

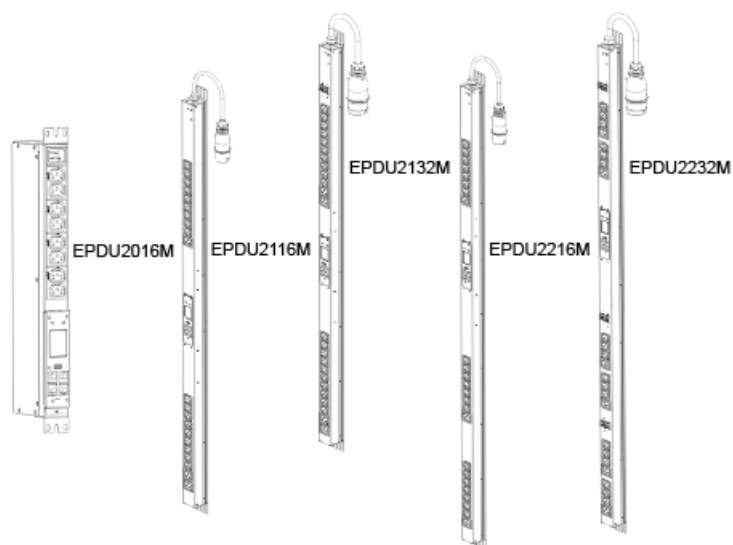
Easy PDU Metered Rack Power Distribution Unit

User Guide

EPDU2016M EPDU2116M EPDU2132M EPDU2216M EPDU2232M

TME63709

Release date 02/2025



Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Introduction	7
Watchdog Features	8
Network Interface Watchdog Mechanism	8
Resetting the Network Timer	8
Network Port Sharing (NPS)	8
Display ID	8
Installation Instructions for an NPS Group	9
How to Assign Specific Display IDs	9
About Network Management Cards	10
Types of User Accounts	10
Getting Started	11
Establish Network Settings	11
About DHCP and BOOTP Server Configuration	14
About IPv4 Setup	16
About IPv6 Setup	16
Network Management with Other Applications	16
Recover from a Lost Password	17
Reset to Defaults	18
Using the Command Line Interface	18
Using the Web UI	19
Display Interface	20
LED Descriptions	21
Display Panel Screens	22
Command Line Interface (CLI)	27
Local Access to the CLI	27
Remote Access to the CLI	28
About the Main Screen	29
Using the CLI	30
Command Syntax	31
Command Response Codes	32
Network Management Card Command Descriptions	33
?	33
about	33
alarmcount	34
boot	34
bye	35
cd	35
clrrst	36
console	36
date	37
delete	38
dir	38
dns	39
eapol	40
email	41
eventlog	43
exit	44
firewall	44

format	45
ftp	45
help	46
lang	46
lastrst	47
ledblink	47
logzip	48
netstat	48
ntp	49
ping	50
portSpeed	50
prompt	51
pwd	51
quit	51
radius	52
reboot	53
resetToDef	53
session	54
smtp	55
snmp	56
snmpv3	57
snmptrap	58
ssh	59
ssl	60
system	62
tcpip	63
tcpip6	64
user	65
userdflt	66
web	67
whoami	68
xferINI	69
xferStatus	69
Device Command Descriptions	70
Network Port Sharing Commands	70
alarmList	71
bkLowLoad	72
bkNearOver	73
bkOverLoad	74
bkPeakLoad	75
bkReading	76
bkRestrictn	77
devLowLoad	78
devNearOver	78
devOverLoad	79
devPeakLoad	79
devReading	80
devStartDly	81
displD	81
humAlGen	82
humHyst	83

humLow	84
humMin.....	85
humReading.....	86
humStatus.....	87
lcd	88
lcdBlink	88
logToFlash	89
modbus.....	90
phBal	91
phBalAIGen.....	91
phLowLoad	92
phNearOver	93
phOverLoad	94
phPeakCurr.....	95
phReading	96
phRestrictn.....	97
prodInfo	98
sensorName.....	99
tempAIGen.....	100
tempHigh	101
tempHyst.....	102
tempMax.....	103
tempReading.....	104
tempStatus.....	105
Web User Interface (Web UI).....	106
Log On to the Web UI.....	106
URL Address Formats.....	107
First Log On	107
Limited Status Page	108
Web UI Features	110
Tabs.....	110
Device Status Icons	110
Quick Links	111
Network Port Sharing (NPS) On the Web UI.....	111
About the Home Page.....	112
Status.....	113
View Alarms, NPS Groups, and Load Status	113
View Network Information	115
Control.....	116
Manage User Sessions	116
Reset the Network Interface.....	117
Configuration	117
Configure Load Thresholds.....	118
Configure Name and Location for the Rack PDU	119
Set the Coldstart Delay for the Rack PDU	119
Reset Peak Load and kWh	120
Configure Phase Load Balance.....	120
Configure Temperature and Humidity Sensors	121
Manage Security Settings.....	123
Configure Network Settings	135
Configure Notifications	153

Configure Identification.....	164
Configure Date and Time Settings.....	165
Configure Daylight Savings.....	166
How to Create and Import Settings With the User Config File	167
Configure Quick Links	167
Test: Blink the LCD or LEDs	167
Logs Tab.....	168
Event Log.....	168
Data Log	169
Firewall Logs	171
Use FTP or SCP to Retrieve Log Files	171
View Customer Support Information.....	173
How to Export Configuration Settings.....	175
Summary of the Procedure.....	175
Contents of the .ini File.....	175
.ini and Network Port Sharing	175
Detailed Procedures	176
Retrieve .ini File.....	176
Edit .ini File.....	177
Transfer the File To a Single Rack PDU	177
Transfer the File To Multiple Rack PDUs	177
The Upload Event and Error Messages	178
The Event and Its Error Messages	178
Messages in Config.ini	178
Errors Generated By Overridden Values	178
Related Topics	178
Updating Firmware	179
Firmware File Transfer Methods	179
Use the Firmware Update Utility	180
Use FTP or SCP to Update One Rack PDU	181
Use XMODEM To Upgrade One Rack PDU	182
Use a USB Drive To Transfer and Update Files	182
How To Update Multiple Rack PDUs.....	183
Use the Firmware Upgrade Utility For Multiple Upgrades	183
Upgrade Firmware for Network Port Sharing (NPS) Groups	183
Verifying Upgrades and Updates.....	184
Verify the Success Or Failure of the Transfer.....	184
Last Transfer Result Codes	184
Verify the Version Numbers of Installed Firmware	184
Troubleshooting	185
Rack PDU Access Issues.....	185
SNMP Issues	185
Download Log Files to a USB Flash Drive.....	186
Worldwide Customer Support.....	186
Source Code Copyright Notice	187

Introduction

The Easy PDU Metered Rack Power Distribution Unit (PDU) may be used as a stand-alone, network-manageable power distribution device or up to four devices can be connected together using one network connection. The Rack PDU provides real-time remote monitoring of connected loads. User-defined alarms warn of potential circuit overloads. Switched models provide full control over outlets through remote commands and user interface settings.

Your Rack PDU comes with a terminator installed in the display In or Out port. In stand-alone operation, one terminator must be installed in the display In or Out port. To use Network Port Sharing between up to four units, a terminator must be installed in the In port at one end of the group and another on the Out port at the other end of the group.

You can manage a Rack PDU through its Web User Interface (Web UI), its Command Line Interface (CLI), Data Center Expert, or Simple Network Management Protocol (SNMP). (To use the PowerNet MIB with an SNMP browser, see the PowerNet SNMP Management Information Base (MIB) Reference Guide, available at www.apc.com.) Rack PDUs have these additional features:

The Rack PDU has these additional features:

- Monitor device power, apparent power, power factor, energy, and frequency.
- Monitor phase voltage, current, power, apparent power, and power factor.
- Monitor bank current and peak current (for models that support breaker banks).
- Configurable alarm thresholds that provide network and visual alarms to help avoid overloaded circuits.
- Various levels of access: Super User, Administrator, Device User, Read-Only, and Network-Only User (These are protected by user name and password requirements).
- Multiple user login feature which allows up to four users to be logged in simultaneously.
- Event and data logging. The event log is accessible by Telnet, Secure CoPy (SCP), File Transfer Protocol (FTP), serial connection, or Web browser (using HTTPS access with SSL/ TLS, or using HTTP access). The data log is accessible by Web browser, SCP, or FTP.
- Support for Modbus TCP. You can use this feature to monitor the Rack PDU through a building management system.
- Email notifications for Rack PDU and Network Management Card (NMC) system events.
- SNMP traps, Syslog messages, and email notifications based on the severity level or category of the Rack PDU and NMC system event.
- Security protocols for authentication and encryption.
- Network Port Sharing (NPS). Up to four Rack PDUs of any model can be connected using the In and Out ports so that only one network connection is necessary.
- NPS guest firmware auto-update feature allows the NPS host to automatically pass a firmware update to its connected guests.
- Log files can be downloaded by inserting a USB Flash drive into the USB port on the Display Interface of the Rack PDU.

NOTE: The Rack PDU does not provide power surge protection. To ensure that the device is protected from power failure or power surges, connect the Rack PDU to a Schneider Electric Uninterruptible Power Supply (UPS).

Watchdog Features

To detect internal problems and recover from unanticipated inputs, the Rack PDU uses internal, system-wide watchdog mechanisms. When it restarts to recover from an internal problem, a “Network Interface Restarted” event is recorded in the Event Log.

Network Interface Watchdog Mechanism

The Rack PDU implements internal watchdog mechanisms to help protect itself from becoming inaccessible over the network. For example, if the Rack PDU does not receive any network traffic for 9.5 minutes (either direct traffic, such as SNMP, or broadcast traffic, such as an Address Resolution Protocol [ARP] request), it assumes that there is a problem with its network interface and restarts. The network interface watchdog mechanism is only enabled on a Rack PDU that discovers an active network interface connection at start-up.

Resetting the Network Timer

To help ensure that the Rack PDU does not restart if the network is quiet for 9.5 minutes, the Rack PDU attempts to contact the default gateway every 4.5 minutes. If the gateway is present, it responds to the Rack PDU, and the response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network and is on the same subnet. The network traffic of that computer should restart the 9.5-minute timer frequently enough to prevent the Rack PDU from restarting.

Network Port Sharing (NPS)

You can use the Network Port Sharing feature to view the status of and configure and manage up to eight Rack PDUs using only one network connection. This is made possible by connecting the Rack PDUs via the In and Out ports on the Rack PDU front panel.

An NPS group consists of one host Rack PDU (which provides the network connection) and several guest Rack PDUs. The host Rack PDU supports many features that are not supported by guest PDUs in the NPS group. These include, but are not limited to:

- SNMP rPDU2 Group OIDs
- Initiating AOS/APP firmware updates for guest Rack PDUs
- Time synchronization for guest Rack PDUs
- Data logging for the guest Rack PDUs

Display ID

The display ID is a number, 1 to 16, used to uniquely identify the Rack PDUs in a group. After two or more are connected to one another in an NPS group, they can be identified on the various interfaces by the use of this **Display ID**. You can see this Display ID in the top left corner of the LCD display.

Installation Instructions for an NPS Group

Connect up to eight using the In and Out ports on the display interface of each unit.

NOTE: To reduce the possibility of communication issues, the maximum total length of cabling (Cat5e+) connecting Rack PDUs in a group should not exceed 10 meters.

Connect the **Network** port of one of the grouped Rack PDUs to a network hub or switch. This unit will be the Host for the Rack PDU group. Guest PDU data can be viewed on the Host PDU. Set up network functionality for this Host Rack PDU as specified in . The Host PDU will automatically discover any Guest PDUs connected through the In and Out ports. The Rack PDU group is now available from the Host PDU's IP address.

Only one Rack PDU in an NPS group is allowed to be the host. If two host units are connected together, one will automatically be chosen to be the single host for the NPS group. You also have the option to select a particular guest to be the host as long as that guest has an active network link.

How to Assign Specific Display IDs

You can assign specific Display IDs by powering up the units manually for the first time in the desired order (1 to 16). Before powering up any of the Rack PDUs connected in a group, determine the Display ID order. Then, first turn on the unit that you would like to have Display ID 1. After that unit has initialized and the LCD has started displaying its screens, turn on the unit that you would like to have Display ID 2. Continue in the same way for units 3–16, if applicable for your setup.

Alternatively, you can assign specific display IDs from the Web UI and CLI..

- Web UI: Go to **Configuration > RPDU > Device**. Enter the new ID in the **Display ID** field.
- CLI: Use the `dispId` command.

About Network Management Cards

The Schneider Electric Network Management Card (NMC) enables essential and secure remote monitoring and management of your Rack PDU.

To ensure your Network Management Card has the latest firmware which is independently certified to the IEC 62443-4-2 standard, your NMC includes a 1-year Secure NMC System (SNS) subscription.

For further information including the latest documentation, please visit www.apc.com/secure-nmc. Select the Software and Firmware tab to download the Secure NMC System update tool for your device. Select the Documents tab to download the Secure NMC System (SNS) Tool User Guide.

For more cyber security guidance, please refer to *Network Management Card 3 - Security Handbook* on https://www.apc.com/us/en/download/document/SPD_CCON-BDYD7K_EN/.

NOTE: SNS subscriptions are not currently available in China or Japan.

Types of User Accounts

The Rack PDU has various levels of access which are protected by user name and password requirements. Up to four users are allowed to login to the same Rack PDU simultaneously.

NOTE: You will be prompted to enter a new password the first time you connect to the RPDU with the Super User account. All other account types are disabled by default, and cannot be enabled until the Super User default password (**apc**) is changed.

- Super User: There is only one Super User account, which cannot be deleted. The super user can use all of the menus in the web UI and all of the commands in the CLI.

The default user name and password for the Super User are both **apc**.

- Administrator: There can be multiple Administrator accounts. An Administrator can use all of the menus in the Web UI and all of the commands in the CLI.

The Super User or another Administrator can manage an Administrator account (enable, disable, change password, etc.).

- Device User: A Device User has read and write access to device-related menus. Administrative functions like session management (**Control > Security > Session Management**) and firewall management (**Configuration > Security > Firewall**) are not available to Device Users.
- A Network-Only User (remote user) can only log on using the web UI and CLI (via Telnet or SSH). A Network-Only User has read/write access only to the network related menus.

Getting Started

To start using the Rack PDU:

1. Follow the installation instructions provided with your Rack PDU to install the Rack PDU, apply power to the Rack PDU, and connect the Rack PDU to your network.
2. Log onto the Rack PDU and establish the network settings (see [Establish Network Settings](#), page 11).
3. Begin using the Rack PDU with one of the following:
 -
 - [Command Line Interface \(CLI\)](#), page 27
 - [Web User Interface \(Web UI\)](#), page 106
 - [SNMP protocol](#) (see [Configure SNMP Settings](#), page 147)

Establish Network Settings

The Rack PDU must receive TCP/IP settings before it can operate on the network. By default, the Rack PDU uses Dynamic Host Configuration Protocol (DHCP) to auto-assign dynamic IP settings, which change periodically. If you have specific requirements for the TCP/IP settings or require a static IP address, you can assign the TCP/IP settings manually through the CLI.

- To use the default configuration method, see [DHCP Configuration](#), page 11.
- To set the TCP/IP settings manually, see [Static IP Configuration](#), page 12.
- To use the Device IP Configuration utility, see [Device IP Configuration Utility](#), page 13.

Once the TCP/IP settings are configured, you can export them to other Rack PDUs using a .ini file. For instructions using the .ini file, see [How to Create and Import Settings With the User Config File](#), page 167.

More information about network settings is available in the following sections:

- [About DHCP and BOOTP Server Configuration](#), page 14
- [About IPv4 Setup](#), page 16
- [About IPv6 Setup](#), page 16

DHCP Configuration

By default, DHCP is enabled to auto-assign a dynamic IP address to your Rack PDU. This setting assumes that a properly configured DHCP server is available to provide TCP/IP settings to the Rack PDU.

