Web GUI: Refers to the web interface. • CLI: Refers to the command line interface (CLI). ▪ The information in parentheses following "CLI" indicates how this user is connected to the CLI. ▪ Serial: The local connection, such as the serial RS-232 or USB connection. ▪ SSH: The SSH connection. ▪ Telnet: The Telnet connection.
Idle Time	The length of time for which a user remains idle.

2. To disconnect any user, click the corresponding Disconnect.
   a. Click Disconnect on the confirmation message.
   b. The disconnected user is forced to log out.

Viewing or Clearing the Local Event Log

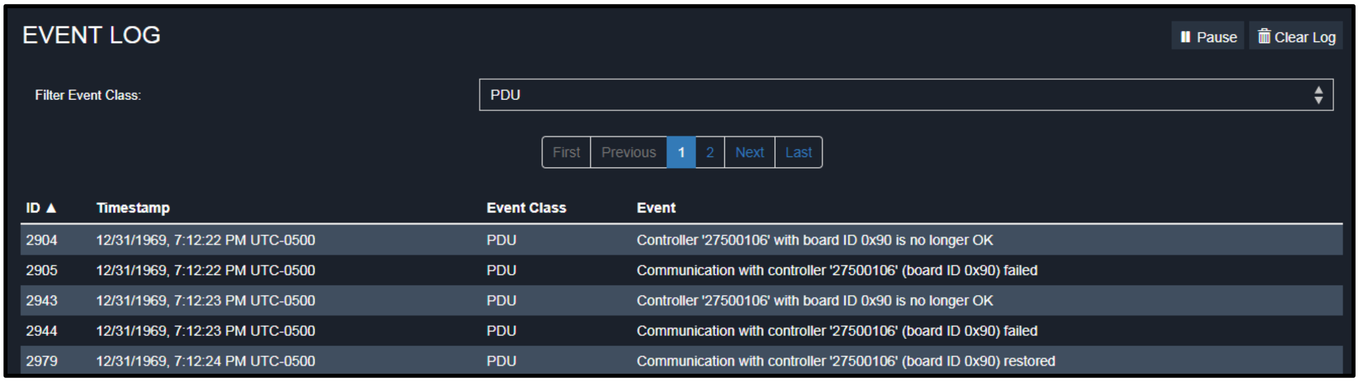
By default, the PDU captures certain system events and saves them in a local (internal) event log.

You can view over 2000 historical events that occurred on the PDU in the local event log. When the log size exceeds 256KB, each new entry overwrites the oldest one.

▶ To display the local log:

1. Choose Maintenance > Event Log.

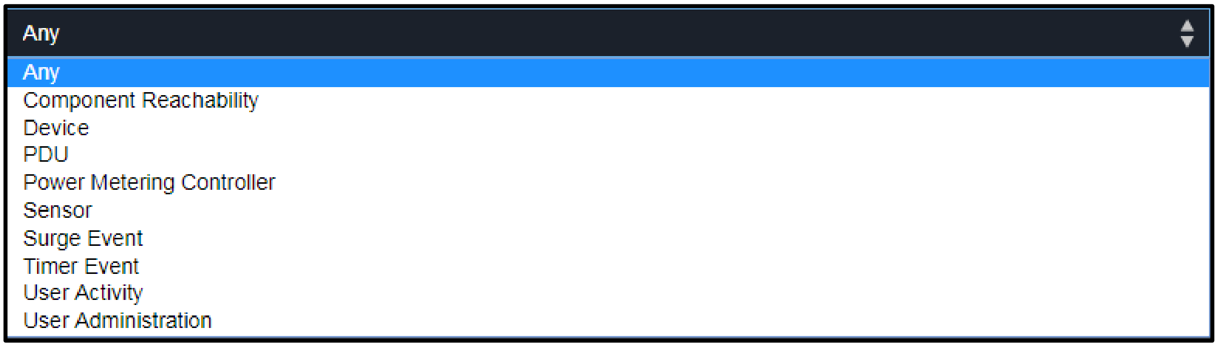
   The Event Log page appears.

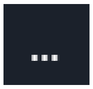


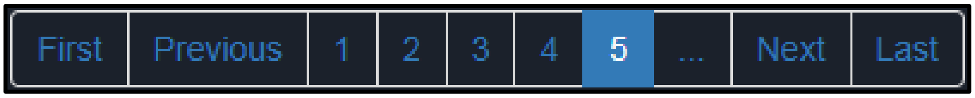
ID ▲	Timestamp	Event Class	Event
2904	12/31/1969, 7:12:22 PM UTC-0500	PDU	Controller '27500106' with board ID 0x90 is no longer OK
2905	12/31/1969, 7:12:22 PM UTC-0500	PDU	Communication with controller '27500106' (board ID 0x90) failed
2943	12/31/1969, 7:12:23 PM UTC-0500	PDU	Controller '27500106' with board ID 0x90 is no longer OK
2944	12/31/1969, 7:12:23 PM UTC-0500	PDU	Communication with controller '27500106' (board ID 0x90) failed
2979	12/31/1969, 7:12:24 PM UTC-0500	PDU	Communication with controller '27500106' (board ID 0x90) restored

2. Click the Pause button to stop updating the page with log information from your PDU.

3. Click the Clear Log button to delete the current log data from the Event Log page and your PDU.
4. To view specific type of events only, select the desired event type in the Filter Event Class field.



5. The List of event logs include entries with the following information.
6. ID number of the event
7. Date and time of the event
8. Event Class
9. A description of the event
10. To navigate other pages of the log, click the pagination bar at the top or bottom of the page.
11. If there are more than 5 pages and the page numbers displayed in the bar does not show the desired one, click  to have it show the next or previous five page numbers, if available.



12. If desired, you can sort the list by clicking the desired column header. See ***Sorting a List*** (on page 28).

Updating the PDU Firmware

Firmware files are available at www.middleatlantic.com.

When performing the firmware upgrade, the PDU keeps each outlet's power status unchanged so no server operation is interrupted. During and after the firmware upgrade, outlets that have been powered on prior to the firmware upgrade remain powered on and outlets that have been powered off remain powered off.

You must be the administrator or a user with the Firmware Update permission to update the PDU firmware.

(www.middleatlantic.com). If you have any questions or concerns about the upgrade, contact Technical Support BEFORE upgrading.

Note: Performing a firware upgrade on some mobile devices, such as an iPad, often require the installation and use of a file manager application.

Important: Do not perform the firmware upgrade over a wireless network connection.

To update the firmware:

1. Choose Maintenance > Update Firmware.
2. Click Browse... to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload process.
4. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.
5. If anything is incorrect, click Discard Upload.
6. To proceed with the update, click Update Firmware.

Important: Do not power off the PDU during the firmware update.

7. During the firmware update:
    a. A progress bar appears on the web interface, indicating the update status.
    b. The outlet LEDs flash if the relay boards are being updated. If the firmware update does not include the update of the relay board firmware, outlet LEDs do NOT flash.
    c. No users can successfully log in to the PDU.
    d. Other users' operation, if any, is forced to suspend.
8. When the update is complete, the PDU resets, and the Login page re-appears.
9. Other logged-in users are logged out when the firmware update is complete.

Important: If you are using the PDU with an SNMP manager, download its MIB again after the firmware update to ensure your SNMP manager has the correct MIB for the latest release you are using. See *Chapter 4: Using SNMP* (on page 194).

Alternative Firmware Updating Methods

Alternatives to updating the firmware:

To use a different method to update the firmware, refer to:

- ***Firmware Update via SCP*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.

- ***Bulk Configuration or Firmware Upgrade via DHCP/TFTP*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.
- ***Firmware Upgrade via USB*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.

A Note about Firmware Upgrade Time

The PDU firmware upgrade time varies from unit to unit, depending on various external and internal factors.

External factors include, but are not limited to: network throughput, firmware file size, and speed at which the firmware is retrieved from the storage location. Internal factors include: the necessity of upgrading the firmware on the microcontroller and the number of microcontrollers that require upgrade (which depends on the number of outlets). The microcontroller is upgraded only when required. Therefore, the length of firmware upgrade time ranges from approximately 3 minutes (without any microcontroller updated) to almost 7 minutes (with all microcontrollers for 48 outlets updated).

Take the above factors into account when estimating the PDU's firmware upgrade time.

The time indicated in this note is for PDU web interface-based upgrades. Upgrades through other management systems may take additional time beyond the control of the PDU itself. This note does not address the upgrades using other management systems.

Full Disaster Recovery

If the firmware upgrade fails, causing the PDU to stop working, you can recover it by using a special utility rather than returning the device.

Contact Technical Support for the recovery utility, which works in Windows XP/Vista/7/10 and Linux. In addition, an appropriate PDU firmware file is required in the recovery procedure.

Note: All PDUs can be recovered via either a USB or serial RS-232 connection.

Viewing Firmware Update History

The firmware upgrade history is permanently stored on the PDU. It remains available even though you perform a device reboot or any firmware update.

▶ **To view the firmware update history:**

1. Choose Maintenance > Firmware History.

   Each firmware update event consists of:

   - Update date and time
   - Previous firmware version
   - Update firmware version

- Update result

2. If desired, you can sort the list by clicking the desired column header. See ***Sorting a List*** (on page 28).

Bulk Configuration

The Bulk Configuration feature lets you save generic settings of a configured PDU to your computer. You can use this configuration file to copy common settings to other PDUs of the same model and firmware version. See ***Bulk Configuration Restrictions*** (on page 174).

Note that **NO device-specific data is saved** to the bulk configuration file, such as environmental sensors or certain network settings. For a list of device-specific settings that are *not* saved, see ***Device-Specific Settings NOT Included*** (on page 175).

Because the date and time settings are saved in the configuration file, users should exercise caution when distributing the configuration file to the PDUs in a different time zone than the source device.

*Tip: To back up or restore "all" settings of a particular PDU, use the Backup/Restore feature instead. See **Backup and Restore of Device Settings** (on page 175).*

Viewing Or Editing Existing Bulk Profiles

To view or edit existing bulk profiles:

1. Choose Maintenance > Bulk Configuration.

   The Bulk Profiles and Bulk Configuation page appears.

   If desired, you can sort the list in the Bulk Profiles section by clicking the desired column header. See ***Sorting a List*** (on page 28).

Column	Description
#	The assigned nuber to the bulk profile.
Name	The name of the bulk profile.
Description	▪ The description of the bulk profile.
Default Profile	A check mark appears in the corresponding row of the default profile.

2. Click an existing Bulk Profile on the list.

   Its corresponding Edit Bulk Profile page appears.

   Note: The Bulit in bulk profile may be viewed from the Bulk Profiles and Edit Bulk Profile pages, but cannot be edited.

3. Make changes as desired.

4. Click Save.

Adding a Bulk Profile

To add a bulk profile:

1. Choose Maintenance > Bulk Configuration.

   The Bulk Profiles and Bulk Configuation page appears.

2. Click +.

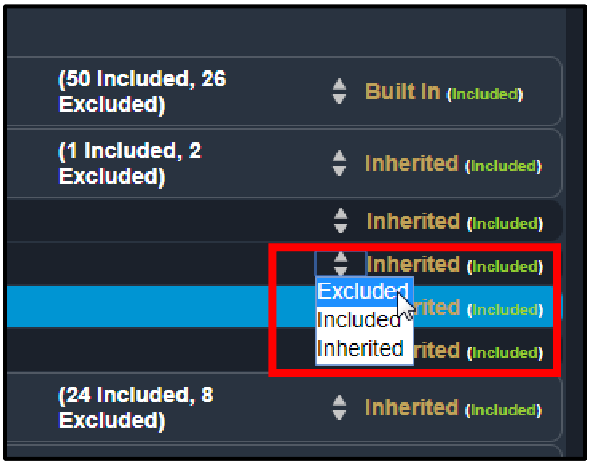
   The New Bulk Profile screen appears.

   If desired, you can sort the list by clicking the desired column header. See *Sorting a List* (on page 28).