To discover the IP address in the display interface:

1. On the display interface of the Rack PDU, connect a network cable to the **Network** port.
2. Go to the **Network Status** screen in the display interface. Observe the IP address automatically assigned to the
3. On your computer, open a web browser. Enter the IP address of the Rack PDU in the web browser.
4. Log on to the Rack PDU with the default Super User name and password (**apc** and **apc**). You will be required to change the default password. The new password must have at least one lowercase character, one uppercase character, one number, and one symbol.

Static IP Configuration

Log on to the CLI, then configure the TCP/IPv4 or TCP/IPv6 settings.

To log on to the CLI:

This procedure assumes that a Virtual COM Port (VCP) driver is installed on the computer. If needed, download and install the VCP driver for your operating system from ftdichip.com.

1. Open an application to view the COM ports for the computer, according to the instructions for your operating system. (In Windows operating systems, you can view ports in the Device Manager.)
2. Use a serial cable to connect the **Serial** port of the Rack PDU to a USB port on the computer.

A newly occupied serial COM port should appear in the port-viewing application. Take note of the port number or re-assign the port as needed.

3. Run a terminal program (such as Tera Term® or HyperTerminal®) and configure the selected serial COM port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Use the port to make a serial connection to the Rack PDU.
4. Press ENTER up to three times to display the `User Name` prompt. Log on to the Rack PDU with the default Super User name and password (**apc** and **apc**). You will be required to change the default password. The new password must have at least one lowercase character, one uppercase character, one number, and one symbol.

Configure TCP/IPv4 Settings

1. Contact your network administrator to obtain the IP address, subnet mask, and default gateway for the Rack PDU.
2. Use these three commands to configure network settings. (Text in *italics* indicates a variable.)


```
tcpip6 -i yourIPAddress
tcpip6 -s yourSubnetMask
tcpip6 -g yourDefaultGateway
```

For each variable, type a numeric value that has the format xxx.xxx.xxx.xxx. For example, to set a system IP address of 156.205.14.141, enter the following command: `tcpip6 -i 156.205.14.141`

NOTE: Do NOT use the loopback address (127.0.0.1) as the default gateway. Doing so disables the network connection of the Rack PDU. To enable the network connection again, you must log on using a serial connection and reset the TCP/IP settings to their defaults.

NOTE: You can also enter all three command options on the same line:

```
tcpip6 -i yourIPAddress tcpip6 -s yourSubnetMask tcpip6
-g yourDefaultGateway
```

3. Type `exit`, and then press ENTER. The Rack PDU restarts to apply the changes.

Configure TCP/IPv6 Settings

1. Contact your network administrator to obtain the IP address, subnet mask, and default gateway for the Rack PDU.
2. Use these three commands to configure network settings. (Text in *italics* indicates a variable.)

```
tcpip6 -man enable
tcpip6 -i yourIPAddress
tcpip -g yourDefaultGateway
tcpip -d6 DHCPv6 mode
```

NOTE: For the IP address and Default Gateway, type a numeric value that has the format `xxxx:xxxx:xxxx:xxxx/xx`. Do NOT use the loopback address (127.0.0.1) as the default gateway. Doing so disables the network connection of the Rack PDU. To enable the network connection again, you must log on using a serial connection and reset the TCP/IP settings to their defaults.

NOTE: The *DHCPv6 mode* can be `router`, `statefull`, `stateless`, or `never`.

3. Type `exit`, and then press ENTER. The Rack PDU restarts to apply the changes.

Device IP Configuration Utility

SNMP is disabled by default, and must be enabled for the Device IP configuration Utility to function. You can enable SNMP from the CLI. (See [Local Access to the CLI](#), page 27 for instructions to access the CLI. See [snmp](#), page 56 to enable snmp).

The Device IP Configuration Utility can discover Rack PDUs that do not have an IP address assigned. Once discovered, you can configure the IP address settings for the Network Management Cards (NMCs). You can also search for devices already on the network by entering an IP range to define the search. The Utility scans the IP addresses in the defined range and discovers Rack PDUs that already have a DHCP-assigned IP address.

NOTE:

- For detailed information on the Wizard, see the FAQ article *How do I configure APC Network Management Card network settings?* (FA156064).
- To use the DHCP Option 12, see the FAQ article *Which DHCP options are used when an APC Network Management Device makes a DHCPv4 request?* (FA156110).
- To find an FAQ article, go to www.apc.com, and select your location if prompted to do so. Then select **Support > Browse FAQs** and enter the article number or title of the FAQ in the Search bar.

System Requirements

The Device IP Configuration Utility is a Windows application designed specifically to remotely configure the basic TCP/IP settings of Network Management Cards. The Utility runs on Microsoft®Windows® 2000, Windows Server® 2003, Windows Vista®, Windows XP®, Windows 7, Windows Server 2008, Windows 8, and Windows 10, and Windows 12. This utility supports Network Management Cards that have firmware version 3.x.x or higher and is for IPv4 only.

Install the Device IP Configuration Utility

1. Go to the download center at www.se.com/ww/en/download, click **Select location**, then select your country from the available options.
2. Enter "Network Management Card Device IP Configuration Utility" in the Search bar. Download the latest version of the Network Management Card Device IP Configuration Utility.

3. Extract the .zip file to your desktop, and run the executable file (*DevIPSetup.exe*).

NOTE: If you leave the **Start a Web browser when finished** option enabled, you can use **apc** for both the user name and password to access the Rack PDU through your browser.

When Installed, the Device IP configuration Utility is available through the Windows **Start** menu options.

About DHCP and BOOTP Server Configuration

The default TCP/IP configuration setting, **DHCP**, assumes that a properly configured DHCP server is available to provide TCP/IP settings to the Rack PDU. You can also configure the setting for BOOTP. After configuring the BOOTP or DHCP server, you can log into the CLI and view the IP address assigned to your Rack PDU.

NOTE: A user configuration (INI) file can function as a BOOTP or DHCP boot file.

DHCP Server Configuration

You can use an RFC2131/RFC2132-compliant DHCP server to configure the TCP/IP settings for the Rack PDU.

1. The Rack PDU sends out a DHCP request that uses the following to identify itself:
 - A Vendor Class Identifier (APC by default)
 - A Client Identifier (by default, the MAC address of the Rack PDU)
 - A User Class Identifier (by default, the identification of the application firmware installed on the Rack PDU)
 - A Host Name (by default, apcXXYYZZ with XXYYZZ being the last six digits of the Rack PDU serial number). This is known as DHCP Option 12.
2. A properly configured DHCP server responds with a DHCP offer that includes all the settings that the Rack PDU needs for network communication. The DHCP offer also includes the Vendor Specific Information option (DHCP option 43). The Rack PDU can be configured to ignore DHCP offers that do not encapsulate the APC cookie in DHCP option 43 using the following hexadecimal format. (The Rack PDU does not require this cookie by default.)

Option 43 = 01 04 31 41 50 43

- The first byte (01) is the code.
- The second byte (04) is the length.
- The remaining bytes (31 41 50 43) are the APC cookie. See your DHCP server documentation to add code to the Vendor Specific Information option.

NOTE: By selecting the **Require vendor specific cookie to accept DHCP Address** check box in the Web UI, you can require the DHCP server to provide an “APC” cookie, which supplies information to the Rack PDU.

BOOTP Server Configuration

For the Rack PDU to use a BOOTP server to configure its TCP/IP settings, it must find a properly configured RFC951-compliant BOOTP server.

1. In the BOOTPTAB file of the BOOTP server, enter the Rack PDU MAC address, IP address, subnet mask, and default gateway, and, optionally, a bootup file name. Look for the MAC address on the bottom of the Rack PDU.

2. Use a serial connection to access the CLI, then enter `-b <bootp>` to enable BOOTP. The default username and password are both **apc**.

See [Local Access to the CLI](#), page 27 for detailed instructions to access the CLI.

3. Enter `-Y` to reboot the Rack PDU.

When the Rack PDU reboots, the BOOTP server provides it with the TCP/IP settings.

- If you specified a bootup file name, the Rack PDU attempts to transfer that file from the BOOTP server using TFTP or FTP. The Rack PDU assumes all settings specified in the bootup file.
- If you did not specify a bootup file name, you can configure the other settings of the Rack PDU remotely through its Web UI or CLI. The default user name and password are **apc** for both interfaces. To create a bootup file, see your BOOTP server documentation.

About IPv4 Setup

You must define three TCP/IP settings for the Rack PDU before it can operate on the network:

- The IP address of the Rack PDU
- The subnet mask of the Rack PDU
- The IP address of the default gateway (only needed if you are going off-segment)

NOTE: If a default gateway is unavailable, use the IP address of a computer that is located on the same subnet as the Rack PDU and is usually running. The Rack PDU uses the default gateway to test the network when traffic is very light.

NOTE: Do NOT use the loopback address (127.0.0.1) as the default gateway. Doing so disables the network connection of the Rack PDU. To enable the network connection again, you must log on using a serial connection and reset the TCP/IP settings to their defaults.

For detailed information on how to use a DHCP server to configure the TCP/IP settings on a Rack PDU, see **DHCP Response Options** under *Configure IPv4 Network Settings*, page 136.

About IPv6 Setup

IPv6 network configuration provides flexibility to accommodate your requirements. IPv6 can be used anywhere an IP address is entered on this interface. You can configure IPv6 using the CLI, the Web UI, or DHCP.

Network Management with Other Applications

These applications and utilities work with a Rack PDU which is connected to the network.

- PowerNet® Management Information Base (MIB) with a standard MIB browser — Allows you to perform SNMP SETs and GETs and use SNMP traps.
- Data Center Expert — Provides enterprise-level power management and management of agents, Rack PDUs, and environmental monitors.
- EcoStruxure™ IT — Provides cloud-based monitoring of your Rack PDU via SNMP.
- Device IP Configuration Utility — Allows you to configure the basic settings of one or more Rack PDU over the network.
- Security Wizard — Allows you to create components needed to help with security for the Rack PDUs when you are using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) and related protocols and encryption routines.

Recover from a Lost Password

To recover from a lost password, you must reset the Rack PDU to its default configuration. Export the .ini file after configuring your Rack PDU and keep it in a safe place. If you have this file saved, you will be able to retrieve your configuration after a lost password event.

To reset the Rack PDU:

1. On the display interface, hold down the **Reset** button for 20–25 seconds, ensuring the status LED is flashing green during this time. When the status LED turns off, release the **Reset** button to allow the Rack PDU to complete its reboot process.

2. Access the Rack PDU through a secure connection with the default username and password (**apc** and **apc**).

Secure connections include a local connection to the CLI by serial cable, a remote connection to the CLI by SSH, or a connection to the web UI by HTTPS. Instructions for each of these secure connections are covered in this manual. Insecure connections are disabled by default.

3. Reset the username and password, then configure the Rack PDU settings as needed.

Reset to Defaults

You can use the CLI or the web UI to reset the Rack PDU to its default settings.

Using the Command Line Interface

You can use a local computer (a computer that connects to the Rack PDU or other device through the serial port) to access the Command Line Interface.

1. Open an application to view the COM ports for the computer, according to the instructions for your operating system. (In Windows operating systems, you can view ports in the Device Manager.)
2. Use a serial cable to connect the **Serial** port of the Rack PDU to a USB port on the computer.

A newly occupied serial COM port should appear in the port-viewing application. Take note of the port number or re-assign the port as needed.

3. Run a terminal program (such as Tera Term® or HyperTerminal®) and configure the selected serial COM port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Use the port to make a serial connection to the Rack PDU.
4. At the CLI, use one of the following commands to set the Rack PDU to its default parameters: `reset -p all` or `reset -p keepip`
`reset -p all` resets all parameters to the default settings, including the IP address. The default IP setting, DHCP, assigns a dynamic IP address via DHCP server.
`reset -p keepip` resets all parameters except for the IP address.
5. Enter `reboot` to restart the device.

NOTE: Press the **Reset** button on the LCD front panel only to reboot the device itself without resetting to defaults.

Using the Web UI

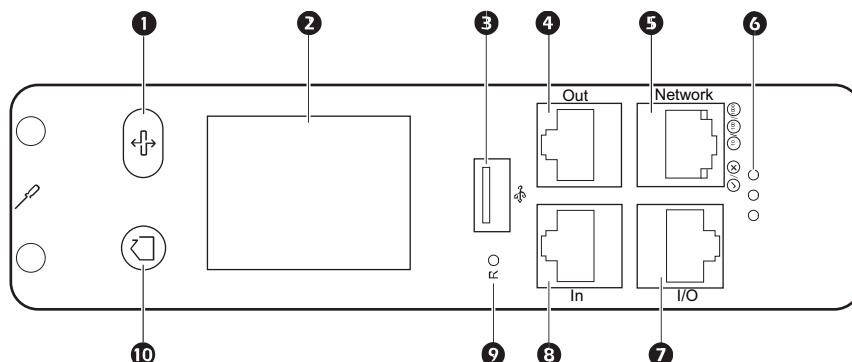
1. Go to **Control > Network > Reset/Reboot**.
2. Select the desired setting.

Setting	Description
Reboot Management Interface	This setting only restarts the Rack PDU's Network Management Interface. It does not affect the ON/OFF status of the outlets.
Reset All	Reset all configuration values except for account information and the event log. You can select Exclude TCP/IP to reset all configuration values except the ones that determine how the PDU obtains its TCP/IP configuration. The default TCP/IP setting is DHCP .
Reset Only	Select a specific set of parameters to reset. The following parameters are only available for NPS groups: <ul style="list-style-type: none">• TCP/IP: Set the TCP/IP configuration to DHCP, its default setting. This requires that the Rack PDU receive its TCP/IP settings from a DHCP server.• Event Configuration: Resets only the events to their default configuration. Any configuration changes, by event or by group, revert to their default settings.• RPDU to Defaults: Resets only the Rack PDU settings to their default configurations.

3. Click **Apply** to save your changes.

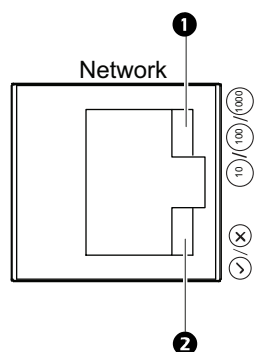
Display Interface

During normal operation, the LCD will flash periodically. When a critical alarm is triggered, the buzzer will beep. Press any button on the display to turn off the buzzer.



Item	Description	
1	Scroll Button	Press once to display the menu. Press additional times to move the highlight bar down the menu list until you reach the desired item.
2	Display Panel	Shows information about the Rack PDU.
3	USB Port	Connect a flash drive for firmware upgrades or to download data logs. (5V at 100 mA)
4	Out Port	For use with Network Port Sharing feature.
5	Network port (10/100/1000 Base-T Connector)	Connect the Rack PDU to the network. For detailed information on the Light emitting diodes (LEDs), see LED Descriptions , page 21.
6	Speakers	Not used.
7	I/O (RJ45 Serial Port)	Port to connect optional Temp/Humidity Sensor (EPDU-TH or EPDU-TH3). Port to connect the Rack PDU to a terminal emulator program for local access to the Command Line Interface.
8	In Port	For use with Network Port Sharing feature.
9	Reset Button	Reset the Rack PDU without affecting the status of the outlets.
10	Main Menu Button / Select Button	Press to view menu information or navigate back to the main menu. The display screen shows MAIN below the button. With the menu item highlighted, press this button to display the Rack PDU information. The display screen shows SELECT below the button.

LED Descriptions



10/100/1000 LED ①

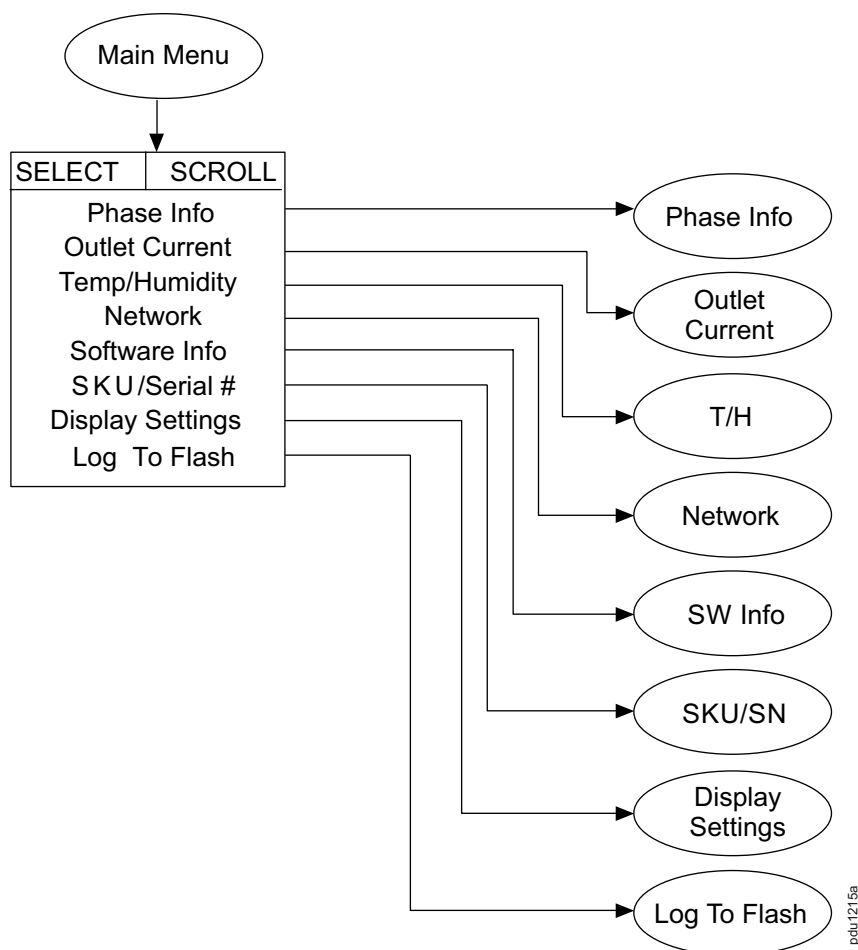
Condition	Description
Off	One of the following situations exists: <ul style="list-style-type: none"> The Rack PDU is not receiving input power. The cable that connects the Rack PDU to the network is disconnected or defective. The device that connects the Rack PDU to the network is turned off. The Rack PDU is not operating properly. It may need to be repaired or replaced. Contact Customer Support.
1 Blink	The Rack PDU is connected to a network operating at 10 Megabits per second (Mbps).
2 Blink	The Rack PDU is connected to a network operating at 100 Mbps.
3 Blink	The Rack PDU is connected to a network operating at 1000 Mbps.

Network Status LED ②

Condition	Description
Off	One of the following situations exists: <ul style="list-style-type: none"> The Rack PDU is not receiving input power. The Rack PDU is not operating properly. It may need to be repaired or replaced. Contact Customer Support.
Solid Green	The Rack PDU has valid TCP/IP settings.
Flashing Green	The Rack PDU is making DHCP or BOOTP requests.
<p>If you do not use a BOOTP or DHCP server, see Establish Network Settings, page 11 to configure the TCP/IP settings of the Rack PDU.</p> <p>To use a DHCP server, see Configure IPv4 Network Settings, page 136.</p>	

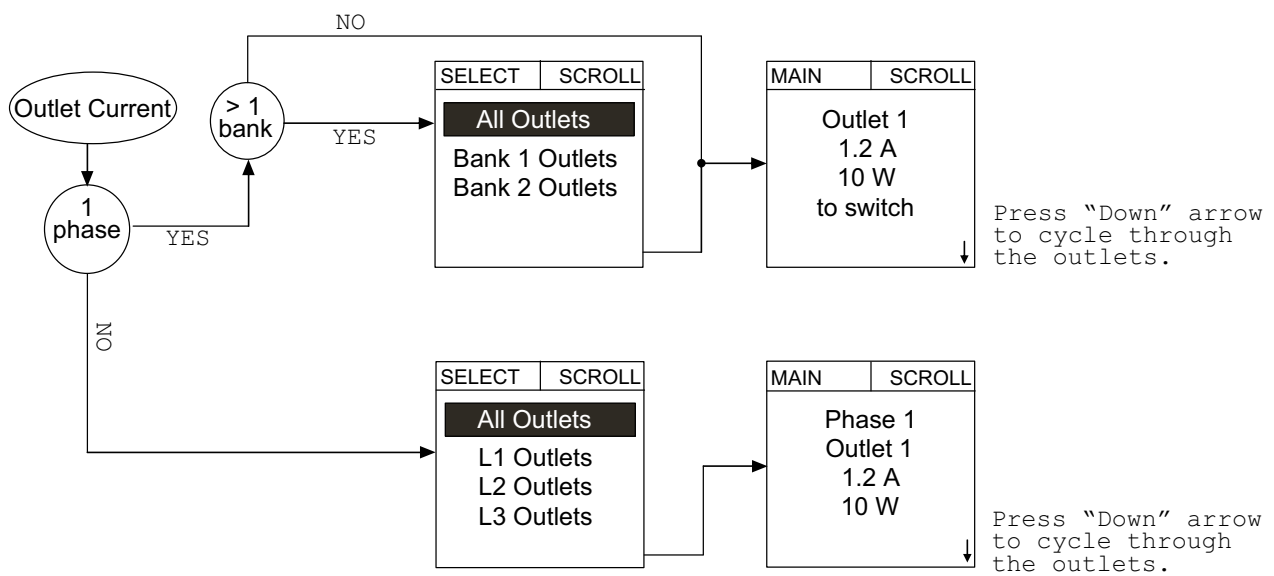
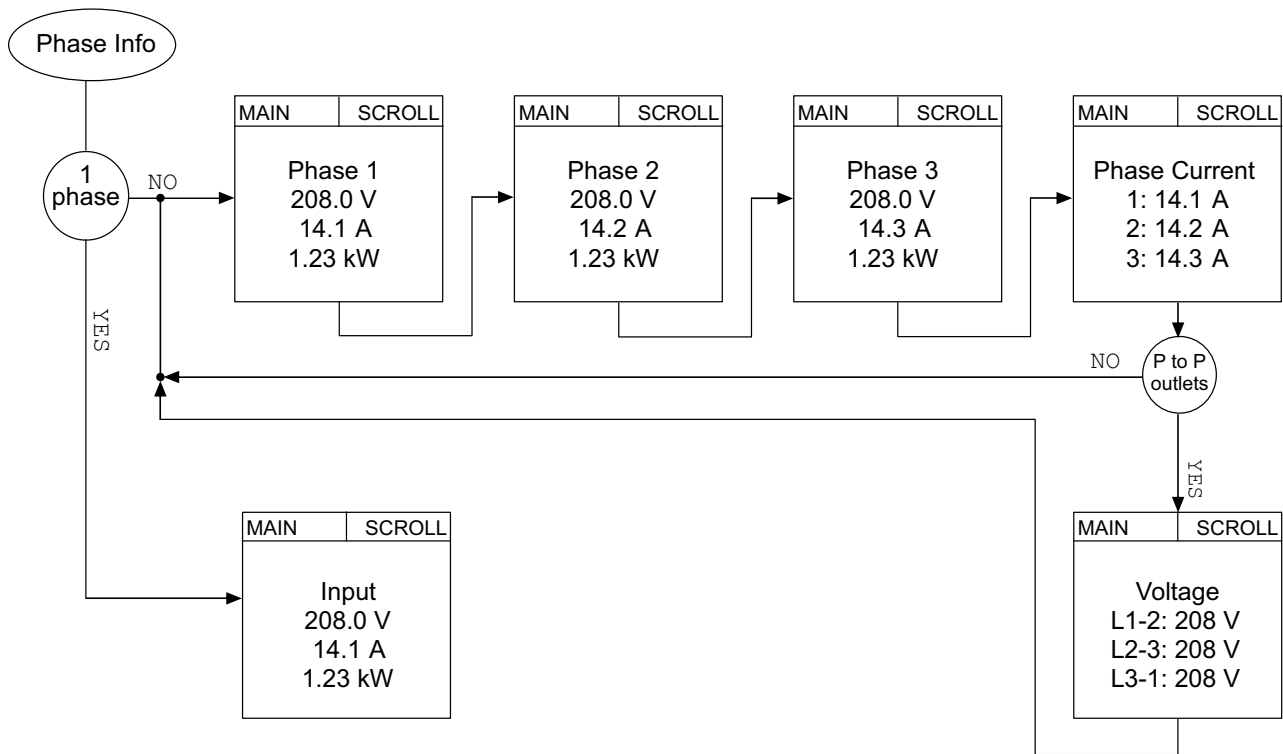
Display Panel Screens

Main Menu



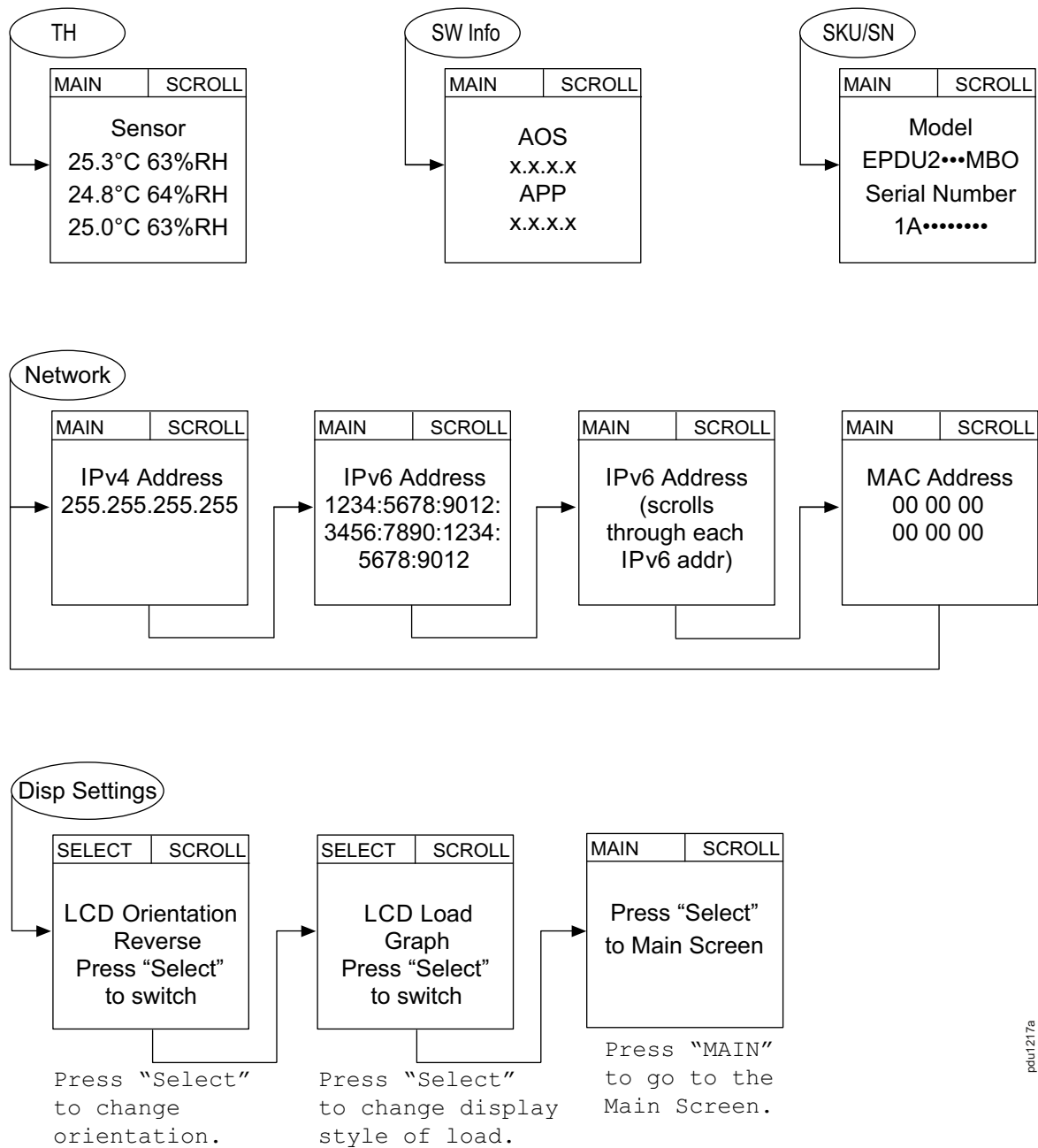
The display screen is restricted to four lines per page. If there are more than four available selections, they will appear on multiple pages. **Temp/Humidity** only appears when an EPDU-TH3 sensor is attached.