3. Configure the following.
4. Profile Name: Add a name for your new bulk profile with no spaces.

   Note: The name must only contain alphanumeric, +, -, or / characters.

5. Description: Add a description for your new bulk profile.
6. Select the Select as default profile checkbox as desired.
7. Modify the Filter settings as desired. Use the drop-down to select Inherited, Included, or Excluded for each setting.



8. Click Save.

Saving a Bulk Configuration File

To save a bulk configuration file:

You must have the Administrator Privileges or "Unrestricted View Privileges" to download the configuration. See *Creating Roles* (on page 76).

1. Log in to the PDU whose settings you want to copy from.
2. Choose Maintenance > Bulk Configuration.

   The Bulk Profiles and Bulk Configuation page appears.
3. Use the drop-down to select whether you want your bulk configuration file encrypted or stored as clear text.
4. Click Download Bulk Configuration.
5. When prompted to open or save the configuration file, click Save.
6. The file is saved in the XML format, and, if encrypted is selected as the backup format, its content is encrypted using the AES-128 encryption algorithm.

Restoring a Bulk Configuration File

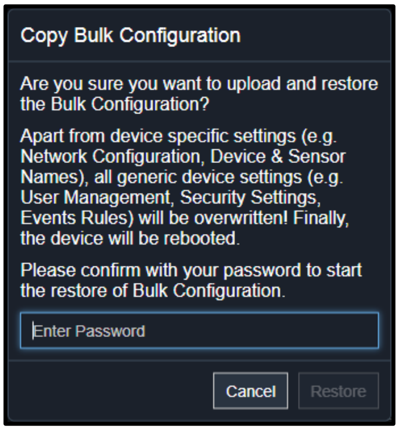
▶ To restore a bulk configuration:

You must have the Administrator Privileges to upload the configuration. See ***Creating Roles*** (on page 76).

1. Log in to another PDU of the same model running the same firmware.
2. Choose Maintenance > Bulk Configuration.

   The Bulk Profiles and Bulk Configuation page appears.
3. Click Browse... to to select the configuration file.
4. Click 'Upload & Restore Bulk Configuration' to copy it.

   A message appears, prompting you to confirm the operation and enter the admin password.



Copy Bulk Configuration

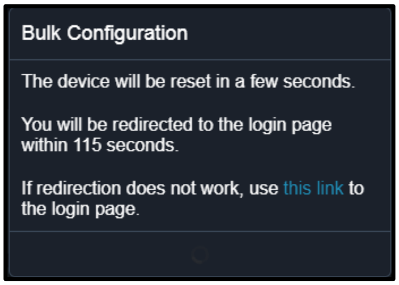
Are you sure you want to upload and restore the Bulk Configuration?

Apart from device specific settings (e.g. Network Configuration, Device & Sensor Names), all generic device settings (e.g. User Management, Security Settings, Events Rules) will be overwritten! Finally, the device will be rebooted.

Please confirm with your password to start the restore of Bulk Configuration.

5. Enter the admin password, and click Restore.

A second message appears notifying you that your PDU will reset and you'll be take to the login page.



Bulk Configuration

The device will be reset in a few seconds.

You will be redirected to the login page within 115 seconds.

If redirection does not work, use this link to the login page.

6. Wait until the PDU resets and the login page re-appears.

Note: On startup, the PDU performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

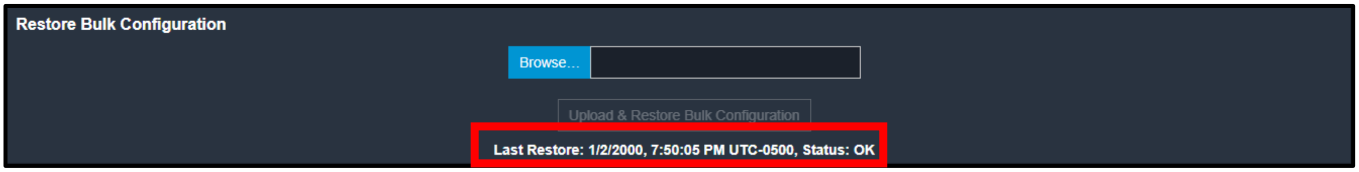
Viewing the Last Configuration Copying Record

▶ To view the last configuration copying record:

1. Choose Maintenance > Bulk Configuration.

   The Bulk Profiles and Bulk Configuation page appears.

2. After copying a bulk configuration or device backup file to the PDU, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.



Restore Bulk Configuration

Last Restore: 1/2/2000, 7:50:05 PM UTC-0500, Status: OK

Understanding Alternative Bulk Configuration Methods

▶ Bulk configuration method alternatives:

To use a different method to perform bulk configuration, refer to:

- ***Bulk Configuration via SCP*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.
- ***Bulk Configuration or Firmware Upgrade via DHCP/TFTP*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.
- ***Configuration or Firmware Upgrade with a USB Drive*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.

Bulk Configuration Restrictions

A source device is the PDU where the bulk configuration file is downloaded/saved.

A target device is the PDU that loads this bulk configuration file.

▶ Restrictions for bulk configuration:

- The target device must be running the same firmware version as the source device.
- The target device must be of the same model type as the source device.
- Bulk configuration is permitted between devices of the same model number type. For instance, you can copy a bulk configuration file from a RLNK-P915R to other RLNK-P915R models.

Device-Specific Settings NOT Included

The settings saved in the bulk configuration file include user and role configurations, thresholds, event rules, security settings, date/time and so on.

Note: Because the date and time settings are saved in the configuration file, users should exercise caution when distributing the configuration file to the PDUs in a different time zone than the source device.

The bulk configuration file does NOT contain device-specific information, including:

- Device name
- SNMP system name, contact and location
- Network settings (IP address, gateway, netmask and so on)
- Device logs
- Names, states and values of environmental sensors and actuators
- TLS certificate
- Component monitoring entries
- Outlet names and states

Backup and Restore of Device Settings

Unlike the bulk configuration file, the backup file contains ALL device settings, including device-specific data like device names and network settings. To back up or restore a PDU's settings, you should perform the Backup/Restore feature.

All PDU information is captured in the XML backup file except for the device logs and TLS certificate.

*Note: To perform bulk configuration among multiple PDUs, use the Bulk Configuration feature instead. See **Bulk Configuration** (on page 171).*

Saving Device Settings

▶ To save device settings:

You must have the Administrator Privileges or "Unrestricted View Privileges" to download a backup file. See ***Creating Roles*** (on page 76).

1. Choose Maintenance > Backup/Restore.

   The Backup/Restore page appears.

2. Use the drop-down to select whether you want your bulk configuration file encrypted or stored as clear text.
3. Click Download Device Settings. Save the file to your computer.
4. The file is saved in the XML format, and, if encrypted is selected as the backup format, its content is encrypted using the AES-128 encryption algorithm.

Copy Device Settings

▶ To copy device settings:

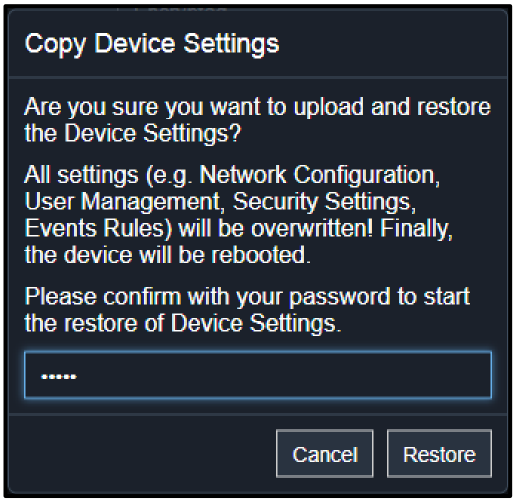
You must have the Administrator Privileges to copy the device settings. See ***Creating Roles*** (on page 76).

1. Choose Maintenance > Backup/Restore.

   The Backup Restore page appears.

2. Click Browse... to to select the backup file.
3. Click 'Upload & Restore Device Settings' to upload the file.

   A message appears, prompting you to confirm the operation and enter the admin password.



Copy Device Settings

Are you sure you want to upload and restore the Device Settings?

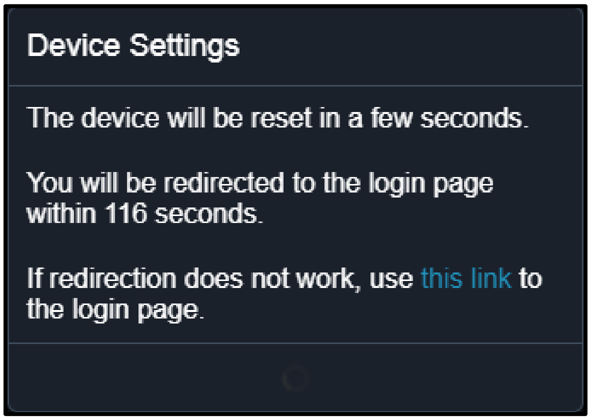
All settings (e.g. Network Configuration, User Management, Security Settings, Events Rules) will be overwritten! Finally, the device will be rebooted.

Please confirm with your password to start the restore of Device Settings.

•••••

4. Enter the admin password, then click Restore.

A device settins pop-up appears.



Device Settings

The device will be reset in a few seconds.

You will be redirected to the login page within 116 seconds.

If redirection does not work, use this link to the login page.

5. Wait until the PDU resets and the Login page re-appears, indicating that the restore is complete.

Note: On startup, the PDU performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

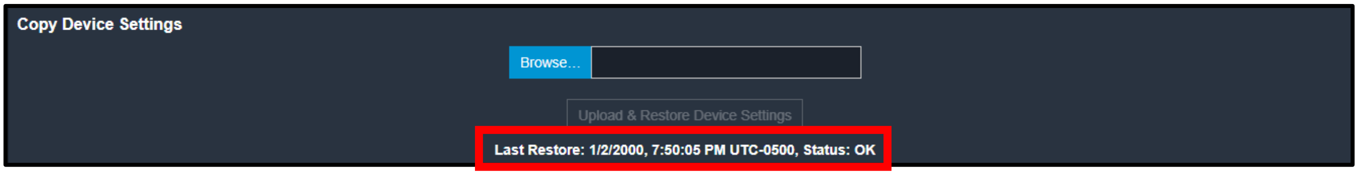
Viewing the Last Configuration Copying Record

▶ To view the last configuration copying record:

1. Choose Maintenance > Backup/Restore.

   The Backup/Restore page appears.

2. After copying a bulk configuration or device backup file to the PDU, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.



Copy Device Settings

Last Restore: 1/2/2000, 7:50:05 PM UTC-0500, Status: OK

Understanding Alternative Backup/Restore Methods

▶ Backup/Restore method alternatives:

To use a different method to perform backup/restore, refer to:

- ***Backup and Restore via SCP*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.

Network Diagnostics

The PDU provides the following tools in the web interface for diagnosing potential networking issues.

- Ping: The tool is useful for checking whether a host is accessible through the network or Internet.
- Trace Route: The tool lets you find out the route over the network between two hosts or systems.
- List TCP Connections: You can use this function to display a list of TCP connections.

Tip: These network diagnostic tools are also available through CLI. See ***Network Troubleshooting*** *in the Premium+ PDU With RackLink Advanced User Manual at* ***www.middleatlantic.com****.*

Choose Maintenance > Network Diagnostics, and then perform any function below.

Running a Ping Request

▶ To run a Ping request:

1. Choose Maintenance > Network Diagnostics.

   The Network Diagnostics page appears.

2. In the Ping section of the page, type values in the following fields.

Field	Description
Network Host	The name or IP address of the host that you want to check.
Number of Requests	A number up to 20. This determines how many packets are sent for pinging the host.

3. Click Run Ping to ping the host.
4. The Ping results then appear in a pop-up.

Running a Trace Route

▶ To run a Trace Route:

1. Choose Maintenance > Network Diagnostics.

   The Network Diagnostics page appears.