Submenus 1-2



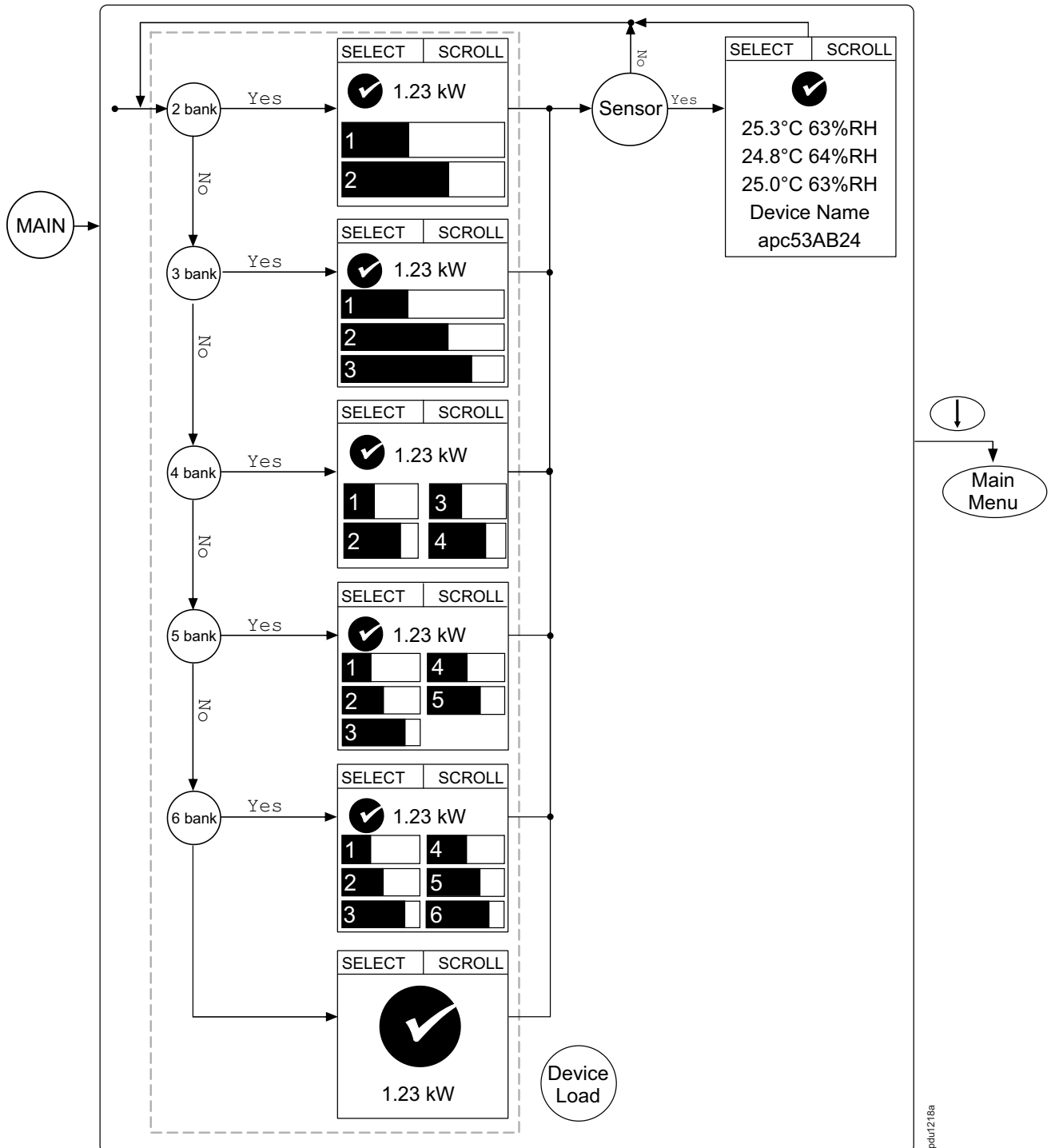
pdu1216a

Submenus 3–7



pdu1217a

Monitor Screens

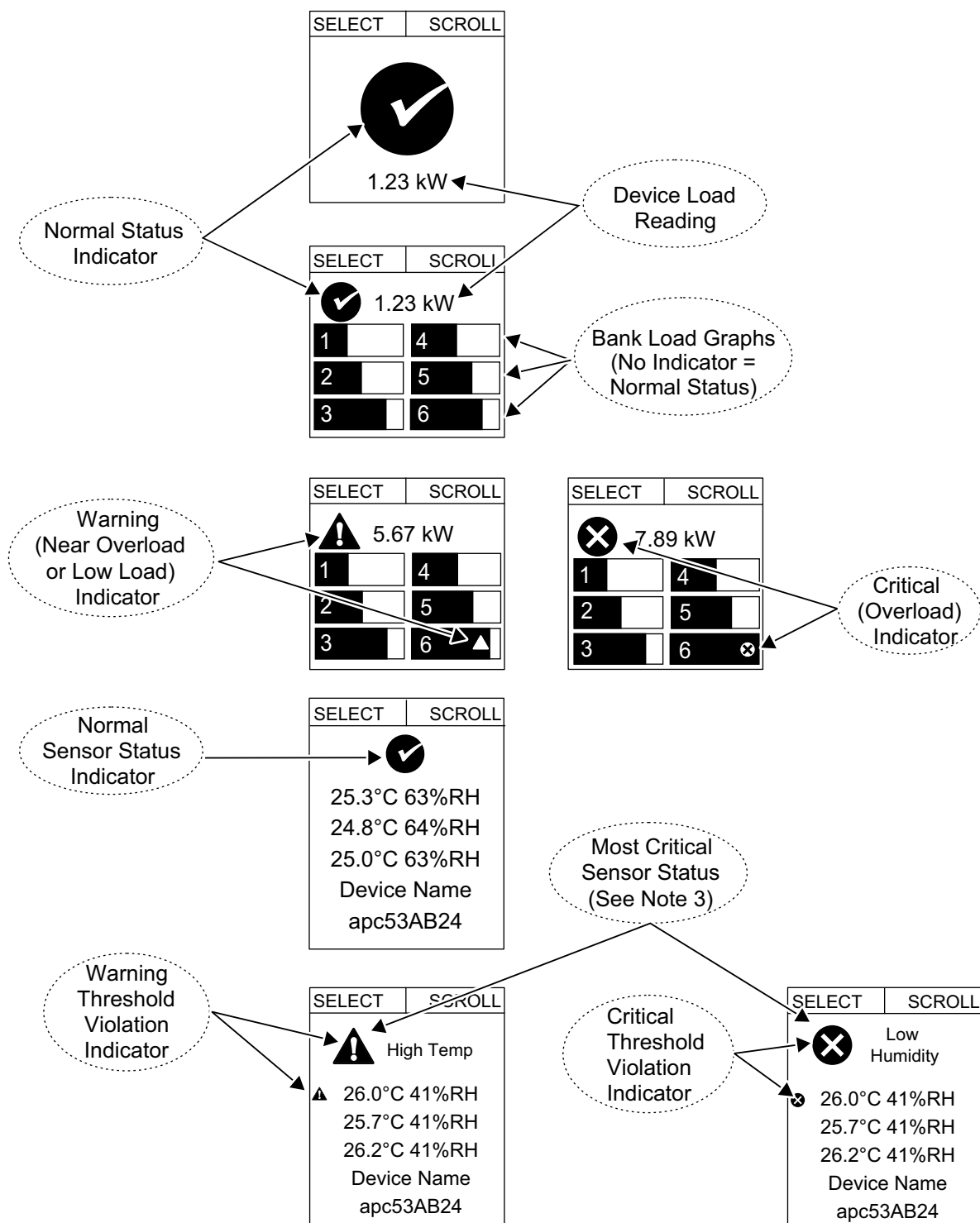


NOTE: Numeric and graph pages will not display if no bank exists. A total device power page will be added when using the numeric load display if banks exist on your equipment.

SELECT	SCROLL
Bank Current	
1: 10.5 A	
2: 10.6 A	

pdu1220a

Monitor Status Indicators



pdu1219a

NOTE:

1. The simplified display screens will show device load alarms only when no banks are present. The display screens will show bank load alarms only when banks are present. Phase and Outlet alarms/warnings are NOT displayed.
2. The icon in the upper-left corner of the display interface is the indicator of either a warning or critical event. You must connect an optional Temperature/Humidity sensor (EPDU-TH3) to the Rack PDU to use the temperature and humidity status screens.
3. For simplicity, both warning and critical temperature threshold violations display as **High Temp**. Similarly, both warning and critical humidity threshold violations display as **Low Humidity**.

Command Line Interface (CLI)

You can use the Command Line Interface (CLI) to view the status of and configure and manage the Rack PDU. The CLI uses YMODEM to perform file transfers. However, you cannot read the current file through YMODEM.

You can access the CLI locally with a serial connection to your computer. You can also access the CLI remotely with SSH or Telnet.

Local Access to the CLI

This procedure assumes that a Virtual COM Port (VCP) driver is installed on the computer. If needed, download and install the VCP driver for your operating system from ftdichip.com.

1. Open an application to view the COM ports for the computer, according to the instructions for your operating system. (In Windows operating systems, you can view ports in the Device Manager.)
2. Use a serial cable to connect the **Serial** port of the Rack PDU to a USB port on the computer.

A newly occupied serial COM port should appear in the port-viewing application. Take note of the port number or re-assign the port as needed.

3. Run a terminal program (such as Tera Term® or HyperTerminal®) and configure the selected serial COM port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Use the port to make a serial connection to the Rack PDU.
4. Press ENTER up to three times to display the `User Name` prompt. Log on to the Rack PDU with the default Super User name and password (**apc** and **apc**). You will be required to change the default password. The new password must have at least one lowercase character, one uppercase character, one number, and one symbol.

Remote Access to the CLI

You can choose to access the CLI through SSH and/or Telnet. By default, SSH is enabled and Telnet is disabled. You can use the `console` command to enable or disable either Telnet or SSH. If needed, you can also use the Web UI (under **Configuration > Network > Console > Access**) to enable or disable Telnet or SSH.

SSH for High-security Access

If you use the higher security of SSL/TLS for the web UI, use SSH for access to the CLI. SSH encrypts user names, passwords, and transmitted data. The interface, user accounts, and user access rights are the same whether you access the CLI through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer. See the *Network Management Card 3 Security Handbook*(SPD_CCON-BDYD7K_EN) on www.se.com/ww/en/download for more information on configuring and using SSH. You must select a location to view and download user manuals from the website.

Telnet for Basic Access

Telnet provides the basic security measure of authentication by user name and password, but not the high-security benefits of encryption.

To access the CLI via Telnet:

1. At a command prompt, type `telnet` and the IP address for the Rack PDU (for example, `telnet 139.225.6.133`, when the Rack PDU uses the default Telnet port of 23), and press ENTER.

If the Rack PDU uses a non-default port number (from 5000 to 32768), you must include a colon or a space, depending on your Telnet client, between the IP address (or DNS name) and the port number. (These are commands for general use; some clients do not allow you to specify the port as an argument and some types of Linux might require extra commands).

2. Enter the user name and password. If you cannot remember your user name or password, see the procedure to *Recover from a Lost Password*, page 17.

About the Main Screen

The following screen is displayed when you log on to the CLI of a Rack Rack PDU.

Schneider Electric		Network Management Card AOS		vx.x.x.x
(c) Copyright 2023 All Rights Reserved		C4CPDU APP		vx.x.x.x

Name	: Test Lab	Date	: 03/12/2023	
Contact	: Don Adams	Time	: 5:58:30	
Location	: Building 3	User	: Administrator	
Up Time	: 0 Days 21 Hours 21 Minute	Stat	: P+ N4+ N6+ A+	

IPv4	: Enabled	IPv6	: Enabled	
Ping response	: Enabled			

HTTP	: Disabled	HTTPS	: Enabled	
FTP	: Disabled	Telnet	: Disabled	
SSH/SCP	: Enabled	SNMPv1	: Disabled	
SNMPv3	: Disabled			

Super User	: Enabled	RADIUS	: Disabled	
Administrator	: Disabled	Device User	: Disabled	
Read-only User	: Disabled	Network-Only User	: Disabled	
Type ? For command listing				
Use tcpip for IP address (-i), subnet (-s), and gateway (-g)				

pdu1686a

Two fields identify the operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the type of device that connects to the network (for example, a Rack PDU).

```
Network Management Card AOS      vx.x.x.x
RPDU APP                        vx.x.x.x
```

Three fields identify the system name, contact person, and location of the Rack PDU.

```
Name                Test Lab
Contact             Don Adams
Location            : Building 3
```

An Up Time field reports how long the Rack PDU Management Interface has been running since it was last turned on or reset.

Up Time: 0 Days, 21 Hours, 21 Minutes

Two fields identify when you logged in, by date and time.

```
Date:                11/2/2023
Time:                09:06:45
```

The `User` field identifies whether you logged in through the **Super User**, **Administrator**, **Device User**, or **Network-Only** account.

User: Administrator

A `Stat` field reports the Rack PDU status.

Stat: P+ N4+ N6+ A+

P+	The APC Operating System (AOS) is functioning properly.
----	---

IPv4 only	IPv6 only	IPv4 and IPv6*	Description
N+	N+	N4+ N6+	The network is functioning properly.
N?	N6?	N4? N6?	A BOOTP request cycle is in progress.
N-	N6-	N4- N6-	The Rack PDU failed to connect to the network.
N!	N6!	N4! N6!	Another device is using the Rack PDU IP address.
* The N4 and N6 values can be different from one another: you could, for example, have N4- N6+.			

A+	The application is functioning properly.
A-	The application has a bad checksum.
A?	The application is initializing.
A!	The application is not compatible with the AOS.

NOTE: If P+ is not displayed, contact the APC Customer Care Center at www.apc.com/support.

The remaining fields show which protocols and user accounts are enabled.

Using the CLI

At the CLI, you can use commands to configure the Rack PDU. To use a command, type the command and press ENTER. Commands, arguments, and options are case-sensitive.

While using the CLI, you can also do the following:

- Type `help` and press ENTER to view a list of available commands, based on your account type.
- Type `bye` to close the connection to the CLI.

Command Syntax

Item	Description
-	Options are preceded by a hyphen.
< >	Definitions of options are enclosed in angle brackets. For example: - i <ipv4 address>
[]	If a command accepts multiple options or an option accepts mutually exclusive arguments, the values may be enclosed in brackets.
	A vertical line between items enclosed in brackets or angle brackets indicates that the items are mutually exclusive. You must use one of the items.

Example of a command that supports multiple options:

```
tcpip [-m <manual | dhcp>] [-i <ipv4 address>] [-s <subnet mask>]  
[-g <gateway>]
```

In this example the `tcpip` command accepts any of the following options:

- `-m` defines the mode to assign the IP address
- `-i` defines the ipv4 address
- `-s` defines the subnet mask
- `-g` defines the gateway address

Example of a command that accepts mutually exclusive arguments for an option:

```
tcpip [-m <manual | dhcp>]
```

In this example, the option `-m` accepts only two arguments: `manual` or `dhcp`. For example, to set the manual network mode, type:

```
tcpip -m manual
```

The command will fail if you type an argument that is not specified.

Command Response Codes

The command response codes enable scripted operations to detect error conditions reliably without having to match error message text:

Code	Message	Code	Message
E000	Success	E200	Input error
E001	Successfully issued	E201	No response
E002	Reboot required for change to take effect	E202	User already exists
E100	Command failed	E203	User does not exist
E101	Command not found	E204	User does not have access to this command
E102	Parameter error	E205	Exceeds maximum users
E103	Command line error	E206	Invalid value
E104	User Level Denial	E207	Outlet command error: Device not initialized.
E105	Command Prefill	E208	Outlet command error: Previous command is pending
E106	Data Not Available	E209	Outlet Command Error: Database rejected request.
E107	Serial communication with the Rack PDU has been lost	E210	Outlet Command Error: Outlet restricted.
E108	EAPoL disabled due to invalid/encrypted certificate		

Network Management Card Command Descriptions

?

Access: Super User, Administrator, Device User, Network-Only User

Description: View a list of all the CLI commands available to your account type. To view help text for a specific command, type the command followed by a question mark.

Argument	Description
<command>	View help text for a specific command.

Example : To view a list of options that are accepted by the `alarmcount` command, type

```
apc> alarmcount ?
Usage: alarmcount -- Display Alarms
      alarmcount [-p <all | warning | critical |
informational>]
```

Error Message: E000, E102

about

Access: Super User, Administrator, Device User, Network-Only User

Description: View hardware and firmware information. This information is useful in troubleshooting and enables you to determine if updated firmware is available at the website.

Parameters: None

Error Message: E000

alarmcount

Access: Super User, Administrator, Device User, Network-Only User

Description: Displays alarms present in the system.

Parameters:

Option	Argument	Description
-p	all	View the number of active alarms reported by the Rack PDU. Information about the alarms is provided in the Event Log.
	warning	View the number of active warning alarms.
	critical	View the number of active critical alarms.
	informational	View the number of active informational alarms.

Example: To view all active warning alarms, type

```
apc> alarmcount -p warning
E000: Success
WarningAlarmCount: 0
```

Error Message: E000, E102

boot

Access: Super User, Administrator, Network-Only User

Description: Define how the Rack PDU will obtain its network settings, including the IP address, subnet mask, and default gateway. Then configure the BOOTP or DHCP server settings.

Parameters:

Option	Argument	Description
-b <boot mode>	dhcp bootp manual	Define how the TCP/IP settings will be configured when the Rack PDU turns on, resets, or restarts.
-c	[<enable disable>] (Require DHCP Cookie)	dhcp and dhcpBootp boot modes only. Enable or disable the requirement that the DHCP server provide the APC cookie.
The default values for these three settings generally do not need to be changed.		
-v	[<vendor class>]	APC.
-i	[<client id>]	The MAC address of the Rack PDU, which uniquely identifies it on the network.
-u	[<user class>]	The name of the application firmware module.

Example: To use a DHCP server to obtain network settings:

1. Type `boot -b dhcp`
2. Enable the requirement that the DHCP server provide the APC cookie:

```
apc> boot -c enable
E000: Success
```

Error Message: E000, E102

bye

Access: Super User, Administrator, Device User, Network-only User

Description: Exit the CLI session. This works the same as the `exit` or `quit` commands.

Parameters: None.

Example:

```
apc> bye  
Connection Closed - Bye
```

Error Message: None.

cd

Access: Super User, Administrator, Device User

Description: Navigate to a folder in the directory structure of the Rack PDU. The working directory is set back to the root directory '/' when the you log out of the CLI.

Parameters: <directory name>

Example 1: To change to the `ssh` folder and confirm that an SSH security certificate was uploaded to the Rack PDU,

1. Type `cd ssh` and press ENTER.
2. Type `dir` and press ENTER to list the files stored in the SSH folder.

Example 2: To return to the previous directory folder, type `cd . .`

Error Message: E000, E102

clrrst

Access: Super User, Administrator

Description: Clear the network interface reset reason. See lastrst, page 47 for more information on the reset reason.

Example: None

Error Message: None

console

Access: Super User, Administrator

Description: Define whether users can access the Command Line Interface using Telnet, which is disabled by default, or Secure SHell (SSH), which is enabled by default and provides protection by transmitting user names, passwords, and data in encrypted form. You can change the Telnet or SSH port setting for additional security. Alternately, disable network access to the Command Line Interface.

Parameters:

Option	Argument	Description
-S	<enable disable>	Enable or Disable SSH access to the device. Enabling SSH enables SCP.
-t	<enable disable>	Enable or Disable Telnet access to the device.
-pt	<telnet port n>	Define the Telnet port used to communicate with the Rack PDU (23 by default).
-ps	<SSH port n>	Define the SSH port used to communicate with the Rack PDU (22 by default).
-b	2400 9600 19200 38400	Configure the speed of the console port connection (9600 bps by default).

Example 1: To enable SSH access to the Command Line Interface, type
console -S enable

Example 2: To change the Telnet port to 5000, type
console -pt 5000

Error Message: E000, E102

date

Access: Super User, Administrator

Definition: Configure the date and time used by the Rack PDU.

NOTE: To configure an NTP server to define the date and time for the Rack PDU, see [ntp](#), page 49.

Parameters:

Option	Argument	Description
-d	<"datestring">	Set the current date. The format must match the current -f setting.
-t	<00:00:00>	Configure the current time, in hours, minutes, and seconds. Use the 24-hour clock format.
-f	mm/dd/yy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd	Select the numerical format in which to display all dates in this user interface. Each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.
-z	<time zone offset>	Set the difference with GMT in order to specify your time zone. This enables you to synchronize with other people in different time zones.

Example 1: To display the date using the format yyyy-mm-dd, type

```
date -f yyyy-mm-dd
```

Example 2: To define the date as October 30, 2009, using the format configured in the preceding example, type

```
date -d "2009-10-30"
```

Example 3: To define the time as 5:21:03 p.m., type

```
date -t 17:21:03
```

Error Message: E000, E100, E102

delete

Access: Super User, Administrator

Description: Delete a file in the file system. (To delete the event log, see eventlog, page 43.)

Parameters:

Argument	Description
<file name>	Type the name of the file to delete.

Example: To delete a file,

1. Navigate to the folder that contains the file. For example, to navigate to the logs folder, type
cd logs
2. To view the files in the logs folder, type
dir
3. To delete a file, type
delete <file name>

Error Messages: E000, E102

dir

Access: Super User, Administrator, Device User, Network-Only User

Description: View the files and folders stored on the Rack PDU.

Parameters: None

Example:

```
apc> dir
E000: Success
1024 Jan 2 4:34 apc_hw21_aos_2.5.0.8.bin
6249332 Jan 2 4:34 apc_hw21_rpdu2g_1.1.0.15.bin
45000 Sep 30 1996 config.ini
      0  Apr  23  18:53  db/
      0  Apr  23  18:53  ssl/
      0  Apr  23  18:53  ssh/
      0  Apr  23  18:53  logs/
      0  Apr  23  18:53  sec/
      0  Apr  23  18:53  fw1/
      0  Apr  23  18:53  email/
      0  Apr  23  18:53  eapol/
      0  Apr  23  18:53  tmp/
      0  Apr  23  18:53  upsfw/
```

Error Messages: E000

dns

Access: Super User, Administrator

Definition: Configure the manual Domain Name System (DNS) settings.

Parameters:

Option	Argument	Description
-OM	enable disable	Override the manual DNS. When this setting is enabled, configuration data from other sources (typically DHCP) takes precedence over the manual configuration set here.
-y	<enable disable>	System-hostname sync
-p	<primary DNS server>	Set the primary DNS server.
-s	<secondary DNS server>	Set the secondary DNS server.
-d	<domain name>	Set the domain name.
-n	<domain name IPv6>	Set the domain name IPv6.
-h	<host name>	Set the host name.

Example:

```
apc > dns -OM
E000: Success
Override Manual DNS Settings: enabled
```

Error Message: E000, E102

eapol

Access: Super User, Administrator

Description: Configure EAPoL (802.1X Security) settings.

Parameters:

Option	Argument	Description
-S	enable disable	Enable or disable EAPoL.
-n	<supplicant name>	Set the supplicant name.
-p	<private key passphrase>	Set the private key passphrase.

Example 1: To display the result of an `eapol` command:

```
apc>eapol
E000: Success
Active EAPoL
Settings
-----
-----
      Status:      enabled
      Supplicant   NMC-Supplicant
      Name:
      Passphrase:  <hidden>
      CA file      Valid Certificate
      Status
      Private Key   Valid Certificate
      Status
      Public Key    Valid Certificate
      Status
```

Example 2: To enable EAPoL:

```
apc>eapol -S enable
E000: Success
Reboot required for change to take effect.
```


email

Access: Super User, Administrator**Description:** Configure parameters for email, which the Rack PDU uses to send event notifications.**Parameters:**

Option	Argument	Description
-g[n]	<enable disable>	Enables (default) or disables sending email to the recipient.
-t[n]	<To Address>	The user and domain names of the recipient. To use email for paging, use the email address for the recipient's pager gateway account (for example, myacct100@skytel.com). The pager gateway will generate the page.
-o[n]	<long short> (Format)	The long format contains name, location, contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.
-l[n]	<Language Code>	The language which the email notification will be sent in. Only English is available at this time.
-r [n]	<Local recipient custom> (Route)	<p>Set the SMTP Server options:</p> <p>Local (recommended): Choose this option if your SMTP server is located on your internal network, or is set up for your e-mail domain. Choose this setting to limit delays and network outages. If you choose this setting, you must also enable forwarding at the SMTP server of the device, and set up a special external e-mail account to receive the forwarded e-mail. NOTE: Check with your SMTP server administrator before making these changes.</p> <p>Recipient: This setting sends email directly to the recipient's SMTP server, which is determined by an MX record lookup of the domain of the To: Address. The device tries only once to send the e-mail. A network outage or a busy remote SMTP server can cause a time-out and cause the e-mail to be lost. This setting requires no additional administrative tasks on the SMTP server. NOTE: When using this setting, the "From Address" will match the "To Address", authentication and encryption (TLS) will be disabled, and port 25 will be used.</p> <p>Custom: This setting allows each email recipient to have its own server settings. These settings are independent of the settings given by the <code>smtp</code> command.</p>
Custom Route Option		
-f[n]	<From Address>	<p>The contents of the From field in email messages sent by the Rack PDU in the format <code>user@ [IP_address]</code> if an IP address is specified as Local SMTP Server), or in the format <code>user@domain</code> if DNS is configured and the DNS name is specified as Local SMTP Server in the email messages.</p> <p>The local SMTP server may require that you use a valid user account on the server for this setting. See the server documentation.</p>
-s{n}	<SMTP Server>	The IPv4/ IPv6 address or DNS name of the local SMTP server. This definition is required only when the <code>-r</code> option is set to <code>Local</code> .
-p[n]	<Port>	The SMTP port number, with a default of 25. Common ports are 25 for unencrypted e-mail, and 465 and 587 for SSL/TLS encrypted e-mail. You can change the port setting to any port from 1 to 65535.
-a[n]	<enable disable> (Authentication)	Enable this if the SMTP server requires authentication.
-u[n]	<User Name>	If the SMTP server requires authentication, type the user name and password here. This performs a simple authentication, not SSL/TLS.
-w[n]	<Password>	
-e[n]	<none ifsupported always implicit>	<p>Specify when encryption is used.</p> <p>none: The SMTP server does not require or support encryption.</p> <p>ifsupported: The SMTP server advertises support for STARTTLS but doesn't require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given. This is typically used with port 25.</p> <p>always: The SMTP server requires the STARTTLS command to be sent on connection to the server. This is typically used with port 587.</p> <p>implicit: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server. This is typically used with port 465.</p>

Option	Argument	Description
-c[n]	<enable disable>	Require CA Root Certificate: This should be enabled if the security policy of your organization does not allow for implicit trust of SSL/TLS connections. If this is enabled, a valid CA certificate for the SMTP server must be installed to the Rack PDU's certificate store using the certificate loader in order for a TLS connection with the SMTP server to succeed.
-i[n]	<Certificate File Name>	This field is dependent on the root CA certificates installed on the Rack PDU and whether or not a root CA certificate is required.
n = Email Recipient Number (1,2,3 or 4)		

Example: To enable email to be sent to email recipient 1 with email address recipient1@apc.com, using the local SMTP server:

```
apc> email -gl enable -rl local -tl recipient1@apc.com
E000: Success
```

Error Message: E000, E102

eventlog

Access: Super User, Administrator, Device User

Description: View the date and time you retrieved the Event Log, the status of the Rack PDU, and the status of sensors connected to the Rack PDU. View the most recent device events and the date and time they occurred. Use the following keys to navigate the Event Log:

Parameters:

Key	Description
ESC	Close the Event Log and return to the Command Line Interface.
ENTER	Update the log display. Use this command to view events that were recorded after you last retrieved and displayed the log.
SPACEBAR	View the next page of the Event Log.
B	View the preceding page of the Event Log. This command is not available at the main page of the Event Log.
D	Delete the Event Log. Follow the prompts to confirm or deny the deletion. Deleted events cannot be retrieved.

Example:

```
apc> eventlog
---- Event Log -----
Date:05/30/2021 Time: 13:22:26
-----
Metered Rack PDU: Communication Established
Date          Time          User          Event
-----
2/9/2024      13:17:22      System        Set Time.
2/9/2024      13:16:57      System        Configuration change. Date format
2/9/2024      13:16:49      System        preference.
2/9/2024      13:16:49      System        Set Date.
2/9/2024      13:16:35      System        Configuration change. Date format
2/9/2024      13:16:08      System        preference.
2/9/2024      13:16:08      System        Set Date.
2/9/2024      13:15:30      System        Set Time.
2/9/2024      13:15:00      System        Set Time.
2/9/2024      13:13:58      System        Set Date.
2/9/2024      13:12:22      System        Set Date.
2/9/2024      13:12:08      System        Set Date.
2/9/2024      13:11:41      System        Set Date.
<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

Error Message: E000, E100

exit

Access: Super User, Administrator, Device User, Network-only User

Description: Exit the CLI session. This works the same as the `bye` or `quit` commands.

Parameters: None.

Example:

```
apc> exit
Bye
```

Error Message: None.

firewall

Access: Super User, Administrator

Description: Enable, disable, or configure the internal Rack PDU firewall feature.

Parameters:

Parameters	Argument	Description
-S	<enable disable>	Enable or disable the firewall.
-f	<file name to activate>	Name of the firewall to activate.
-t	<file name to test> <duration time in minutes>	Name of firewall to test and duration time in minutes.
-fe		Shows active file errors.
-te		Shows test file errors.
-c		Cancel a firewall test.
-r		Shows active firewall rules.
-l		Shows firewall activity log.
-Y		Skip firewall test prompt.

Example: To enable the firewall policy file *example.fwl*, type

```
apc> firewall -f example.fwl
E000: Success
```

Error Message: E000, E102

format

Access: Super User, Administrator

Description: Reformat the file system of the Rack PDU and erase all security certificates, encryption keys, configuration settings, and the event and data logs. Be careful with this command.

NOTE: You must confirm by entering “YES” when prompted.

NOTE: To reset the Rack PDU to its default configuration, use the `resetToDef` command instead.

Parameters:

Option	Definition
-f	This will delete all configuration data, event and data logs, certificates and keys. Network settings will NOT be preserved.
-p	This will delete all configuration data, event and data logs, certificates and keys. Network settings WILL be preserved.

Example:

```
apc> format -p
```

```
Format FLASH file system
```

```
Warning: This will delete all configuration data,
         event and data logs, certs and keys.
```

```
All network configuration settings WILL be preserved.
```

```
Enter 'YES' to continue or <ENTER> to cancel: YES
```

Error Message: None

ftp

Access: Super User, Administrator

Description: Enable or disable access to the FTP server. Optionally, change the port setting to the number of any unused port from 5001 to 32768 for added security.

NOTE: The system will reboot if any configuration is changed.

NOTE: FTP is disabled by default, and Secure CoPy (SCP) is automatically enabled when the Super User password is set via SSH.

Parameters:

Option	Argument	Definition
-p	<port number> (valid ranges are: 21 and 5000-32768)	Define the TCP/IP port that the FTP server uses to communicate with the Rack PDU (21 by default). The FTP server uses both the specified port and the port one number lower than the specified port.
-s	<enable disable>	Configure access to the FTP server.

Example: To change the TCP/IP port to 5001, type

```
apc> ftp -p 5001
E000: Success
```

Error Message: E000, E102

help

Access: Super User, Administrator, Device User, Network-Only User

Description: View a list of all the CLI commands available to your account type. To view help text for a specific command, type the command followed by `help`.

Parameters: [<command>]

Example 1: To view a list of commands available to someone logged on as a Device User, log on to the CLI as the Device User, then type
`help`

Example 2: To view a list of options that are accepted by the `alarmcount` command, type

```
apc> alarmcount help
Usage: alarmcount -- Display Alarms
      alarmcount [-p <all | warning | critical |
      informational>]
```

lang

Access: Super User, Administrator, Device User

Description: Displays the language in use.

Parameters: None

Example:

```
apc> lang
E000: Success
```

```
Languages
enUs - English
```

Error Message: None

lastrst

Access: Super User, Administrator

Description: View the last network interface reset reason. Use the output of this command to troubleshoot network interface issues with the guidance of technical support.

Option	Description
02 NMI Reset	The network interface was reset via the Reset button on the Rack PDU front display.
09 Coldstart Reset	The network interface was reset by removing power from the hardware.
12 WDT Reset	The network interface was reset via a firmware command.

Parameters: None

Example:

```
apc> lastrst
09 Coldstart Reset
E000: Success
```

Error Message: E000, E102

ledblink

Access: Super User, Administrator

Description: Sets the status LED to blink for the specified amount of time. Use this command to help visually locate the Rack PDU.

Parameters:

Argument	Definition
<time>	Number of minutes to blink the LED.

Example:

```
apc> ledblink 1
E000: Success
```

Error Message: E000, E102

logzip

Access: Super User, Administrator

Description: Creates a single, compressed archive of the log files available from the NMC and Rack PDU. These files can be used by technical support to troubleshoot issues.

Parameters:

Option	Argument	Definition
-m	<email recipient> (1-4)	The identifying number (1-4) of the email recipient to which the zip file will be sent. Enter the number of one of the four possible email recipients configured.

Example:

```
apc> logzip -m 1
Generating files
/dbg/debug_ZA1023006009.tar
Emailing log files to email recipient - 1
E000: Success
```

Error Message: E000, E102

netstat

Access: Super User, Administrator

Description: View the status of the network and all active IPv4 and IPv6 addresses.

Parameters: None

Example:

```
apc> netstat
Current IP Information:
Family    mHome    Type      IPAddress                Status
IPv6      4         auto      FE80::2CO:B7FF:FE51:F304/64 configured
IPv6      0         manual    ::1/128                   configured
IPv4      0         manual    127.0.0.1/32              configured
```

Error Message: E000, E10

ntp

Access: Super User, Administrator

Description: View and configure the Network Time Protocol parameters.

Parameters:

Option	Argument	Definition
-OM	enable disable	Override the manual settings.
-p	<primary NTP server>	Specify the primary server.
-s	<secondary NTP server>	Specify the secondary server.
-e	enable disable	Enable or disable the use of NTP.
-u	<update now>	Immediately update the Rack PDU time from the NTP server.

Example 1: To enable the override of manual setting, type
`ntp -OM enable`

Example 2: To specify the primary NTP server, type
`ntp -p 150.250.6.10`

Error Message: E000, E102

ping

Access: Super User, Administrator, Device User, Network-Only User

Description: Determine whether the device with the IP address or DNS name you specify is connected to the network. Four inquiries are sent to the address.

Parameters:

Option	Argument	Description
n/a	<IP address or DNS name>	Type an IP address with the format xxx.xxx.xxx.xxx, or the DNS name configured by the DNS server.
-t		Ping until stopped.

Example: To determine whether a device with an IP address of 192.168.1.50 is connected to the network, type

```
apc> ping 192.168.1.50
E000: Success
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
```

Error Message: E000, E100, E102

portSpeed

Access: Super User, Administrator, Network-Only User

Description: Define the communication speed of the Ethernet port.

NOTE: The Port Speed setting can be changed to 1000 Mbps. However, this change can only be made via the Web UI.

Parameters:

Option	Arguments	Description
-s	auto 10H 10F 100H 100F	<p>auto enables the Ethernet devices to negotiate to transmit at the highest possible speed.</p> <p>H = Half Duplex (communication in only one direction at a time)</p> <p>F = Full Duplex (communication in both directions simultaneously)</p> <p>10 = 10 Megabits</p> <p>100 = 100 Megabits</p>

Example: To configure the TCP/IP port to communicate using 100 Mbps with half-duplex communication, type