2. In the Trace Route section of the page, type values in the following fields.

Field or Setting	Description
Host Name	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation.

Field or Setting	Description
Use ICMP Packets	Select this checkbox to use the Internet Control Message Protocol (ICMP) packets to perform the trace route command.

3. Click Run.
4. The Trace Route results then appear in a pop-up.

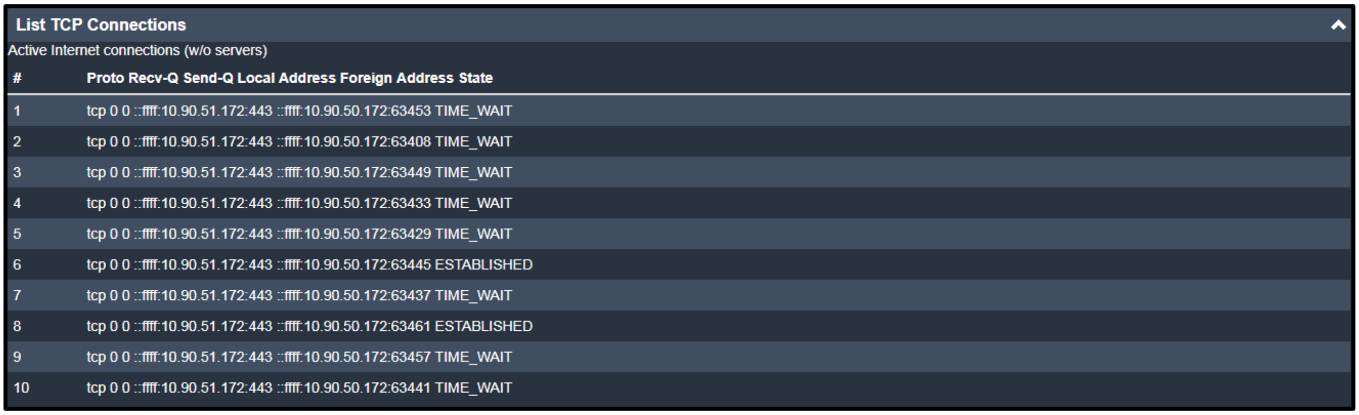
Listing TCP Connections

▶ To list TCP Connections:

1. Choose Maintenance > Network Diagnostics.

   The Network Diagnostics page appears.

2. Click the List TCP Connections title bar to show the list.



Active Internet connections (w/o servers)

#	Proto Recv-Q Send-Q Local Address Foreign Address State
1	tcp 0 0 ::ffff:10.90.51.172:443 ::ffff:10.90.50.172:63453 TIME_WAIT
2	tcp 0 0 ::ffff:10.90.51.172:443 ::ffff:10.90.50.172:63408 TIME_WAIT
3	tcp 0 0 ::ffff:10.90.51.172:443 ::ffff:10.90.50.172:63449 TIME_WAIT
4	tcp 0 0 ::ffff:10.90.51.172:443 ::ffff:10.90.50.172:63433 TIME_WAIT
5	tcp 0 0 ::ffff:10.90.51.172:443 ::ffff:10.90.50.172:63429 TIME_WAIT
6	tcp 0 0 ::ffff:10.90.51.172:443 ::ffff:10.90.50.172:63445 ESTABLISHED
7	tcp 0 0 ::ffff:10.90.51.172:443 ::ffff:10.90.50.172:63437 TIME_WAIT
8	tcp 0 0 ::ffff:10.90.51.172:443 ::ffff:10.90.50.172:63461 ESTABLISHED
9	tcp 0 0 ::ffff:10.90.51.172:443 ::ffff:10.90.50.172:63457 TIME_WAIT
10	tcp 0 0 ::ffff:10.90.51.172:443 ::ffff:10.90.50.172:63441 TIME_WAIT

Downloading Diagnostic Information

Important: This function is used by MAP Technical Support for assistance and troubleshooting.

You can download the diagnostic file from the PDU to a client machine. The file is compressed into a .tgz file and should be sent to Technical Support for interpretation.

This feature is accessible only by users with Administrative Privileges or Unrestricted View Privileges.

▶ To retrieve a diagnostic file:

1. Choose Maintenance > Download Diagnostic.

   The Download Diagnostic page appears.

2. Click .

3. The system prompts you to save or open the file. Click Save.
4. Email this file as instructed by Technical Support.

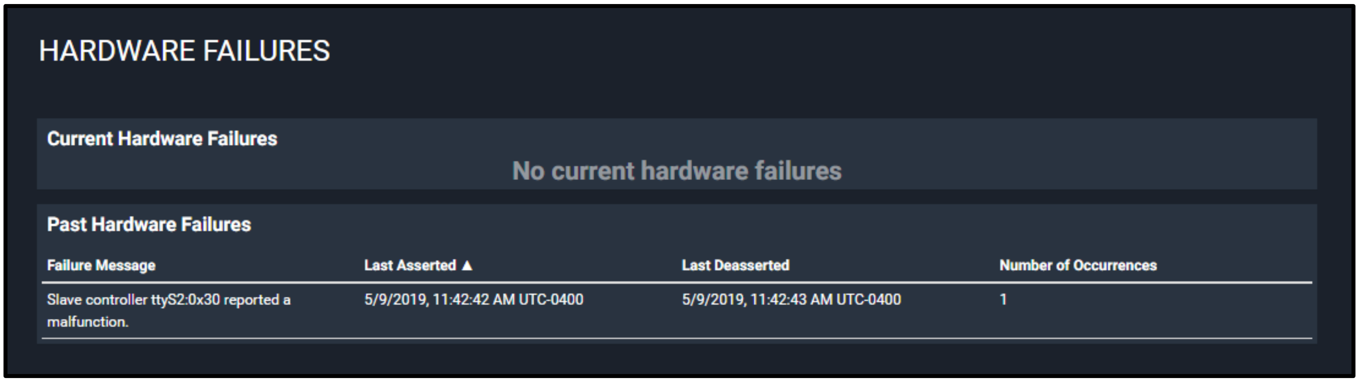
Viewing Hardware Failures

Using the web interface, you can view any hardware issues your PDU has detected, including current and past occurrences.

▶ To display hardware failure information:

1. Choose Maintenance > Hardware Failures.

   The Hardware Failures page appears.



HARDWARE FAILURES

Current Hardware Failures

No current hardware failures

Past Hardware Failures

Failure Message	Last Asserted ▲	Last Deasserted	Number of Occurrences
Slave controller ttyS2:0x30 reported a malfunction.	5/9/2019, 11:42:42 AM UTC-0400	5/9/2019, 11:42:43 AM UTC-0400	1

The page is divided into Current Hardware Failures and Past Hardware Failure sections.

Note: Current hardware failures, if any, also appear on the Alarms section of the dashboard. See ***Alarms*** *(on page 30).*

Hardware issues	Description
Network device not detected	A specific networking interface of the PDU is not detected.
I2C Bus stuck	A specific I2C bus is stuck, which affects the communication with sensors.
Slave controller not reachable	Communication with a specific slave controller fails.
Slave controller malfunction	A specific slave controller does not work properly.
Outlet power state inconsistent	The physical power state of a specific outlet is different from the chosen power state set by the software.

Resetting Your PDU via Unit Reset

You can remotely reboot the PDU via the web interface.

Resetting the PDU does not interrupt the operation of connected components because there is no loss of power to outlets.

During and after the reboot, outlets that have been powered on prior to the reboot remain powered on, and outlets that have been powered off remain powered off.

Rebooting the PDU

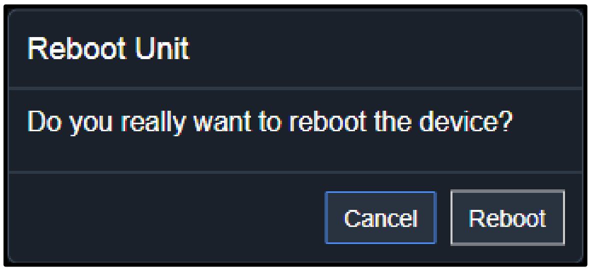
▶ **To reboot the PDU:**

1. Choose Maintenance > Unit Reset.

   The Unit Reset page appears.

2. Click > Reboot Unit.

   A pop-up appears asking you to confirm the reboot.

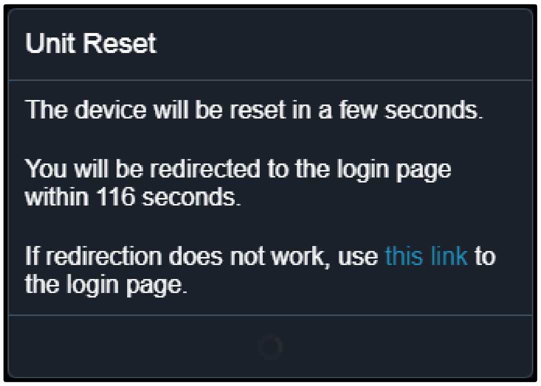


Reboot Unit

Do you really want to reboot the device?

3. Click Reboot.

   A pop-up appears with a message and countdown timer showing the remaining time of the operation. It takes about one minute to complete.



Unit Reset

The device will be reset in a few seconds.

You will be redirected to the login page within 116 seconds.

If redirection does not work, use this link to the login page.

4. When the restart is complete, the login page appears.

Note: If you are not redirected to the login page after the restart is complete, click the text "this link" in the countdown message.

Resetting All Settings to Factory Defaults

You must have the Administrator Privileges to reset all settings of the PDU to factory defaults.

Important: Exercise caution before resetting the PDU to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and other settings. Only active energy data and firmware upgrade history are retained.

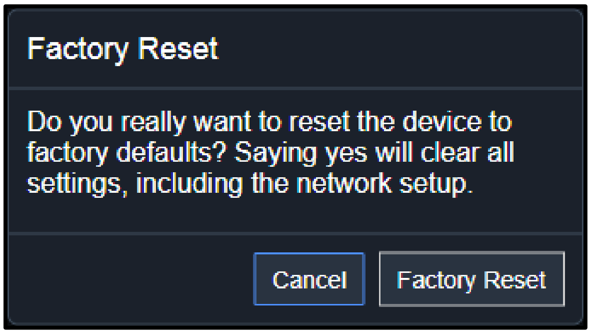
▶ To reset the device to factory defaults:

1. Choose Maintenance > Unit Reset

   The Unit Reset page appears.

2. Click Reset to Factory Defaults.

   A pop-up appears.

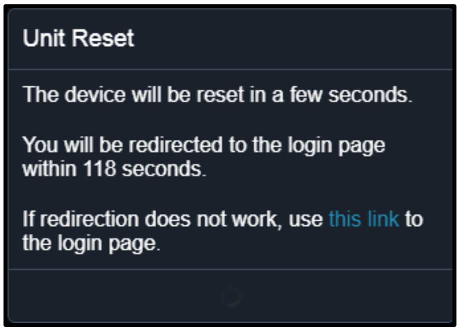


Factory Reset

Do you really want to reset the device to factory defaults? Saying yes will clear all settings, including the network setup.

3. Click Factory Reset to reset the PDU to factory defaults.

   A pop-up appears with a message and countdown timer showing the remaining time of the operation. It takes about two minutes to complete.



Unit Reset

The device will be reset in a few seconds.

You will be redirected to the login page within 118 seconds.

If redirection does not work, use this link to the login page.

4. When the reset is complete, the login page appears.

Note: If you are not redirected to the login page after the reset is complete, click the text "this link" in the countdown message.

Understanding Alternative Reset Methods

▶ Reset method alternatives:

There are two more methods to reset the device to factory defaults.

- Use the "mechanical" reset button
- Perform the CLI command

For details, see Appendix B: Resetting to Factory Defaults (on page 205).

Retrieving Software Package Information via About PDU

You can check the current firmware version and the information of all open source packages embedded in the PDU through the web interface.

▶ To retrieve the embedded software package information:

1. Choose Maintenance > About PDU

   The About PDU page appears.

2. A list of open source packages is displayed.
3. You can click any link to access related information or download any software package.

PDU

The PDU's generic information and PDU-level global settings are available on the PDU page.

To open the PDU page, click 'PDU' in the *Menu* (on page 27).

Viewing PDU Details

▶ Device information shown:

- Firmware version
- Serial number
- MAC address
- Rating

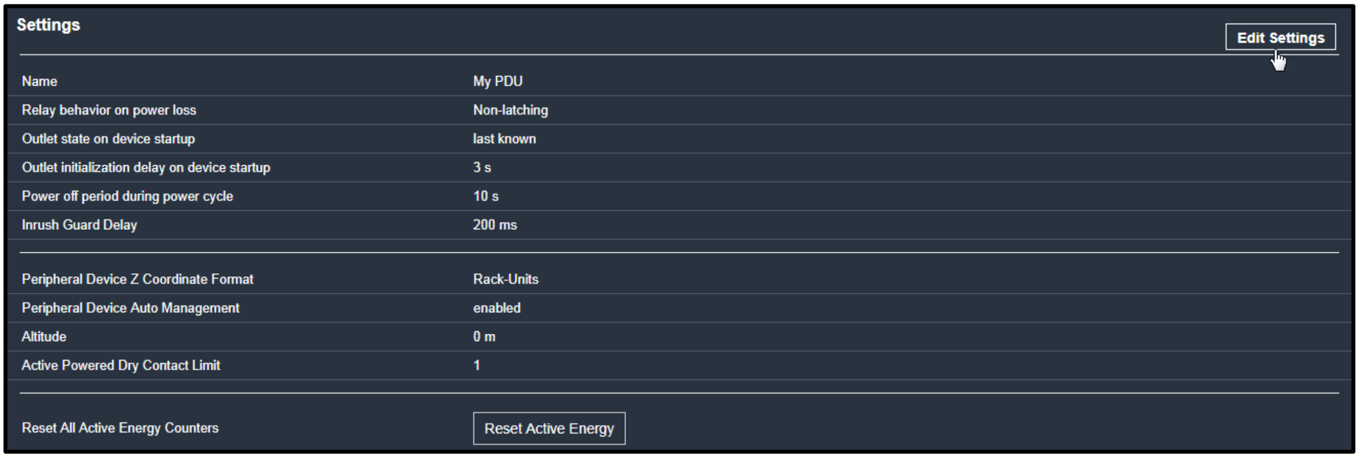
Configuring Global Settings

▶ To configure global settings:

1. Choose PDU

The About PDU page appears.

2. Click Edit Settings.



Settings

Name	My PDU
Relay behavior on power loss	Non-latching
Outlet state on device startup	last known
Outlet initialization delay on device startup	3 s
Power off period during power cycle	10 s
Inrush Guard Delay	200 ms
Peripheral Device Z Coordinate Format	Rack-Units
Peripheral Device Auto Management	enabled
Altitude	0 m
Active Powered Dry Contact Limit	1
Reset All Active Energy Counters	Reset Active Energy

3. Now you can configure the fields.
4. Click ⬍ to select an option.
5. Select or deselect the checkbox.
6. Adjust the numeric values.
7. For time-related fields, if option selection using ⬍ is not preferred, the value must include a time unit, such as '50 s'. See ***Time Units*** (on page 188).

Field	Function	Note
Name	Customizes the device name.	
Relay behavior on power loss	Selects an operating mode to determine the latching relay behavior when PDU power is lost. • *Options: Non-latching and Latching* • *Non-latching has all relays open at the power loss while latching may have the relays closed.*	See ***PDU Latching Relay Behavior*** (on page 187).

Field	Function	Note
Outlet state on device startup	Determines the initial power state of ALL outlets after the PDU powers up. - *Options: on, off, and last known* See ***Options for Outlet State on Startup*** (on page 188).	- After removing power from the PDU, you must wait for a minimum of 10 seconds before powering it up again. Otherwise, the default outlet state settings may not work properly. - You can override the global outlet state setting on a per-outlet basis so specific outlets behave differently on startup. See ***Outlet Configuration Page*** (on page 42).
Outlet initialization delay on device startup	Determines how long the PDU waits before providing power to all outlets during power cycling or after recovering from a temporary power loss. - *Range: 1 second to 1 hour*	See ***Initialization Delay Use Cases*** (on page 188).
Power off period during power cycle	Determines the power-off period after the outlet is switched OFF during a power cycle. - *Range: 1 second to 1 hour*	- Power cycling the outlet(s) turns the outlet(s) off and then back on. - You can override this global power cycle setting on a per-outlet basis so specific outlets' power-off period is different. See ***Outlet Configuration Page*** (on page 42).
Inrush Guard Delay	Prevents a circuit breaker trip due to inrush current when many devices connected to the PDU are turned on. - *Range: 100 milliseconds to 2 seconds*	

Field	Function	Note
Peripheral Device Z Coordinate Format	Determines how to describe the vertical locations (Z coordinates) of environmental sensor packages. - *Options: Rack-Units and Free-Form*	- Rack Units: The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors or dry contacts. - Free-Form: Any alphanumeric string can be used for specifying the Z coordinate. The value can be 0 to 24 characters long.
Peripheral Device Auto Management	Enables or disables the automatic management feature for environmental sensor packages. - *The default is to enable it.*	See ***How the Automatic Management Function Works*** (on page 188).
Altitude	Provide an altitude value in feet or meters (depending on your configured preferences).	
Active Powered Dry Contact Limit	This value is the maximum number of allowed powered dry contact sensors connected to your PDU.	Setting this value lower than the number of connected sensors limits how many are controllable in your system. This is available in order to limit power consumption.

8. Click Save.

Resetting Active Energy Counters

To reset ALL active energy counters:

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

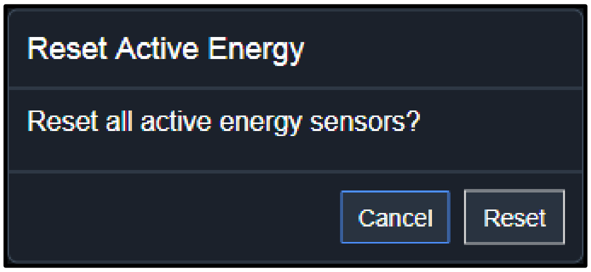
Only users with the "Admin" role assigned can reset active energy readings.

1. Choose PDU

   The About PDU page appears.

2. Click .

A pop-up appears confirming the reset.



Reset Active Energy

Reset all active energy sensors?

4. Click Reset.
5. All active energy readings on this PDU are reset to zero.

Tip: You can choose to reset the active energy reading of an individual inlet or outlet. See ***Inlet*** *(on page 189) or* ***Outlet Configuration Page*** *(on page 42).*

PDU Latching Relay Behavior

The PDU incorporates latching relays in models with outlet switching. Unlike non-latching relays, latching relays do NOT require power to keep their contacts closed.

PDU outlet switching can be configured to operate as a true latching relay or to simulate a non-latching relay. The operating mode determines the latching relay behavior when PDU power is lost. Regardless of which mode is selected, power is not required to keep relay contacts closed.

▶ Non-Latching Mode:

- Relay always opens when power is lost. This insures all relays are open when power is applied to the PDU.
- Always select this mode if the combined in-rush current of the devices connected to the PDU trip circuit breakers when power is applied to the PDU.
- This is the factory default operating mode.

▶ Latching Mode:

- Relay does not open when power is lost.
- This is the preferred operating mode ONLY if you are sure in-rush current does not trip circuit breakers when power is applied to the PDU.
- Power to the outlet is not disrupted if a PDU internal failure occurs.
- In Latching mode, the following features are disabled.
  - PDU-level outlet state on startup: See ***Options for Outlet State on Startup*** (on page 188).
  - Outlet-level outlet state on startup: See ***Outlet Controls*** (on page 40).

- PDU-level outlet initialization delay on startup: See ***Options for Outlet State on Startup*** (on page 188).

Options for Outlet State on Startup

The following are available options for initial power states of outlets after powering up the PDU.

Option	Function
on	Turns on the outlet(s).
off	Turns off the outlet(s).
last known	Restores the outlet(s) to the previous power state(s) before the PDU was powered off.

Initialization Delay Use Cases

Apply the initialization delay in either of the following scenarios.

- When power may not initially be stable after being restored
- When UPS batteries may be charging

Tip: When there are a large number of outlets, set the value to a lower number so that you can avoid a long wait before all outlets are available.

How the Automatic Management Function Works

After enabling the automatic management function:

When the total number of managed sensors and dry contacts has not reached the upper limit yet, the PDU automatically brings newly connected environmental sensors and dry contacts under management after detecting them.

A PDU can manage up to 32 sensors/dry contacts.

After disabling the automatic management function:

The PDU no longer automatically manages any newly added environmental sensors and dry contacts, and therefore neither ID numbers are assigned nor sensor readings or states are available for newly added ones.

You must manually manage new sensors/dry contacts. See ***Peripherals*** (on page 57).

Time Units

If you choose to type a new value in the time-related fields, such as the Inrush Guard Delay field, you must add a time unit after the numeric value. For example, you can type '15 s' for 15 seconds.

Note that different fields have different range of valid values.

Time units:

Unit	Time
ms	millisecond(s)
s	second(s)
min	minute(s)
h	hour(s)
d	day(s)

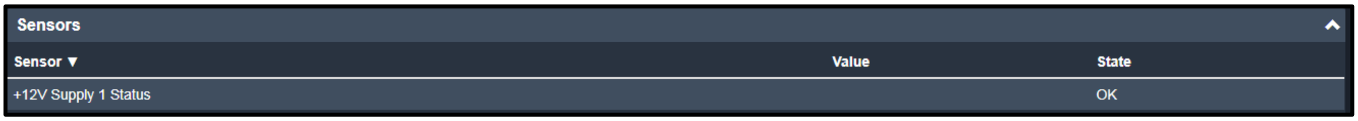
Viewing PDU Sensor Power Information

To view PDU sensor power information:

1. Choose PDU

   The About PDU page appears.

2. Click the Sensors title bar to display sensor power information as follows:



Sensors

Sensor ▼	Value	State
+12V Supply 1 Status		OK

3. The PDU's internal 12V power supply status appears here.

Inlet

You can view all inlet information, configure inlet-related settings, or reset the inlet active energy on the Inlet page. To open this page, click 'Inlet' in the *Menu* (on page 27).

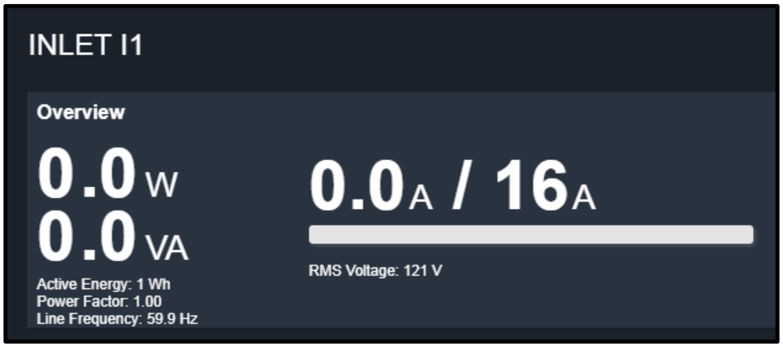
Inlet thresholds, when enabled, help you identify whether the inlet enters the warning or critical level. In addition, you can have the PDU automatically generate alert notifications for any warning or critical status. See *Event Rules and Actions* (on page 120).

Inlet Overview

Generic inlet overview information shown:

1. Choose Inlet.

   The Inlet page appears.



INLET I1

Overview

0.0 W
0.0 VA

Active Energy: 1 Wh
Power Factor: 1.00
Line Frequency: 59.9 Hz

0.0A / 16A

RMS Voltage: 121 V

- The left side of the Overview section of the screen lists the following data:
  - Active power (kW or W)
  - Apparent power (kVA or VA)
  - Active energy (kWh or Wh)
  - Power factor
  - Line frequency (Hz)
  - The right side shows the current and voltage data per phase. For a single-phase device, it shows only one line, but for a three phase device, it shows three lines (L1, L2, and L3).
  - Inlet data from top to bottom includes:
  - RMS current (A)
  - A bar showing the RMS current level
  - RMS voltage (V)
  - The RMS current bar automatically changes color to indicate the current status (if the thresholds have been enabled).