```
apc> portspeed -s 100H
E000: Success
Reboot required for change to take effect.
```

Error Message: E000, E102

prompt

Access: Super User, Administrator, Device User, Network-Only User

Description: Configure the command line interface prompt to include or exclude the account type of the currently logged-in user. Any user can change this setting; all user accounts will be updated to use the new setting.

Parameters:

Option	Argument	Description
-s	long	The prompt includes the account type of the currently logged-in user.
	short	The default setting. The prompt is four characters long: apc>

Example:

```
apc> prompt -s long
E000: Success
```

```
Administrator@apc>prompt -s short
E000: Success
```

Error Message: E000, E102

pwd

Access: Super User, Administrator, Device User, Network-Only User

Description: Output the path of the current working directory.

Parameters: None

Example:

```
apc> pwd
/
```

```
apc> cd logs
E000: Success
```

```
apc> pwd
/logs
```

Error Message: E000, E102

quit

Access: Super User, Administrator, Device User, Network-only User

Description: Exit the CLI session. This works the same as the `exit` or `bye` commands.

Parameters: None.

Example:

```
apc> quit
Bye
```

Error Message: None.

radius

Access: Super User, Administrator, Network-Only User

Description: View the existing RADIUS settings and configure basic authentication parameters for up to two RADIUS servers. Additional authentication parameters are available in the Web UI.

For detailed information about configuring your RADIUS server, see the *Network Management Card 3 Security Handbook*.

Parameters:

Option	Argument	Description
-a	<local radiusLocal radius>	Configure RADIUS authentication: local = RADIUS is disabled. Local authentication is enabled. radiusLocal = RADIUS, then Local Authentication. RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used. radius = RADIUS is enabled. Local authentication is disabled.
-p1 -p2	<server IP>	The server name or IP address of the primary or secondary RADIUS server.
-o1 -o2	<port>	The port number of the primary or secondary RADIUS server. NOTE: RADIUS servers use port 1812 by default to authenticate users. The Rack PDU supports ports 1 to 65535.
-s1 -s2	<server secret>	The shared secret between the primary or secondary RADIUS server and the Rack PDU.
-t1 -t2	<server timeout>	The time in seconds that the Rack PDU waits for a response from the primary or secondary RADIUS server.

Example 1: To view the existing RADIUS settings for the Rack PDU, type `radius` and press ENTER.

Example 2: To configure a 10-second timeout for a secondary RADIUS server, type

```
apc> radius -t2 10
E000: Success
```

Error Message: E000, E102

reboot

Access: Super User, Administrator, Network-Only User

Description: Restart the network management interface of the Rack PDU only. This does not affect the output power of the Rack PDU.

Option	Description
-Y	Skip confirmation prompt (Uppercase Y only)

Example 1:

```
apc> reboot
E000: Success
Reboot Management Interface
Enter 'YES' to continue or <ENTER> to cancel: YES
Rebooting...
```

Example 2:

```
apc> reboot -Y
E000: Success
Reboot Management Interface
Rebooting...
```

Error Message: E000, E100

resetToDef

Access: Super User, Administrator

Description: Reset all configurable parameters to their defaults. Delete all accounts and clear Event and Data Logs.

NOTE: Certain non-configurable parameters are not reset using `resetToDef`, and can only be erased from the Rack PDU by formatting the file system using the `format` command.

Parameters:

Option	Arguments	Description
-p	all keepip	<p>Caution: This resets all configurable parameters to their defaults.</p> <p>all = Reset all configuration changes, including event actions, device settings, and TCP/IP settings.</p> <p>keepip = Reset all configuration changes, <i>except</i> for the TCP/IP settings.</p>

Example: To reset all of the configuration changes *except* the TCP/IP settings, type

```
apc> resettodef -p keepip
Reset to Defaults Except TCP/IP
Enter 'YES' to continue or <ENTER> to cancel: YES
```

Error Message: E000, E100

session

Access: Super User, Administrator

Description: Records who is logged in (user), the interface, the address, time and ID.

Parameters:

Option	Arguments	Description
-d	[-d <session nID>] (Delete)	Delete the session for the current user with the specified session ID.
-m	<enable disable> (MultiUser Enable)	Enable to allow two or more users to log on at the same time. Disable to allow only one user to log in at a time.
-a	<enable disable> (Remote Authentication Override)	The Rack PDU supports RADIUS storage of passwords on a server. Enable Remote Authentication Override to allow a local user to log on using a username and password for the Rack PDU that is stored locally on the Rack PDU.

Example:

```
apc> session
User      Interface  Address          Logged In Time    ID
-----
apc       Telnet      10.169.118.1-    00:00:03          19
          00
E000: Success
```

Error Message: E000, E102

smtp

Access: Super User, Administrator, Network-Only User

Description: Configure the settings for the local e-mail server.

Parameters:

Option	Arguments	Description
-f	<From Address>	The address from which e-mail will be sent by the Rack PDU.
-s	<SMTP Server>	The IPv4/IPv6 address or DNS name of the local SMTP server.
-p	<Port>	The SMTP port number, 25 by default. Common ports are 25 for unencrypted e-mail, and 465 and 587 for SSL/TLS encrypted e-mail. You can change the port setting to any port from 1 to 65535.
-a	<enable disable>	Enable this if your SMTP server requires authentication.
-u	<User Name>	If the SMTP server requires authentication, type the user name and password here.
-w	<Password>	
-e	<none ifavail always implicit>	<p>Encryption options:</p> <p>none: The SMTP server does not require/support encryption.</p> <p>ifavail: The SMTP server advertises support for STARTTLS but does not require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given. This is typically used with port 25.</p> <p>always: The SMTP server requires the STARTTLS command to be sent upon connection to the server. This is typically used with port 587.</p> <p>implicit: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server. This is typically used with port 465.</p>
-c	<enable disable>	<p>Require CA Root Certificate.</p> <p>This should be enabled if the security policy of your organization does not allow for implicit trust of SSL/TLS connections. If this is enabled, a valid CA certificate for the SMTP server must be installed to the Rack PDU's certificate store using the certificate loader in order for a TLS connection with the SMTP server to succeed.</p>
-i	<certificate file name>	The file name of the certificate.

Example:

```
apc> smtp
E000: Success
```

```

From:          address@example.com
Server:        mail.example.com
Port:          25
Auth:          disabled
User:          User
Password:      <not set>
Encryption:    none
Req. Cert:     disabled
Cert File:     <n/a>
```

Error Message: E000, E102

snmp

Access: Super User, Administrator, Network-Only User

Description: Enable or disable and configure SNMPv1.

NOTE: SNMPv1 is disabled by default. The Community Name (`-c [n]`) must be set before SNMPv1 communications can be established.

Parameters:

Option	Arguments	Description
<code>-S</code>	<code><enable disable></code>	Enable or disable SNMPv1
<code>-c [n]</code>	<code><Community></code>	Specify a community name or string.
<code>-a [n]</code>	<code><read write writeplus disable></code>	Indicate the usage rights.
<code>-n [n]</code>	<code><IP or Domain Name></code>	Specify the IPv4/IPv6 address or the domain name of the Network Management Station.
[n] = the access control number: 1,2,3, or 4.		

Example: To enable SNMP version1, type

```
apc> snmp -S enable
E000: Success
Reboot required for change to take effect.
```

Error Message: E000, E102

snmpv3

Access: Super User, Administrator

Description: Enable or disable and configure SNMPv3.

NOTE: SNMPv3 is disabled by default. A valid user profile must be enabled with passphrases (-a [n], -c [n]) set before SNMPv3 communications can be established.

Parameters:

Option	Arguments	Description
-s	<enable disable>	Enable or disable SNMPv3
-u [n]	<User Name>	Specify a user name, an authentication phrase and encryption phrase.
-a [n]	<Auth phrase>	
-c [n]	<Crypt phrase>	
-ap [n]	<sha md5 none>	Indicate the type of authentication protocol.
-pp [n]	<aes des none>	Indicate the privacy (encryption) protocol.
-ac [n]	<enable disable>	Enable or disable access.
-au [n]	<User profile name>	Give access to a specified user profile.
-n [n]	<IP or Domain Name>	Specify the IPv4/IPv6 address or the hostname for the Network Management Station.
[n] = Access Control # = 1, 2, 3, through 8		

Example: To give access level 2 to user "JMurphy", type

```
apc> snmpv3 -au2 "JMurphy"
```

```
E000: Success
```

*Reboot required for change to take effect

Error Message: E000, E102

snmptrap

Access: Super User, Administrator, Network-Only User

Description: Enable or disable SNMP trap generation

Parameters:

Option	Arguments	Description
-c[n]	<Community>	Specify a community name or string.
-r[n]	<Receiver NMS IP>	The IPv4/IPv6 address or host name of the trap receiver.
-l[n]	<Language code>	Specify a language. English (enUS) is the only available option at this time.
-t[n]	[snmpV1 snmpV3]	Specify the trap type: SNMPv1 or SNMPv3.
-p[n]	<Port>	Specify the SNMP trap port number for this trap receiver (162 by default). The range is 1 to 65535.
-g[n]	[enable disable]	Enable or disable trap generation for this trap receiver. Enabled by default.
-a[n]	[enable disable]	Enable or disable authentication of traps for this trap receiver, SNMPv1 only.
-u[n]	<profile1 profile2 profile3 profile4>	Select the identifier of the user profile for this trap receiver, SNMPv3 only.
n = Trap receiver # = 1, 2, 3, 4, 5, or 6		

Example: To enable and configure an SNMPv1 trap for Receiver 1, with the Community Name of public, receiver 1 IP address of 10.169.118.100, using the default English language, type

```
apc> snmptrap -c1 public -r1 10.169.118.100 -l1 enUS -t1
snmpV1 -g1 enable
E000: Success
```

Error Message: E000, E102

ssh

Access: Super User, Administrator, Network-Only User

Description: Show, delete, and generate SSH server keys.

NOTE: You must use the `ssh key` command to use the options below.

Parameters:

Option	Argument	Description
-s		Display the current SSH server key in use.
-f		Display the current SSH server key's fingerprint.
-d		Delete the current SSH server key in use.
-i	<filename>.p15	Import the SSH server key from a PKCS #15 file.
-ecdsa	<256> (bit size)	Generate an Elliptic Curve Digital Signature Algorithm (ECDSA) SSH server key with the specified size in bits.
-rsa	<1024 2048 4096> (bit size)	Generate a Rivest–Shamir–Adleman (RSA) SSH server key with the specified size in bits.

Example 1: To delete the SSH server key, type

```
apc> ssh key -d
E000: Success
```

Example 2: To import the SSH server key from a .p15 file generated by the NMC Security Wizard CLI Utility, type

```
apc> ssh key -i nmc.p15
E000: Success
```

Error Messages: E000, E102

ssl

Access: Super User, Administrator, Network-Only User

Description: Configure and manage the Rack PDU's public key and Web UI certificate, and create a Certificate Signing Request (CSR).

NOTE: There are three sets of options for this command, indicated below (key, csr, and cert).

Configure public keys (key):

Option	Argument	Description
-s		Display the current public key in use.
-d		Delete the current public key in use.
-i	<filename>.p15	Import the public key from a PKCS #15 file.
-ecdsa	<256 384 521>	Generate an Elliptic Curve Digital Signature Algorithm (ECDSA) public key with the specified size in bits.
-rsa	<1024 2048 4096>	Generate a Rivest–Shamir–Adleman (RSA) public key with the specified size in bits.

*You can generate a PKCS#15 file with the NMC Security Wizard (available on www.apc.com).

Example 1: To generate a new ECDSA-521 public key, type

```
apc> ssl key -ecdsa 521
E000: Success
```

Example 2: To import the public key from a .p15 file generated by the NMC Security Wizard CLI Utility, type

```
apc> ssl key -i nmc.p15
E000: Success
```

Configure Certificate Signing Request (csr):

Option	Argument	Description
-s	<File Name>	Show the current CSR. If no file path is specified, the command checks the default location: ssl/nmc.csr.
-q	<File Name>	Create a CSR from an active configuration. If no file path is specified, the CSR is stored at the default location: ssl/nmc.csr
-CN	<Common Name>	Create a custom CSR. The Common Name is the fully qualified domain name (FQDN) of the Rack PDU. For example, its IP address or *.nmc.local.
Custom Certificate Signing Request (CSR) options. NOTE: The options below are only available for -CN		
-O	<organization>	The name of your organization.
-OU	<organization unit>	The division of your organization handling the certificate.
-C	<country>	The two-letter country code of where your organization is located.
-san	<Common Name IP Address>	The Common Name or IP address of the Rack PDU.

NOTE: Created Certificate Signing Requests will be stored in the Rack PDU's ssl directory. See [dir](#), page 38.

Example 3: To create a quick CSR from the current configuration, type

```
apc> ssl csr -q
E000: Success
```

Example 4: To create a minimal CSR, type

```
apc> ssl csr -CN 192.168.1.100 -C US
E000: Success
```

Example 5: To create a custom Certificate Signing Request (CSR), type

```
apc> ssl csr -CN apcXXXXXX.nmc.local -C US -san *.nmc.local
-san 190.0.2.0
E000: Success
```

Configure the Web UI's certificate (cert):

Option	Argument	Description
-s	<File Name>	Display the specified certificate. NOTE: Executing this option without an argument will display the current certificate in use.
-f	<File Name>	Display the specified certificate's fingerprint. NOTE: Executing this option without an argument will display the current certificate's fingerprint.
-i	<File Name>	Import a certificate.
NOTE: The argument is optional for all three options. If no file path is specified, the command checks the default location: ssl/nmc.crt.		

Example 6: To show the active certificate, type

```
apc> ssl cert -s
E000: Success
```

Certificate

```
-----
Serial Number: XXXXXxxxxxxxxxxxxx
Issuer: CN=., C=US
Validity:
    Not Before: Mon Oct 11 16:46:44 2021 UTC
    Not After : Sat Dec 15 23:59:59 2035 UTC
Subject: CN=., C=US
Subject Public Key Info:
    Public Key Algorithm: ECDSA (256 bit)
    X:
        xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
        xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
    Y:
        xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
        xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
    Curve: P-256

Thumbprint: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Fingerprint:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Example 7: To display nmc.crt located in the ssl directory, type

```
ssl cert -s ssl/nmc.crt
```

Example 8: To import another certificate (*other.crt*), type

```
apc> ssl cert -i other.crt
```

Error Messages: E000, E102

system

Access: Super User, Administrator

Description: View and set the system name, the contact, the location. Configure system messages, view up time as well as the date and time, the logged-on user, and the high-level system status P, N, A. (See [About the Main Screen](#), page 29 for more information about system status).

Parameters:

Option	Argument	Description
-n	<system name>	Define the device name, the name of the person responsible for the device, and the physical location of the device. NOTE: If you define a value with more than one word, you must enclose the value in quotation marks. These values are also used by StruxureWare Data Center Expert, or EcoStruxure IT Expert and the Rack PDU's SNMP agent.
-c	<system contact>	
-l	<system location>	
-m	<system message>	Show a configurable custom message or banner on the logon page of the Web UI, CLI (Serial, Telnet, SSH), FTP or SCP.
-s	<enable disable>	Allow the host name to be synchronized with the system name so both fields automatically contain the same value. This is the same as using "dns -y". NOTE: When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the host name field).

Example 1: To set the device location as Test Lab, type

```
apc> system -l "Test Lab"
E000: Success
```

Example 2: To set the system name as Don Adams, type

```
apc> system -n "Don Adams"
E000: Success
```

Error Message: E000, E102

tcpip

Access: Super User, Administrator

Description: View and manually configure IPV4 TCP/IP settings for the Rack PDU.

Parameters:

Option	Argument	Description
-s	enable disable	Enable or disable TCP/IP v4.
-i	<IPv4 address>	Type the IP address of the Rack PDU, using the format xxx.xxx.xxx.xxx
-s	<subnet mask>	Type the subnet mask for the Rack PDU.
-g	<gateway>	Type the IP address of the default gateway. Do not use the loopback address (127.0.0.1) as the default gateway.
-d	<domain name>	Type the DNS name configured by the DNS server.
-h	<host name>	Type the host name that the Rack PDU will use.