Status	Bar colors
normal	🟩
above upper warning	🟨
above upper critical	🟥

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

Inlet Sensors

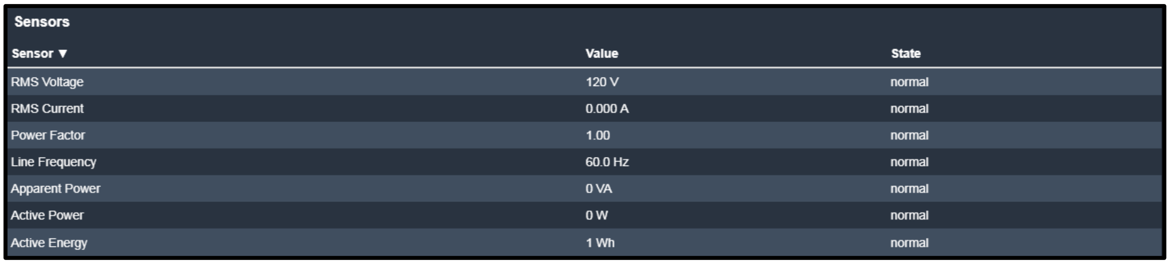
▶ To view inlet sensor information:

1. Choose Inlet.

   The Inlet page appears.

2. View inlet sensor information as follows:

   If desired, you can sort the list by clicking the desired column header. See ***Sorting a List*** (on page 28).



Sensors

Sensor ▼	Value	State
RMS Voltage	120 V	normal
RMS Current	0.000 A	normal
Power Factor	1.00	normal
Line Frequency	60.0 Hz	normal
Apparent Power	0 VA	normal
Active Power	0 W	normal
Active Energy	1 Wh	normal

3. Sensor name, value, and state information is shown.

Inlet Settings

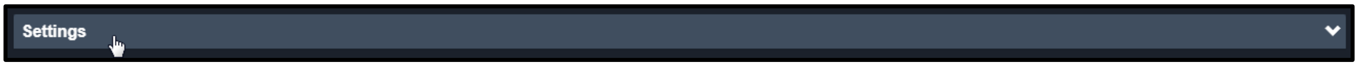
You can edit the Label, Name, and reset active energy settings, if desired.

▶ To customize the inlet's name:

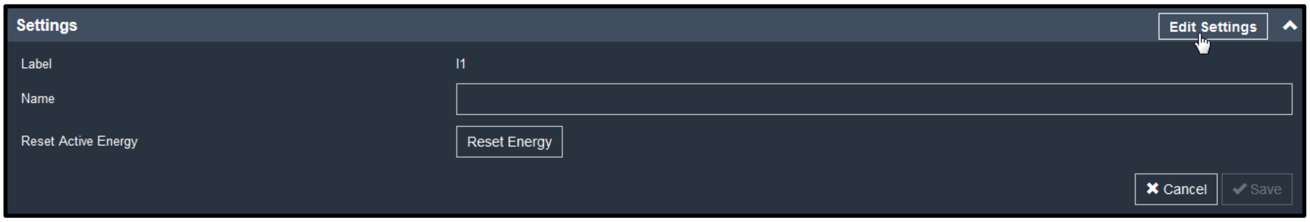
1. Choose Inlet.

   The Inlet page appears.

2. Click the Settings title bar as shown.



3. Click Edit Settings.



Label	I1
Name	
Reset Active Energy	Reset Energy

4. Type a name for the inlet.
   - For example, you can name it to identify the power source.
5. Click Save.
6. The inlet's custom name is displayed on the Inlet or Dashboard page, followed by its label in parentheses.

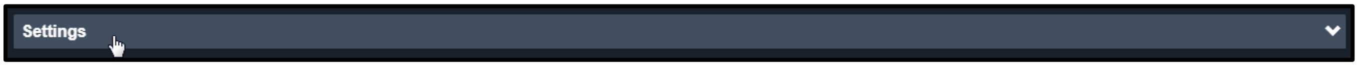
To reset the inlet's active energy counter:

Only users with the "Admin" role assigned can reset active energy readings.

1. Choose Inlet.

   The Inlet page appears.

2. Click the Settings title bar as shown.



3. Click .

4. Click Reset on the confirmation message.

   This inlet's active energy reading is then reset to zero.

---

*Tip: To reset ALL active energy counters on the PDU, see **PDU** (on page 183).*

Summary in the section title:

Information in parentheses adjacent to the title is the total number of alerted sensors.

For example:

- **1 Critical**: 1 sensor enters the critical or alarmed state.

  Numeric sensors enter the critical state.

  State sensors enter the alarmed state.

- **1 Warned**: 1 'numeric' sensor enters the warning state.

List of alerted sensors:

Two icons are used to indicate various sensor states.

Icons	Sensor states
⚠	For numeric sensors: • above upper warning • below lower warning

Icons	Sensor states
⚠	For numeric sensors: • above upper critical • below lower critical
	For state sensors: • alarmed state

For details, see ***Sensor/Dry Contact States*** (on page 64).

Inlet History

The Inlet history section behaves in the same manner as the outlets; however, the readings pertain to the total system power usage. For more information, see ***Oulet History*** on page 49.

Inlet Thresholds

1. The Inlet thresholds section behaves in the same manner as the outlets; however, the readings pertain to the total system power usage. For more information, see ***Outlet Thresholds*** on page 50.

Chapter 4: Using SNMP

This SNMP section helps you set up the PDU for use with an SNMP manager. The PDU can be configured to send traps or informs to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

Enabling and Configuring SNMP

To communicate with an SNMP manager, you must enable SNMP protocols on the PDU. By default the "read-only" mode of SNMP v1/v2c is enabled.

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, you must configure the users with the SNMP v3 access permission and set Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between SNMP and the PDU.

Important: You must download the SNMP MIB for your PDU to use with your SNMP manager. See *Downloading SNMP MIB* (on page 196).

▶ To enable SNMP v1/v2c and/or v3 protocols:

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent section, enable SNMP v1/v2c or SNMP v3, and configure related fields, such as the community strings.
3. If SNMP v3 is enabled, you must determine which users shall have the SNMP v3 access permission. See below.

   For details, see *Configuring SNMP Settings* (on page 92).

▶ To configure users for SNMP v3 access:

1. Choose User Management > Users.
2. Create or modify users to enable their SNMP v3 access permission.
3. If authentication and privacy is enabled, configure the SNMP password(s) in the user settings.

   For details, see *Creating Users* (on page 72).

▶ To enable SNMP notifications:

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Notifications section, enable the SNMP notification feature, and configure related fields. For details, see:

   SNMPv2c Notifications (on page 195).

SNMPv3 Notifications (on page 195).

Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See ***Available Actions*** *(on page 132).*

SNMPv2c Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the Enable SNMP Notifications checkbox is selected.
4. Select SNMPv2c Trap or SNMPv2c Inform as the notification type.
5. Type values in the following fields.

Field	Description
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. • For example, resend a new inform communication once every 3 seconds.
Number of Retries	The number of times you want to resend the inform communication if it fails. • For example, inform communications are resent up to 5 times when the initial communication fails.
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent. You can specify up to 3 SNMP destinations.
Port	The port number used to access the device(s).
Community	The SNMP community string to access the device(s). The community is the group representing the PDU and all SNMP management stations.

6. Click Save.

SNMPv3 Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the Enable SNMP Notifications checkbox is selected.
4. Select SNMPv3 Trap or SNMPv3 Inform as the notification type.

5. For SNMP TRAPs, the engine ID is prepopulated.
6. Type values in the following fields.

Field	Description
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent.
Port	The port number used to access the device(s).
User ID	User name for accessing the device. • Make sure the user has the SNMP v3 access permission.
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. • For example, resend a new inform communication once every 3 seconds.
Number of Retries	Specify the number of times you want to resend the inform communication if it fails. • For example, inform communications are resent up to 5 times when the initial communication fails.
Security Level	Three types are available. • noAuthNoPriv - neither authentication nor privacy protocols are needed. • AuthNoPriv - only authentication is required. • authPriv - both authentication and privacy protocols are required.
Authentication Protocol, Authentication Passphrase, Confirm Authentication Passphrase	The three fields are available when the security level is set to AuthNoPriv or authPriv. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
Privacy Protocol, Privacy Passphrase, Confirm Privacy Passphrase	The three fields are available when the security level is set to authPriv. • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

7. Click Save.

Downloading SNMP MIB

You must download an appropriate SNMP MIB file for successful SNMP communications. Always use the latest SNMP

MIB downloaded from the current firmware of your PDU.

You can download the MIBs from two different pages of the web interface.

▶ MIB download via the SNMP page:

1. Choose Device Settings > Network Services > SNMP.
2. Click the Download MIBs title bar.

3. Select the desired MIB file to download.
   - RLNK-MIB file for PDU power management.
4. Click Save to save the file onto your computer.

▶ MIB download via the Device Information page:

1. Choose Maintenance > Device Information.
2. In the Information section, click the desired download link:
   - RLNK-MIB file for PDU power management.
3. Click Save to save the file onto your computer.

SNMP Gets and Sets

In addition to sending notifications, the PDU is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the PDU, such as the system location, and the current on a specific outlet.
- Set requests are used to configure a subset of the information, such as the SNMP system name.

Note: The SNMP system name is the PDU name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The PDU does NOT support configuring IPv6-related parameters using the SNMP set requests.

Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom PDU MIB.

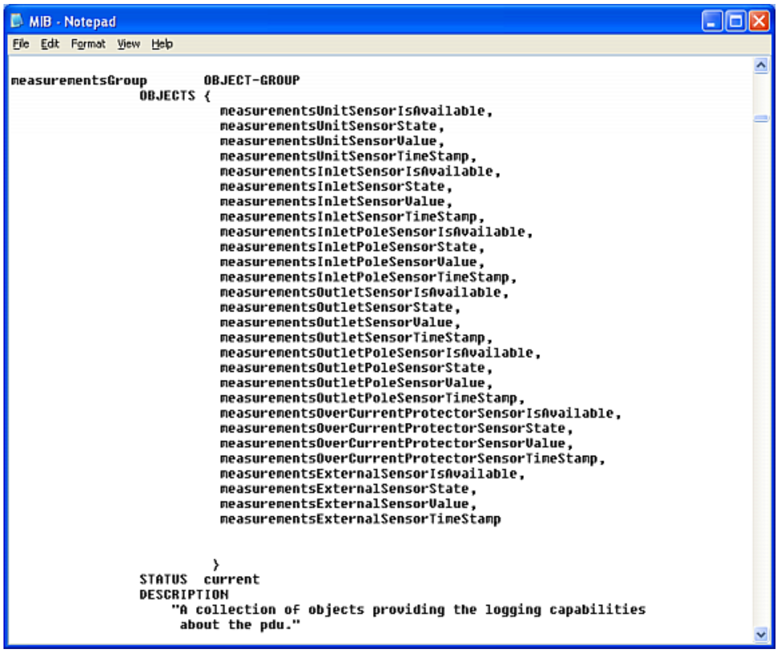
The PDU MIB

The SNMP MIB file is required for using your PDU with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Layout

Opening the MIB reveals the custom objects that describe the system at the unit level as well as at the individual outlet level.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.



```
measurementsGroup        OBJECT-GROUP
                 OBJECTS {
                           measurementsUnitSensorIsAvailable,
                           measurementsUnitSensorState,
                           measurementsUnitSensorValue,
                           measurementsUnitSensorTimeStamp,
                           measurementsInletSensorIsAvailable,
                           measurementsInletSensorState,
                           measurementsInletSensorValue,
                           measurementsInletSensorTimeStamp,
                           measurementsInletPoleSensorIsAvailable,
                           measurementsInletPoleSensorState,
                           measurementsInletPoleSensorValue,
                           measurementsInletPoleSensorTimeStamp,
                           measurementsOutletSensorIsAvailable,
                           measurementsOutletSensorState,
                           measurementsOutletSensorValue,
                           measurementsOutletSensorTimeStamp,
                           measurementsOutletPoleSensorIsAvailable,
                           measurementsOutletPoleSensorState,
                           measurementsOutletPoleSensorValue,
                           measurementsOutletPoleSensorTimeStamp,
                           measurementsOverCurrentProtectorSensorIsAvailable,
                           measurementsOverCurrentProtectorSensorState,
                           measurementsOverCurrentProtectorSensorValue,
                           measurementsOverCurrentProtectorSensorTimeStamp,
                           measurementsExternalSensorIsAvailable,
                           measurementsExternalSensorState,
                           measurementsExternalSensorValue,
                           measurementsExternalSensorTimeStamp


                          }
                 STATUS  current
                 DESCRIPTION
                     "A collection of objects providing the logging capabilities
                      about the pdu."
```

For example, the measurementsGroup group contains objects for sensor readings of the PDU as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor value". pduRatedCurrent, part of the configGroup group, describes the PDU current rating.

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, which causes the PDU to generate a warning and send an SNMP notification when certain parameters are exceeded. For more information, see ***Sensor Threshold Settings*** (on page 51).

Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than theupper warning threshold.

Configuring NTP Server Settings

Using SNMP, you can change the following NTP server-related settings in the unitConfigurationTable:

- Enable or disable synchronization of the device's date and time with NTP servers (synchronizeWithNTPServer)
- Enable or disable the use of DHCP-assigned NTP servers if synchronization with NTP servers is enabled (useDHCPProvidedNTPServer)
- Manually assign the primary NTP server if the use of DHCP-assigned NTP servers is disabled (primaryNTPServerAddressType and primaryNTPServerAddress)
- Manually assign the secondary NTP server (optional) (secondaryNTPServerAddressType and secondaryNTPServerAddress)

*Tip: To specify the time zone, use the CLI or web interface instead. For the CLI, refer to **Setting the Time Zone** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com. For the web interface, see **Setting the Date and Time** (on page 118).*

When using the SNMP SET command to specify or change NTP servers, it is required that both the NTP server's address type and address be set in the command line simultaneously.

For example, the SNMP command to change the primary NTP server's address from IPv4 (192.168.84.84) to host name looks similar to the following:

```
snmpset -v2c -c private 192.168.84.84 firstNTPServerAddressType = dns firstNTPServerAddress
= "angu.pep.com"
```

Retrieving Energy Usage

You can discover how much energy a device consumes by retrieving the Active Energy for the outlet the device is plugged into. The Active Energy values are included in the outletSensorMeasurementsTable, along with other outlet sensor readings.

A Note about Enabling Thresholds

When enabling previously disabled thresholds via SNMP, make sure you set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

Appendix A: Specifications

Dimensions

Model	Length, Width, Height
Rackmount (RLNK-P915R, RLNK-P915R-SP, RLNK-P920R, RLNK-P920R-SP)	20.75” x 15.25” x 3.50” (527mm x 387mm x 89mm)
Compact (RLNK-P415, RLNK-P420)	14” x 9.75” x 4.75” (356mm x 248mm x 121mm)

Weight

Model	Weight
Rackmount (RLNK-P915R, RLNK-P920R)	13.2 lbs. (6 kg)
Rackmount (RLNK-P915R-SP, RLNK-P920R-SP)	12.4 lbs. (5.62 kg)
Compact (RLNK-P415, RLNK-P420)	6.6 lbs. (3 kg)

Maximum Ambient Operating Temperature

The maximum ambient operating temperature (TMA) for the PDU varies from 25 to 35 degrees Celsius, depending on the model and certification standard.

Specification	Measurement
Max Ambient Temperature	25 to 35 degrees Celsius

Electrical Specifications

Specification	Measurement
Operating Voltage	80 – 135 (120 NOM)
Current MAX	15 – 20 A

Specification	Measurement
Current Continuous	12 – 16 A
Idle Power Consumption	<10 W
*VPR for Series Surge Protection	330V L-N
*VPR for MOV	600V L-N
MOV P Current	36,000 A
MOV Joule Rating	634 Joules
Filter Specifications for Roll Off Series Surge Protection	Cutoff Frequency: 19kHz, -40dB/Decade (-28dB@100kHz)
Filter Specifications for Roll Off MOV	Cutoff Frequency: 50kHz, -20dB/decade (-28dB@1MHz)
Operating Frequency	60 Hz
UL/CSA Standard	UL/CSA C22.2 No. 60950-1
FCC/IC Class	Class B

*Surge tests based on the operating duty cycle test method per UL 1449.

Serial RS-232 "RJ-45" Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	RTS	Output	Request to send
2	DTR	Output	Data terminal ready
3	TxD	Output	Transmit data
4	GND	–	Signal ground
5	DCD	Input	Data
6	RxD	Input	Receive data (data in)
7	DSR	Input	Data set ready
8	CTS	Input	Clear to send

RJ45-to-DB9 Cable Requirements for Computer Connections

An RJ45-to-DB9 adapter/cable is required for connecting the PDU to a computer, if the use of a USB cable is not intended.

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

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

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

DB9 pin signal	DB9 pin No.	RJ-45 pin No.	RJ-45 pin signal
CTS	8	1	RTS
DSR	6	2	DTR
RxD	2	3	TxD
GND	5	4	GND
GND	5	5	GND
TxD	3	6	RxD
DTR	4	7	DSR
RTS	7	8	CTS
DCD	1 (Not connected)	N/A	
RI	9 (Not connected)		

Sensor RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	+12V	–	Power (fuse protected)
2	+12V	–	Power (fuse protected)
3	GND	–	Signal Ground
4	RS485_DP	bi-directional	Data Positive of the RS-485 bus

RJ-45 Pin/signal definition			
5	RS485_DN	bi-directional	Data Negative of the RS-485 bus
6	GND	–	Signal Ground
7	1-wire	–	Used for Feature Port
8	GND	–	Signal Ground

Note: A maximum of 500mA power is permitted for both pin 1 and pin 2 altogether.

Expansion RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	+12V	–	Power (fuse protected)
2	+12V	–	Power (fuse protected)
3	GND	–	Signal Ground
4	RS485_DP	bi-directional	Data Positive of the RS-485 bus
5	RS485_DN	bi-directional	Data Negative of the RS-485 bus
6	GND	–	Signal Ground
7	NC	–	No Connection
8	GND	–	Signal Ground

Feature RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DTR	Output	Reserved
2	GND	–	Signal Ground

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
3	+5V	–	Power for CIM (200mA, fuse protected) ⚠ **WARNING**: Pin 3 is only intended for use with Middle Atlantic Products devices. **AVERTISSEMENT**: La broche 3 est uniquement destinée à être utilisée avec les appareils Middle Atlantic Products.
4	TxD	Output	Transmit Data (Data out)
5	RxD	Input	Receive Data (Data in)
6	+12V	–	⚠ **WARNING**: Pin 6 is only intended for use with Middle Atlantic Products devices. Do not connect. **AVERTISSEMENT**: La broche 6 est uniquement destinée à être utilisée avec les appareils Middle Atlantic Products. Ne branchez pas.
7	GND	–	Signal Ground
8	DCD	Input	Reserved

Appendix B: Resetting to Factory Defaults

You can use either the reset button or the command line interface (CLI) to reset the PDU. For information about the CLI, refer to the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.

Important: Exercise caution before resetting the PDU to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and other settings. Only active energy data and firmware upgrade history are retained.

Alternative:

Another method to reset it to factory defaults is to use the web interface. See ***Resetting All Settings to Factory Defaults*** (on page 182).

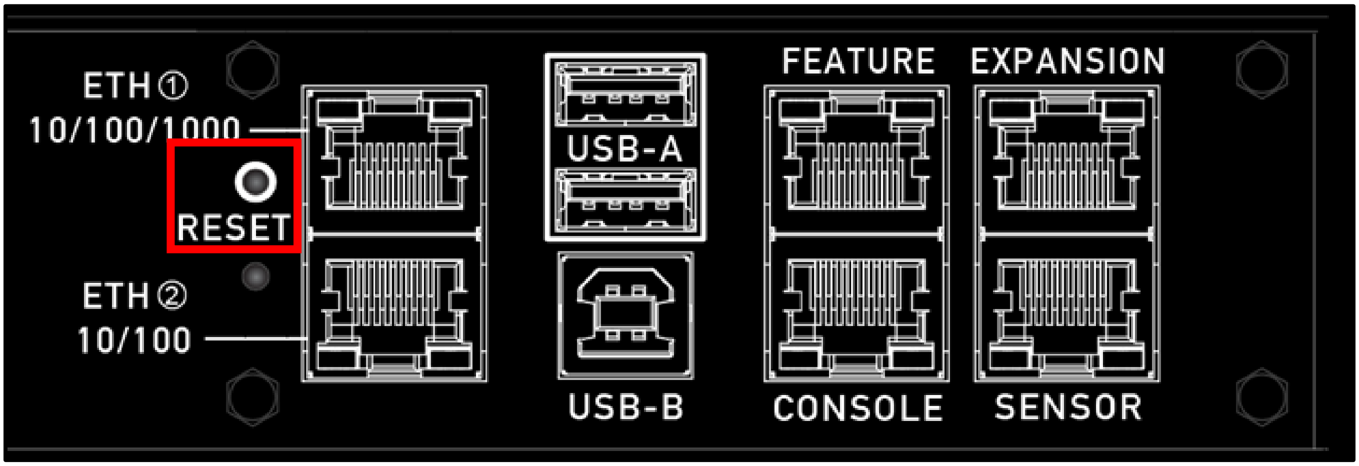
Using the Reset Button

An RS-232 serial connection to a computer is required for using the reset button.

To reset to factory defaults using the reset button:

1. Connect a computer to the PDU. Refer to ***Connecting the PDU to a Computer*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the PDU. For information on the serial port configuration, refer to Step 2 of ***Initial Network Configuration via CLI*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.
3. Press (and release) the Reset button of the PDU while pressing the Esc key of the keyboard several times in rapid succession. A prompt (=>) should appear after about one second.
4. Type *defaults* to reset the PDU to its factory defaults.
5. Wait until the Username prompt appears, indicating the reset is complete.

The reset button location:



Note: HyperTerminal is available on Windows operating systems prior to Windows Vista. For Windows Vista or later versions, you may use PuTTY, which is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

Using the CLI Command

The Command Line Interface (CLI) provides a reset command for restoring the PDU to factory defaults. For information on CLI, refer to ***Using the Command Line Interface*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.

▶ To reset to factory defaults after logging in to the CLI:

1. Connect to the PDU. Refer to ***Logging in to CLI*** or ***Connecting the PDU to a Computer*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com..
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the PDU. For information on the serial port configuration, refer to Step 2 of ***Initial Network Configuration via CLI*** in the Premium+ PDU With RackLink Advanced User Manual at www.middleatlantic.com.
3. Log in to the CLI by typing the user name "admin" and its password.
4. After the # system prompt appears, type either of the following commands and press Enter.

```
#     reset factorydefaults
```

-- OR --

```
#     reset factorydefaults /y
```

5. If you entered the command without "/y" in Step 4, a message appears prompting you to confirm the operation. Type y to confirm the reset.

6. Wait until the Username prompt appears, indicating the reset is complete.

After resetting to factory defaults, you must log into the system for the first time. For more information, see ***Changing Your Password on First Login*** (on page 23).

▶ To reset to factory defaults without logging in to the CLI:

The PDU provides an easier way to reset the product to factory defaults in the CLI prior to login.

1. Connect to the PDU and launch a terminal emulation program as described in the above procedure.
2. At the Username prompt in the CLI, type "factorydefaults" and press Enter.