Example 1: To view the network settings of the Rack PDU, type

```
apc> tcpip
E000: Success
IP Address:      192.168.1.50
MAC Address:     XX XX XX XX XX XX
Subnet Mask:     255.255.255.0
Gateway:         192.168.1.1
Domain Name:     example.com
Host Name:       HostName
```

Example 2: To manually configure an IP address of 192.168.1.49, type

```
apc> tcpip -i 192.168.1.49
E000: Success
Reboot required for change to take effect
```

Error Message: E000, E102

tcpip6

Access: Super User, Administrator

Description: Enable IPv6. View and manually configure these network settings for the Rack PDU:

Parameters:

Option	Argument	Description
-S	enable disable	Enable or disable IPv6.
-man	enable disable	Enable manual addressing for the IPv6 address of the Rack PDU.
-auto	enable disable	Enable the Rack PDU to automatically configure the IPv6 address
-i	<IPv6 address>	Set the IPv6 address of the Rack PDU
-g	<IPv6 gateway>	Set the IPv6 address of the default gateway
-d6	router stateful stateless never	Set the DHCPv6 mode, with parameters of router controlled, stateful (for address and other information, they maintain their status), stateless (for information other than address, the status is not maintained), or never.

Example 1: To view the network settings of the Rack PDU, type `tcpip6` and press ENTER.

```
apc> tcpip6
E000: Success
```

```
IPv6:                      enabled
Manual Settings:           disabled

IPv6 Address:              ::/64
MAC Address:               XX XX XX XX XX XX
Gateway:                   ::
IPv6 Manual Address:       disabled
IPv6 Autoconfiguration:    enabled
DHCPv6 Mode:               router controlled
```

Example 2: To manually configure an IPv6 address of 2001:0:0:0:FFD3:0:57ab for the, type

```
tcpip -i 2001:0:0:0:0:FFD3:0:57ab
```

Error Message: E000, E102

user

Access: Super User, Administrator

Description: Configure the user name, password, and inactivity timeout for each account type.

NOTE: You can't edit a user name; you must delete it and then create a new user.

NOTE: To change the Super User account settings remotely, you must enter the current password (`-cp`).

Parameters:

Option	Argument	Description
<code>-n</code>	<code><user></code>	Indicate the user.
<code>-cp</code>	<code><current password></code>	For a Super User, you must specify the current password. NOTE: The <code>-cp</code> option is only required when changing the Super User's settings remotely.
<code>-pw</code>	<code><user password></code>	Specify these options for a user. NOTE: The description must be enclosed in quotation marks.
<code>-pe</code>	<code><user permission></code>	
<code>-d</code>	<code><user description></code>	
<code>-e</code>	<code>enable disable</code>	Enable or disable access for the particular user account.
<code>-te</code>	<code>enable disable</code>	Enable or disable touch screen access.
<code>-tp</code>	<code><touch screen access pin></code>	This option is only available on certain devices.
<code>-tr</code>	<code>enable disable</code>	Enable the touch screen remote authorization override. This option is only available on certain devices. If you enable this override, the Rack PDU will allow a local user to log on using the password for the Rack PDU that is stored locally on the Rack PDU.
<code>-st</code>	<code><session timeout></code>	Specify how long a session lasts when the keyboard is idle before the user is automatically logged off.
<code>-sr</code>	<code>enable disable</code>	Bypass RADIUS by using the serial console (CLI) connection, also known as Serial Remote Authentication Override
<code>-el</code>	<code>enable disable</code>	Indicate the Event Log color coding.
<code>-lf</code>	<code>tab csv</code>	Indicate the format for exporting a log file.
<code>-ts</code>	<code>us metric</code>	Indicate the temperature scale, Fahrenheit or Celsius.
<code>-df</code>	<code><mm/dd/yyyy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd></code>	Specify a date format.
<code>-lg</code>	<code><language code (e.g. enUs)></code>	Specify a user language. English is the only available language at this time.
<code>-del</code>	<code><user name></code>	Delete a user.
<code>-l</code>		Display the current user list.

Example 1: To change the log off time to 10 minutes for user "JMurphy", type `user -n "JMurphy" -st 10`

Example 2: To change the log off time to 10 minutes for the Super User "apc", type `user -n "apc" -cp <password> -st 10`

Error Message: E000, E102

userdflt

Access: Super User, Administrator

Description: Complimentary function to “user” establishing default user preferences. There are two main features for the default user settings:

- Determine the default values to populate in each of the fields when the Super User or Administrator-level account creates a new user. These values can be changed before the settings are applied to the system.
- For remote users (user accounts not stored in the system that are remotely authenticated such as RADIUS) these are the values used for those that are not provided by the authenticating server. For example, if a RADIUS server does not provide the user with a temperature preference, the value defined in this section will be used.

Parameters:

Options	Argument	Description
-e	<enable disable>	By default, user will be enabled or disabled upon creation.
-pe	<Administrator Device Network-Only>	Specify the user's permission level and account type.
-d	<user description>	Provide a user description. The description must be enclosed in quotation marks.
-st	<session timeout> minute(s)	Provide a default session timeout.
-bl	<bad login attempts>	Number of incorrect login attempts a user has before the system disables their account. Upon reaching this limit, a message is displayed informing the user the account has been locked. The Super User or an Administrator-level account is needed to re-enable the account to allow the user to log back in. NOTE: A Super User account cannot be locked out, but can be manually disabled if necessary.
-el	<enable disable> (Event Log Color Coding)	Enable or disable event log color coding.
-lf	<tab csv> (Export Log Format)	Specify the log export format, tab or CSV.
-ts	<us metrics> (Temperature Scale)	Specify the user's temperature scale. This setting is also used by the system when a user preference is not available (for example, email notifications).
-df	<mm/dd/yyyy dd.mm.yyyy mmm-dd-yy dd- mmm-yy yyyy-mm-dd> (Date Format)	Specify the user's preferred date format.
-lg	<language code (enUs, etc)>	User language. Only enUs is supported at this time.
-sp	<enable disable>	Strong password requirements. When enabled: <ul style="list-style-type: none"> • The password must be 8–64 characters long. • The password must contain at least one lowercase letter, one uppercase letter, one number, and one symbol (! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~).
-pp	<interval in days>	Required password change interval.

Example: To set the default user's session timeout to 60 minutes, type

```
apc> userdflt -st 60
```

```
E000: Success
```

Error Message: E000, E102

web

Access: Super User, Administrator

Description: Enable access to the Web UI using HTTP or HTTPS.

For additional security, you can change the port setting for HTTP and HTTPS to any unused port from 5000 to 32768. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114, type:

```
http://152.214.12.114:5000
```

Parameters:

Option	Argument	Definition
-h	enable disable	Enable or disable access to the user interface for HTTP. HTTP is disabled by default.
-s	enable disable	Enable or disable access to the user interface for HTTPS. HTTPS is enabled by default. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate.
-mp	<minimum protocol>	Specify the minimum protocol used by the web interface: SSL v3.0, TLS v1.1, or TLS v1.2.
-ph	<http port #>	Specify the TCP/IP port used by HTTP to communicate with the Rack PDU (80 by default). The other available range is 5000–32768.
-ps	<https port #>	Specify the TCP/IP port used by HTTPS to communicate with the Rack PDU (443 by default). The other available range is 5000–32768.
-lsp	enable disable	Enable or disable access to the Limited Status page in the Web UI.
-lsd	enable disable	Enable or disable the Limited Status page being used as the default page when accessing the device's IP or hostname in a web browser.
-cs	<0 1 2 3 4>	Select the level of security of TLS v1.2 cipher suites between 0 - 4, where 4 is the highest level of security, and 0 is the lowest level of security. The default value is 4. NOTE: The -cs option is only applied when -mp is set to TLS v1.2. When a value between 0 - 4 is entered, the CLI responds with a list of the currently allowed SSL cipher suites.
-hs	enable disable	Enable/ disable the HTTP Strict Transport Security Header (HSTS) response header.

Example 1: To prevent all access to the Web UI, type

```
apc> web -h disable -s disable
```

Example 2: To define the TCP/IP port used by HTTP, type

```
apc> web -ph 80
E000: Success
```

Error Message: E000, E102

whoami

Access: Super User, Administrator, Device User, Network-Only User

Description: Provides login information on the current user.

Parameters: None

Example:

```
apc> whoami  
E000: Success  
admin
```

Error Message: E000, E102

xferINI

Access: Super User, Administrator

Description: Use XMODEM to upload an INI file while you are accessing the Command Line Interface through a serial connection. After the upload completes:

- If there are any system or network changes, the Command Line Interface restarts and you must log on again.
- If you selected a baud rate for the file transfer that is not the same as the default baud rate for the NMC, you must reset the baud rate to the default to reestablish communication with the NMC.

Parameters: None

Example:

```
apc> xferINI
Enter 'YES' or 'Y' to continue or <ENTER> to cancel: <user
enters 'YES' or 'Y'>
---- File Transfer Baud Rate-----
      1- 2400
      2- 9600
      3- 19200
      4- 38400
> <user enters baudrate selection>
Transferring at current baud rate (9600), press <ENTER>...
<user presses <ENTER>>
Start XMODEM-CRC Transfer Now!
CC
<user starts sending INI>
150 bytes have successfully been transmitted.

apc>
```

Error Message: None

xferStatus

Access: Super User, Administrator

Description: View the result of the last file transfer.

Parameters: None

Example:

```
apc> xferStatus
E000: Success
```

Result of last file transfer: Successful

See for descriptions of the transfer result codes.

Error Message: E000

Device Command Descriptions

Network Port Sharing Commands

The CLI allows commands to be sent to guest Rack PDUs. The user may specify the Display ID of the Rack PDU to be commanded, followed by a colon, before the first argument (or as the first argument, if the command does not normally have arguments). If a Display ID is optional, omitting it will simply command the local Rack PDU.

For example: `<command> [<id#>:]<arg1> <arg2>`

This will send `<command> <arg1> <arg2>` to the Rack PDU with the Display ID specified by `<id#>:.` The Display ID is followed by a colon (:), which is followed by `arg1` with no spaces. Spaces are used to delimit arguments.

alarmList

Access: Super User, Administrator, Device User

Description: Displays alarms present on the device (or another device in the group if NPS is used.)

Parameters: None

Example: To view all active warning systems, enter

```
apc > alarmList
-----Device Alarm Status-----
      1 Critical Alarm Present.
-----
[Critical] rack PDU 1: Internal power supply #2 fault, under
voltage.
      <ESC>- Exit, <ENTER>- Refresh
```

Error Message: E102

bkLowLoad

Access: Super User, Administrator, Device User

Description: Set or view the bank low-load threshold current in amps. You can specify all banks, a single bank, a range, or a comma-separated list of single banks and/or ranges.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all bank#>	all = all bank numbers bank# = a single number, a range of numbers separated with a dash, or a comma-separated list of single bank number and/or number ranges
<current>	The new bank threshold (Amps)

NOTE: The maximum bank number is 2. If the Rack ATS has two circuit breakers, a total bank threshold is provided.

Example 1: To view low-load thresholds for all banks, enter

```
apc> bkLowLoad all
E000: Success
total:  0 A
1:      0 A
2:      0 A
```

Example 2: To view and set the low-load threshold for bank 1, enter

```
apc> bkLowLoad 1
E000: Success
1: 0 A

apc> bkLowLoad 1 1
E000: Success
```

Example 3: To view and set the low-load thresholds for banks 1–2, enter

```
apc> bkLowLoad 1-2
E000: Success
total:  2 A
1:      1 A
2:      1 A

apc> bkLowLoad 1-2 1
E000: Success
```

Error Messages: E000, E102

bkNearOver

Access: Super User, Administrator, Device User

Description: Set or view the bank near-overload threshold current in amps. Only single phase models with two or more circuit breakers support this command. You can specify all banks, a single bank, a range, or a comma-separated list of single banks and/or ranges.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all bank#>	all = all bank numbers bank#: = a single number, a range of numbers separated with a dash, or a comma-separated list of single bank number and/or number ranges
<current>	The new bank threshold (Amps)

Example 1: To view and set the near-overload threshold for all banks, enter

```
apc> bkNearOver all
E000: Success
total: 10 A
1:      10 A
2:      10 A

apc> bkNearOver all 10
E000: Success
E000: Success
E000: Success
```

Example 2: To view and set the near-overload threshold for bank 1, enter

```
apc> bkNearOver 1
E000: Success
1:      10 A

apc> bkNearOver 1 12
E000: Success

apc> bkNearOver all
E000: Success
total: 12 A
1:      12 A
2:      10 A
```

Example 3: To view the near-overload threshold setting for banks 1 and 2 on guest unit 3, enter

```
apc> bkNearOver 3:1-2
E000: Success
1: 16 A
2: 16 A
```

Error Messages: E000, E102

bkOverLoad

Access: Super User, Administrator, Device User

Description: Set or view the bank overload threshold current in amps. Only single phase SKUs with two or more circuit breakers support this command.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all bank#>	all = all bank numbers bank#: = a single number, a range of numbers separated with a dash, or a comma-separated list of single bank number and/or number ranges
<current>	The new bank threshold (Amps)

Example 1: To view bank overload thresholds for all banks, enter

```
apc> bkOverLoad all
E000: Success
total:  24 A
1:      14 A
2:      14 A
```

Example 2: To view the overload threshold for bank 1, enter

```
apc> bkOverLoad 1
E000: Success
1: 14 A
```

Example 3: To set the overload threshold for banks 1 and 2, enter

```
apc> bkOverLoad 1-2 16
E000: Success

apc> bkOverLoad all
E000: Success
total:  32 A
1:      16 A
2:      16 A
```

Error Messages: E000, E102

bkPeakLoad

Access: Super User, Administrator, Device User

Description: Display the peak load measurement from a bank(s). Only single phase SKUs with two or more circuit breakers support this command.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all bank#>	all = all bank numbers bank# : = a single number, a range of numbers separated with a dash, or a comma-separated list of single bank number and/or number ranges
<current>	The new bank threshold (Amps)

Example:

```
apc> bkPeakLoad all
E000: Success
total:  11.0 A
1:      5.0 A
2:      5.0 A
```

```
apc> bkPeakLoad 1
E000: Success
1:      5.0 A
```

```
apc> bkPeakLoad 1-2
E000: Success
1:      5.0 A
2:      6.0 A
```

Error Messages: E000, E102

bkReading

Access: Super User, Administrator, Device User

Description: View the current reading (measurement) in amps for a bank. Only single phase models with two or more circuit breakers support this command.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all bank#>	all = all bank numbers bank#: = a single number, a range of numbers separated with a dash, or a comma-separated list of single bank number and/or number ranges
<current>	The new bank threshold (Amps)

Example :

```
apc> bkReading 1
E000: Success
1:      6.3 A
```

```
apc> bkReading all
E000: Success
total:  11.4 A
1:      6.3 A
2:      5.1 A
```

```
apc> bkReading 1-2
E000: Success
1:      6.3 A
2:      5.1 A
```

Error Messages: E000, E102

bkRestrictn

Access: Super User, Administrator, Device User

Description: View or set or the overload restriction feature to prevent users from applying power to outlets when an overload threshold is violated.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all phase#>	all = all bank numbers phase# = a single number, a range of numbers separated with a dash, or a comma-separated list of single bank number and/or number ranges
<none near over>	Set the overload restriction.

Example 1: To set the overload restriction for phase three to none, enter

```
apc> bkRestrictn 3 none
E000: Success
```

Example 2: To view the overload restrictions for all phases, enter

```
apc> bkRestrictn all
E000: Success
1: over
2: near
3: none
```

Example 3: To view the overload restrictions for all phases on guest Rack PDU 2, enter

```
apc> bkRestrictn 2:all
E000: Success
1: None
2: None
```

Error Messages: E000, E102

devLowLoad

Access: Super User, Administrator, Device User

Description: Set or view the low-load threshold in kilowatts for the device.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
Threshold	New power threshold (Kilowatts)

Example 1: To view the low-load threshold, enter

```
apc> devLowLoad
E000: Success
0.5 kW
```

Example 2: To set the low-load threshold to 1 kW, enter

```
apc> devLowLoad 1.0
E000: Success
```

Error Messages: E000, E102

devNearOver

Access: Super User, Administrator, Device User

Description: Set or view the near-overload threshold in kilowatts for the Rack PDU.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
Threshold	New threshold (Kilowatts)

Example:

```
apc> devNearOver 21.3
E000: Success
```

```
apc> devNearOver
E000: Success
21.3 kW
```

Error Messages: E000, E102

devOverLoad

Access: Super User, Administrator, Device User

Description: Set or view the overload threshold in kilowatts for the device.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
Threshold	New threshold (Kilowatts)

Example:

```
apc> devOverLoad 3 25.5  
E000: Success
```

```
apc> devOverLoad 3  
E000: Success  
25.5 kW
```

Error Messages: E000, E102

devPeakLoad

Access: Super User, Administrator, Device User

Description: Display the peak power measurement from the device.