   ```
   Username:  factorydefaults
   ```

3. Type y on a confirmation message to perform the reset.

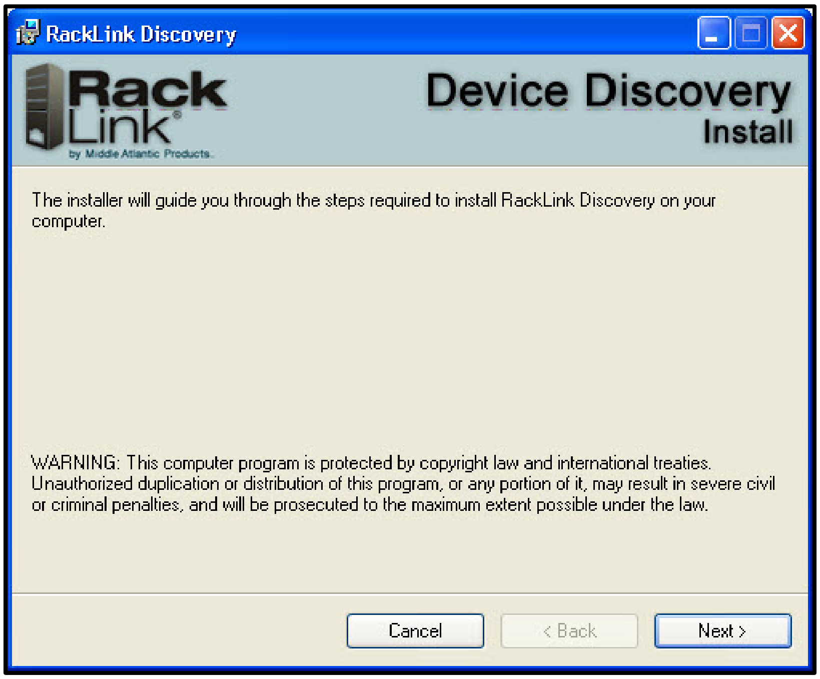
Appendix C: Installing the Device Discovery Software and Accessing a Connected PDU's Web Interface

Installing the RackLink Device Discovery Software on a PC:

▶ To install RackLink Device Discovery software on a PC:

1. Access www.middleatlantic.com.
2. Download and run the `RackLink Device Discovery setup.exe` file.

   The Device Discovery Setup dialog box appears.

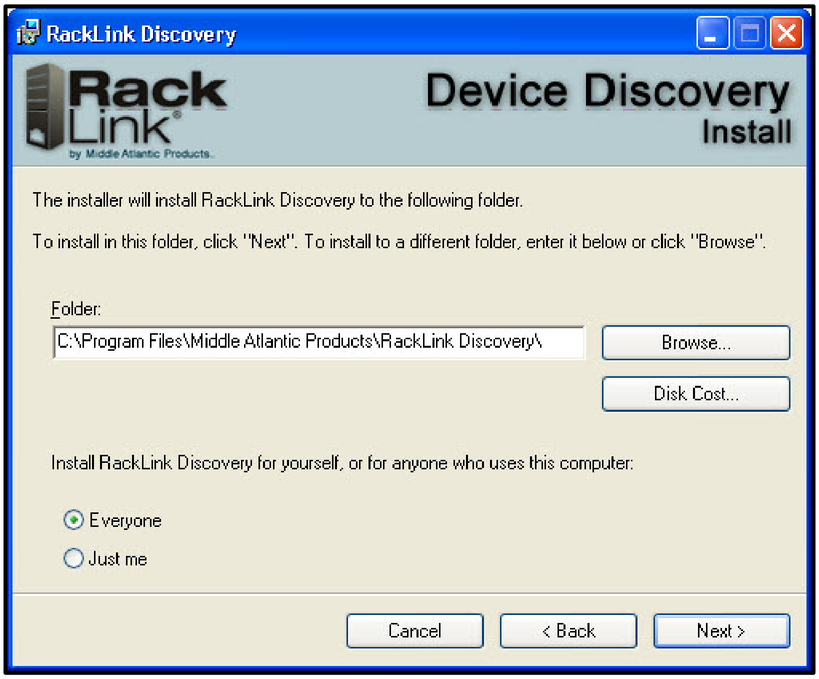


The installer will guide you through the steps required to install RackLink Discovery on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

3. Click Next.

Additional installation options appear.



The installer will install RackLink Discovery to the following folder.

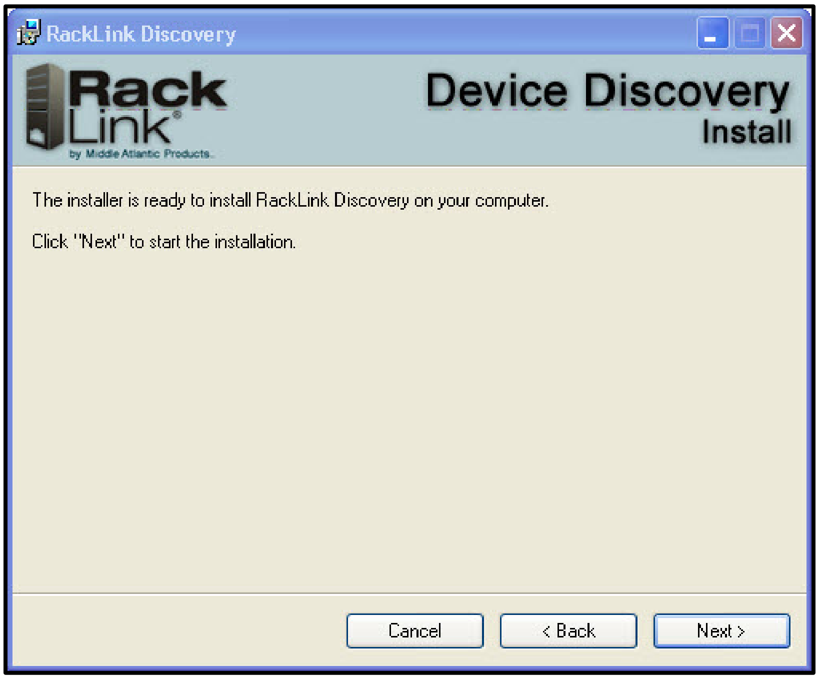
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:
C:\Program Files\Middle Atlantic Products\RackLink Discovery\

Install RackLink Discovery for yourself, or for anyone who uses this computer:

● Everyone
○ Just me

4. Click Browse if you wish to change the software installation folder.
5. If desired, select whether you want to install RackLink Discovery for everyone, or just the current user.
6. Click Next.

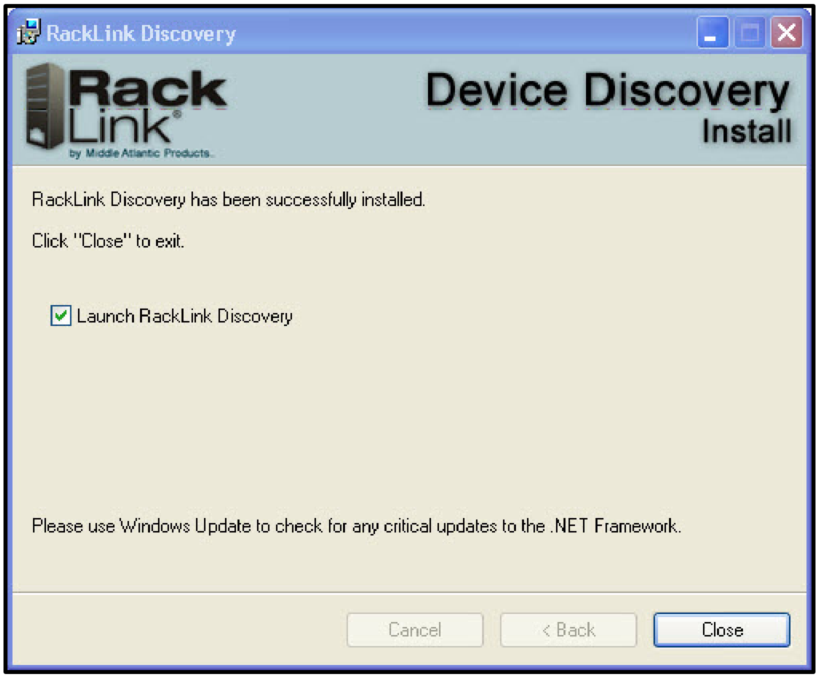


The installer is ready to install RackLink Discovery on your computer.

Click "Next" to start the installation.

The installer indicates that it's ready to install RackLink Discovery on your computer.

7. Click Next to begin the installation.



RackLink Discovery has been successfully installed.

Click "Close" to exit.

☑ Launch RackLink Discovery

Please use Windows Update to check for any critical updates to the .NET Framework.

The installer indicates that RackLink Discovery has been successfully installed and provides a default check box selection to Launch RackLink Discovery after closing the installer.

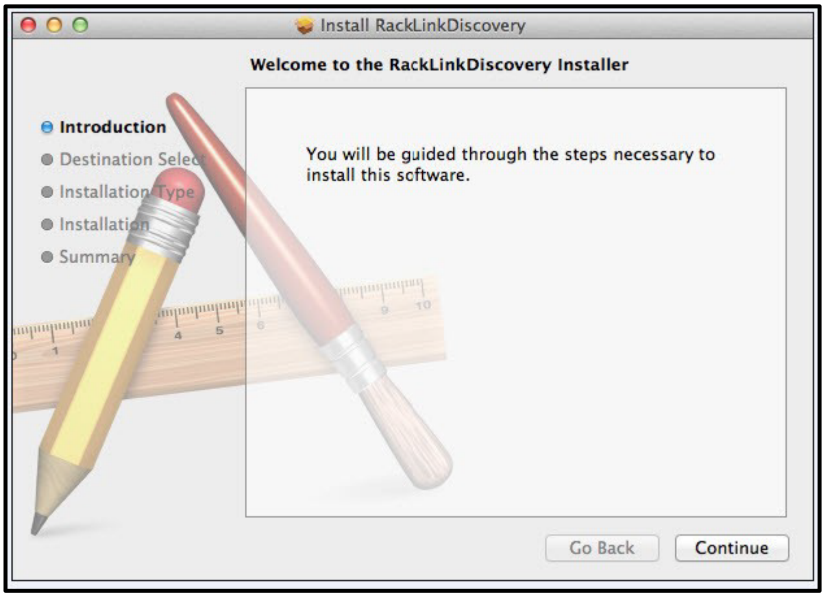
8. Click Close.

Installing the RackLink Device Discovery Software on a MAC:

▶ To install RackLink Device Discovery software on a MAC:

1. Access www.middleatlantic.com.
2. Download and run the `RackLinkDiscovery.pkg` file.

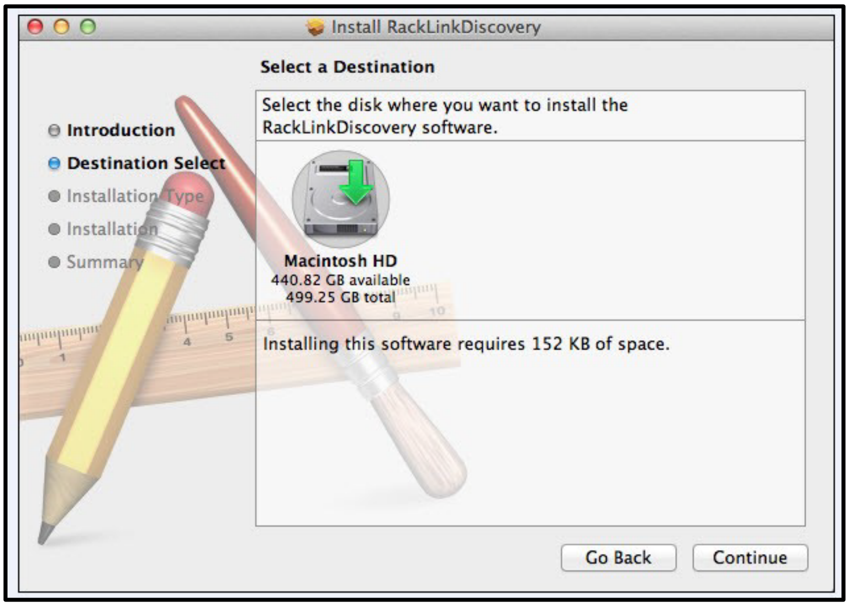
The Device Discovery Setup dialog box appears.



Welcome to the RackLinkDiscovery Installer

You will be guided through the steps necessary to install this scftware.

3. Click the disk and modify the location if you wish to change the software installation folder.



Select a Destination

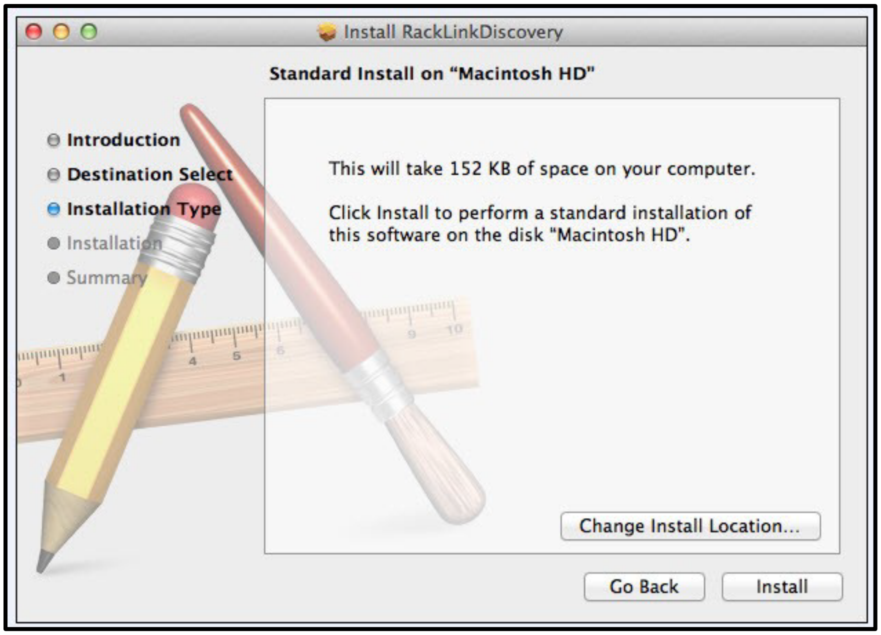
Select the disk where you want to install the RackLinkDiscovery software.

Macintosh HD
440.82 GB available
499.25 GB total

Installing this software requires 152 KB of space.

4. Click Continue.

The Installation Type screen appears.



Install RackLinkDiscovery

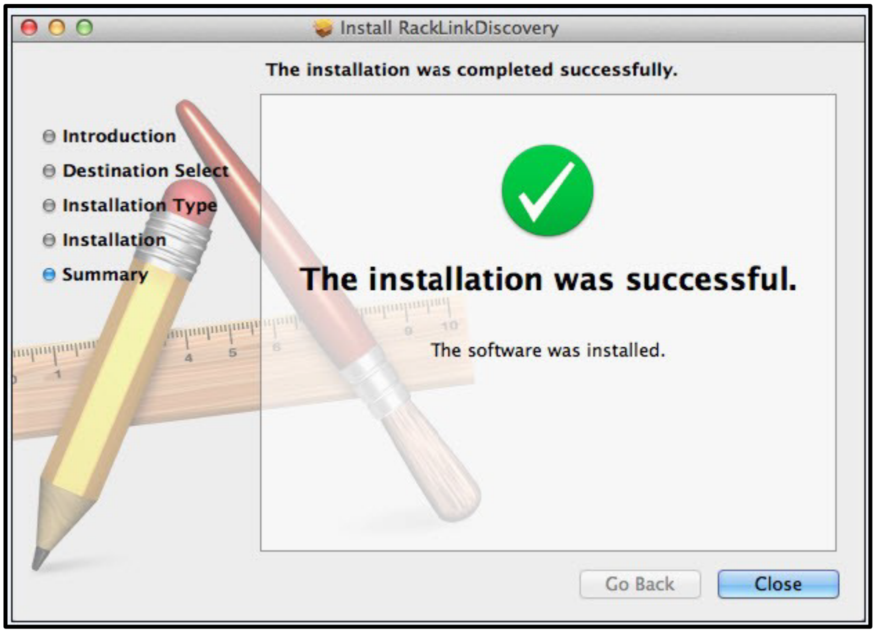
Standard Install on "Macintosh HD"

This will take 152 KB of space on your computer.

Click Install to perform a standard installation of this software on the disk "Macintosh HD".

5. Click Change Install Location if you wish to change the software installation folder.
6. Click Install.

The installer indicates that the installation was completed successfully.



Install RackLinkDiscovery

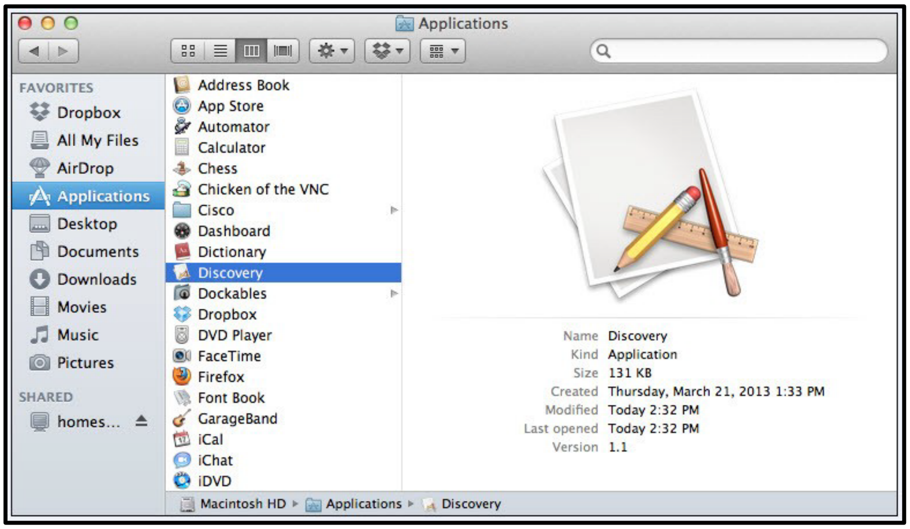
The installation was completed successfully.

The installation was successful.

The software was installed.

7. Click Close.

8. Click Applications in the Finder to locate the RackLink Discovery application.



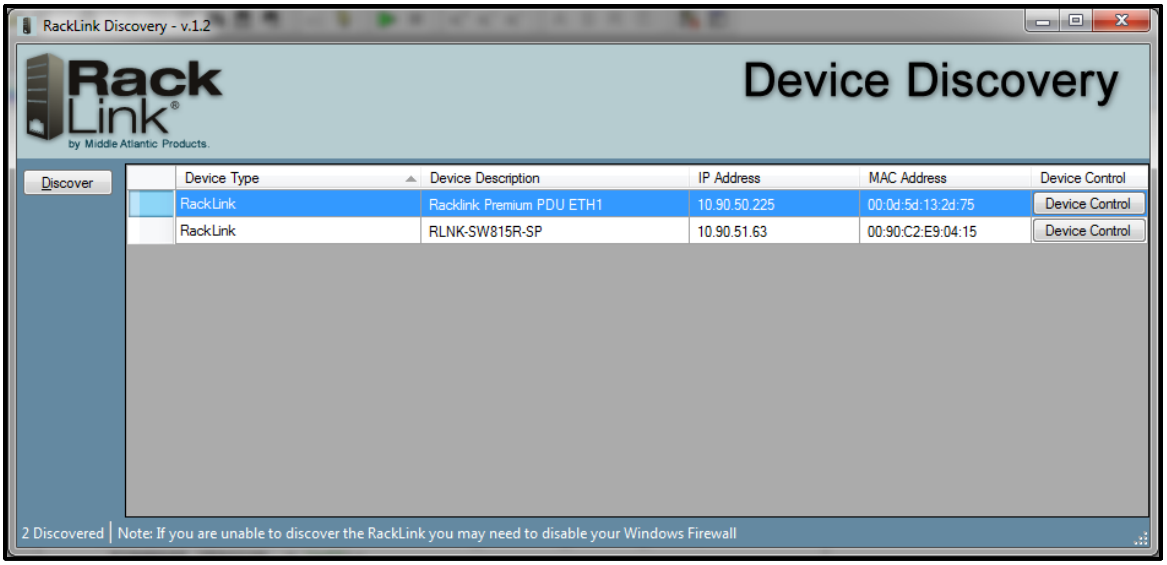
Name	Discovery
Kind	Application
Size	131 KB
Created	Thursday, March 21, 2013 1:33 PM
Modified	Today 2:32 PM
Last opened	Today 2:32 PM
Version	1.1

Using Device Discovery

To use device discovery:

1. After launching your RackLink Device Discovery program, the tool automatically discovers all RackLink devices on the subnet to which you are connected.
2. Use the Discover button to refresh the screen and discover any newly connected RackLink devices. By default, the RackLink device is set for DHCP. You can identify each device by the MAC address or IP address.

Note: You may need to disable your Windows firewall to discover your PDU.

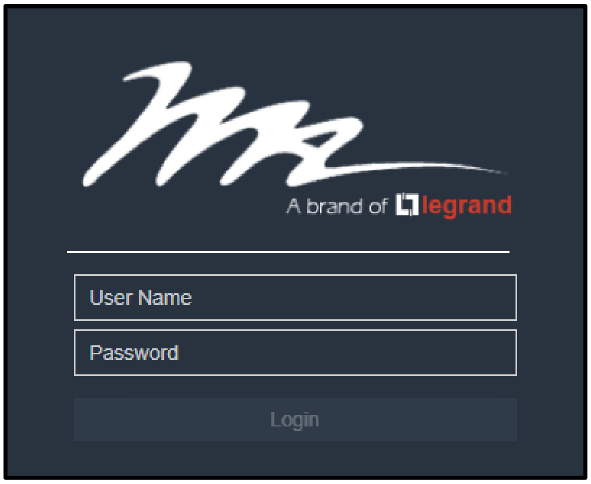


Device Type	Device Description	IP Address	MAC Address	Device Control
RackLink	Racklink Premium PDU ETH1	10.90.50.225	00:0d:5d:13:2d:75	Device Control
RackLink	RLNK-SW815R-SP	10.90.51.63	00:90:C2:E9:04:15	Device Control

2 Discovered | Note: If you are unable to discover the RackLink you may need to disable your Windows Firewall

3. Click Device Control to access the browser-based interface for a specific device.

4. The system prompts you for a username and password.



Note: To log in with the administrator account, the default credentials are Username: `admin`*, Password:* `admin`*.*

After logging in for the first time, the system forces you to change default passwords for security purposes. For more information about changing your password on your first login, see ***Changing Your Password on First Login*** (on page 23).

WARRANTY

For warranty information, refer to http://www.middleatlantic.com/company/about-us.aspx#warranty.

Corporate Headquarters
Voice: 973-839-1011 – Fax: 973-839-1976 – International Voice: +1 973-839-8821 –
Fax: +1 973-839-4982 – www.middleatlantic.com – info@middleatlantic.com

Middle Atlantic Canada
Voice: 613-836-2501 – Fax: 613-836-2690 – ca.middleatlantic.com – customerservicecanada@middleatlantic.ca

Middle Atlantic EMEA Technical Support
Voice: +31 (0) 495 726002 - av.emea.middleatlantic.support@legrand.com

Factory Distribution
United States: New Jersey, California, Illinois - Canada: Ontario - The Netherlands: Weert

At Middle Atlantic Products we are always listening. Your comments are welcome.

Middle Atlantic Products is an ISO 9001 and ISO 14001 Registered Company.