Parameters: None.

Example:

```
apc> devPeakLoad  
E000: Success  
0.0 kW
```

Error Messages: E000, E102

devReading

Access: Super User, Administrator, Device User

Description: View the total power in kilowatts or total energy in kilowatt-hours for the device.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
power	View the total power in kilowatts.
energy	View the total energy in kilowatt-hours.
appower	View the total apparent power in kVA.
pf	View the power factor

Example 1: To view the total power, enter

```
apc> devReading power
E000: Success
5.2 kW
```

Example 2: To view the total energy, enter

```
apc> devReading energy
E000: Success
200.1 kWh
```

Error Messages: E000, E102

devStartDly

Access: Super User, Administrator, Device User

Description: Set or view the amount of time in seconds, which is added to each outlet's Power On Delay before the outlet will turn on after power is applied to the Switched Rack PDU. Allowed values are within the range of 1 to 300 seconds or never (never turn on).

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<time never>	Cold start delay time in whole seconds, or never

Example 1: To view the cold start delay, enter

```
apc> devStartDly
E000: Success
5 seconds
```

Example 2: To set the cold start delay to six seconds, enter

```
apc> devStartDly 6
E000: Success
```

Example 3: To set the cold start delay to six seconds on guest Rack PDU 2, enter

```
apc> devStartDly 2:6
E000: Success
```

Example 4: To view the cold start delay on guest Rack PDU 2, enter

```
apc> devStartDly 2:
E000: Success
6 sec
```

Error Messages: E000, E102

dispID

Access: Super User, Administrator

Description: Sets or view the device's Display ID.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
new_id	Set the Display ID.

Example:

```
apc> dispID
E000: Success
RPDU ID: 1*
apc> dispID 2
E000: Success
RPDU ID: 2*
apc> dispID 3: 2
E000: Success
```

Error Messages: E000, E102

humAlGen

Access: Super User, Administrator, Device User

Description: View or set whether humidity alarms are enabled or disabled.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	all = all sensors sensor name = the name configured for a specific sensor sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges
<enable disable>	Enable or disable humidity alarms.

Example 1: View alarm generation status for all sensors when there is no NPS group.

```
apc> humAlGen all
E000: Success
1: Enabled
2: Enabled
3: Enabled
```

Example 2: View and disable alarm generation for sensor 1 on guest Rack PDU 3.

```
apc> humAlGen 3:1
E000: Success
1: Enabled

apc> humAlGen 3:1 disable
E000: Success

apc> humAlGen 3:1
E000: Success
1: Disabled
```

Error Messages: E000, E102

humHyst

Access: Super User, Administrator, Device User

Description: Set and read the hysteresis for the humidity threshold.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	<p>all = all sensors</p> <p>sensor name = the name configured for a specific sensor</p> <p>sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges</p>
<hysteresis>	New hysteresis value (% RH)

Example 1: View the hysteresis for all sensors when there is no NPS group.

```
apc> humHyst all
E000: Success
1: 1 %RH
2: 1 %RH
3: 1 %RH
```

Example 2: View and set the hysteresis for sensor 1 on guest Rack PDU 3.

```
apc> humHyst 3:1
E000: Success
1: 1 %RH

apc> humHyst 3:1 2
E000: Success

apc> humHyst 3:1
E000: Success
1: 2 %RH
```

Error Messages: E000, E102

humLow

Access: Super User, Administrator, Device User

Description: Set or view the low humidity threshold as a percent of the relative humidity.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	all = all sensors sensor name = the name configured for a specific sensor sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges
<humidity>	New low humidity threshold

Example 1: View the threshold for all sensors when there is no NPS group.

```
apc> humLow all
E000: Success
1: 15 %RH
2: 15 %RH
3: 15 %RH
```

Example 2: View and set the threshold for sensor 1 on guest Rack PDU 3.

```
apc> humLow 3:1
E000: Success
1: 15 %RH

apc> humLow 3:1 16
E000: Success

apc> humLow 3:1
E000: Success
1: 16 %RH
```

Error Messages: E000, E102

humMin

Access: Super User, Administrator, Device User

Description: Set or view the minimum humidity threshold as a percent of the relative humidity.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	<p>all = all sensors</p> <p>sensor name = the name configured for a specific sensor</p> <p>sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges</p>
[humidity]	New minimum humidity threshold

Example 1: View the threshold for all sensors when there is no NPS group.

```
apc> humMin all
E000: Success
1: 10 %RH
2: 10 %RH
3: 10 %RH
```

Example 2: View and set the threshold for sensor 1 on guest Rack PDU 3.

```
apc> humMin 3:1
E000: Success
1: 10 %RH

apc> humMin 3:1 12
E000: Success

apc> humMin 3:1
E000: Success
1: 12 %RH
```

Error Messages: E000, E102

humReading

Access: Super User, Administrator, Device User

Description: View the humidity reading from attached Temperature/Humidity sensors.

NOTE: You must connect at least one Temperature/Humidity sensor (EPDU-TH3) to the Rack PDU to use this command.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	<p>all = all sensors</p> <p>sensor name = the name configured for a specific sensor</p> <p>sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges</p>

Example 1: View the humidity for all sensors when there is no NPS group.

```
apc> humReading 1
E000: Success
1: 25 %RH
2: 26 %RH
3: 25 %RH
```

Example 2: View the humidity for sensor 1 on guest Rack PDU 3.

```
apc> humReading 3:1
E000: Success
1: 25 %RH
```

Error Messages: E000, E102, E201

humStatus

Access: Super User, Administrator, Device User

Description: Display the status of the Temperature/Humidity sensor.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	<p>all = all sensors</p> <p>sensor name = the name configured for a specific sensor</p> <p>sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges</p>

Example 1: View the status for all sensors when there is no NPS group.

```
apc> humStatus all
E000: Success
1: Normal
2: Normal
3: Normal
```

Example 2: View the status for sensor 1 on guest Rack PDU 3.

```
apc> humStatus 3:1
E000: Success
1: Normal
```

Error Messages: None

lcd

Access: Super User, Administrator, Device User

Description: View or set the state of the LCD on the display interface.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
< on off >	Turn the LCD On or Off.

Example 1:

```
apc> lcd off
E000: Success
```

Example 2:

```
apc> lcd 1: on
E000: Success
```

Error Messages: E000, E100, E102

lcdBlink

Access: Super User, Administrator, Device User

Description: Blink the LCD back-light for the specified period of time.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
< time >	The number of minutes (1–10) to blink the display. Press any button on the display interface to cancel the blink duration.

Example:

```
apc> lcdBlink 3
E000: Success
```

Error Messages: E000, E102

logToFlash

Access: Super User, Administrator

Description: Export the log files to a USB flash drive. The file will be a compressed file. It will contain *event.txt*, *config.ini*, *debug.txt*, and *data.txt* files. If an exception occurs, it will also contain *dump.txt*.

Parameters:

Argument	Description
<name>	The appendix to the log file tar name. If no name is entered, the serial number of the device will be used as the name for the debug file.

Example 1:

```
apc> logToFlash 01292018
Creating report file: /debug_01292018.tar
Press <ESC> to abort
0% completed...
Exporting logs... please do not remove USB flash
12% completed...Exporting logs... please do not remove USB
flash...
Exporting logs... please do not remove USB flash
60% completed...
Logs export completed. You may remove USB flash now
```

Example 2:

```
apc> logToFlash
Creating report file: /debug_ZA1234567890.tar
Press <ESC> to abort
0% completed...Exporting logs... please do not remove USB
flash
12% completed...Exporting logs... please do not remove USB
flash...
Exporting logs... please do not remove USB flash
60% completed...Logs export completed. You may remove USB
flash now
```

Error Messages: E000, E102

modbus

Access: Super User, Administrator

Description: View and configure the options for Modbus TCP. The Modbus TCP allows a Building Management System (BMS) to monitor the Rack ATS device.

Parameters:

Option	Argument	Description
-tE	<enable disable>	Enable or disable Modbus TCP.
-tP		View the Modbus TCP port number. (You can set the Modbus TCP port number in the Web UI.)
-tTO	<0 – 64800>	Specify the Modbus TCP communication timeout in seconds, where 0 indicates that the connection never times out.
-ka	<enable disable>	Modbus TCP keep-alive. Sends data packet to the server every two hours and 75 seconds if there is no other communication. Prevents communication timeout when the communication timeout is set to 7,275 seconds or more.
-rDef		Reset the Modbus configuration to defaults.

Example 1: To view modbus settings, type

```
apc> modbus
E002: Success

Slave Address = 0x1
Status = DISABLED
TCP Status = DISABLED
TCP Port Number = 502
TCP Communication Timeout = 5 secs
Keep-alive = ENABLED
```

Example 2: To enable modbus TCP, type:

```
apc> modbus -tE enable
E002: Success
Reboot required for change to take effect.
```

Error Messages: E000, E002, E101, E102

phBal

Access: Super User, Administrator, Device User

Description: Sets or read the phase load balance threshold. Only applies to models with two or more metered phases.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<current>	The new phase load balance threshold (Amps).

Example:

```
apc> phBal 13
E000: Success
apc> phBal
E000: Success
13A
```

Error Messages: E000, E102

phBalAlGen

Access: Super User, Administrator, Device User

Description: Set or read whether phase load balance alarms are enabled or disabled. Only applies to models with two or more metered phases.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<enable disable>	Enable or disable phase load balance alarms.

Example:

```
apc> phBalAlGen enable
E000: Success
apc> phBalAlGen disable
E000: Success
```

Error Messages: E000, E102

phLowLoad

Access: Super User, Administrator, Device User

Description: Set or view the phase low-load threshold.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all phase#>	Select the outlets: all = All device outlets. phase# = A single number or a range of numbers separated with a dash, or a comma-separated list of single phase numbers and number ranges.
<current>	The new phase threshold (Amps).

Example 1: To set the low-load threshold for all phases to 1 A, enter

```
apc> phLowLoad all 1
E000: Success
```

Example 2: To view the low-load threshold for phases 1 through 3, enter

```
apc> phLowLoad 1-3
E000: Success
1: 1 A
2: 1 A
3: 1 A
```

Error Messages: E000, E102

phNearOver

Access: Super User, Administrator, Device User

Description: Set or view the phase near-overload threshold.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all phase#>	Select the outlets: all = All device outlets. phase# = A single number or a range of numbers separated with a dash, or a comma-separated list of single phase numbers and number ranges.
<current>	The new phase threshold (Amps).

Example 1: To set the near-overload threshold for all phases to 10 A, enter

```
apc> phNearOver all 10
E000: Success
```

Example 2: To view the near-overload threshold for phases 1 through 3, enter

```
apc> phNearOver 1-3
E000: Success
1: 10 A
2: 10 A
3: 10 A
```

Error Messages: E000, E102

phOverLoad

Access: Super User, Administrator, Device User

Description: Set or view the phase overload threshold.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all phase#>	Select the outlets: all = All device outlets. phase# = A single number or a range of numbers separated with a dash, or a comma-separated list of single phase numbers and number ranges.
<current>	The new phase threshold (Amps).

Example 1: To set the overload threshold for all phases to 13 A, enter

```
apc> phOverLoad all 13
E000: Success
```

Example 2: To view the overload threshold for phases 1 through 3, enter

```
apc> phOverLoad 1-3
E000: Success
1: 13 A
2: 13 A
3: 13 A
```

Error Messages: E000, E102

phPeakCurr

Access: Super User, Administrator, Device User

Description: Display the peak current measurement from one or more phases.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all phase#>	Select the outlets: all = All device outlets. phase# = A single number or a range of numbers separated with a dash, or a comma-separated list of single phase numbers and number ranges.

Example:

```
apc> phPeakCurr 2
E000: Success
2: 0.0 A
apc> phPeakCurr all
E000: Success
1: 0.0 A
2: 0.0 A
3: 0.0 A
```

Error Messages: E000, E102

phReading

Access: Super User, Administrator, Device User

Description: View the current, voltage, or power for a phase. Set or view the phase near-overload threshold in kilowatts. You can specify all phases, a single phase, a range, or a comma-separated list of phases.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all phase#>	Select the outlets: all = All device outlets. phase# = A single number or a range of numbers separated with a dash, or a comma-separated list of single phase numbers and number ranges.
< current voltage power appower pf >	

Example 1: To view the measurement for current for phase 3, enter

```
apc> phReading 3 current
E000: Success
3: 4 A
```

Example 2: To view the voltage for each phase, enter

```
apc> phReading all voltage
E000: Success
1: 120 V
2: 120 V
3: 120 V
```

Example 3: To view the power for phase 2 on guest Rack PDU 3, enter

```
apc> phReading 3:2 power
E000: Success
2: 40 W
```

Error Messages: E000, E102

phRestrictn

Access: Super User, Administrator

Description: Set or view the overload restriction feature to prevent outlets from turning on when the overload alarm threshold is violated.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all phase#>	Select the outlets: all = All device outlets. phase# = A single number or a range of numbers separated with a dash, or a comma-separated list of single phase numbers and number ranges.
[none near over]	none = No overload restriction. near = Outlets do not turn on when the near overload threshold (phNearOver) is violated. over = Outlets do not turn on when the overload threshold (phOverLoad) is violated.

Example 1: To set the overload restriction for phase three to none, enter

```
apc> phRestrictn 3 none
E000: Success
```

Example 2: To view the overload restrictions for all phases, enter

```
apc> phRestrictn all
E000: Success
1: over
2: near
3: none
```

Error Messages: E000, E102

prodInfo

Access: Super User, Administrator, Device User

Description: View information about the Rack PDU.

Parameters:

Argument	Description
<id#: all>	<p>id#: = The id of a unit in the NPS group (can be 1–8 depending on the group size)</p> <p>all = All rack PDUs in the NPS group.</p> <p>No argument = Host Rack PDU in an NPS group.</p>

Example:

```

apc> prodInfo
E000: Success
RPDU ID: 1*
AOS X.X.X
Metered-by-Outlet Rack PDU X.X.X Model: AP8XXX
Name: room555Main
Location: Room 555
Contact: (xxx) 555-1234
Present Outlets: XX
Switched Outlets: XX
Metered Outlets: XX
Max Current: XX A
Phases: X
Banks: X
Uptime: 0 Days 21 Hours 21
Minutes
NPS Type: Host
NPS Status: Active
Network Link: Link Active

```

Error Messages: E000

sensorName

Access: Super User, Administrator, Device User

Description: Set or view the name assigned to the Rack PDU Temp/Humidity sensor.

NOTE: You must connect at least one Temperature/Humidity sensor (EPDU-TH3) to the Rack PDU to use this command.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	<p>all = all sensors</p> <p>sensor name = the name configured for a specific sensor</p> <p>sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges</p>
<new name>	The new name for the sensor.

Example 1: View the names for all sensors when there is no NPS group.

```
apc> sensorName all
E000: Success
1: Sensor 1
2: Sensor 2
3: Sensor 3
```

Example 2: View and set the name for sensor 1 on guest Rack PDU 3.

```
apc> sensorName 3:1
E000: Success
1: Sensor 1

apc> sensorName 3:1 TempHum3-1
E000: Success

apc> sensorName 3:1
E000: Success
1: TempHum3-1
```

Error Messages: E000, E102

tempAlGen

Access: Super User, Administrator, Device User

Description: View or set whether temperature alarms are enabled or disabled.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	all = all sensors sensor name = the name configured for a specific sensor sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges
<enable disable>	Enable or disable temperature alarms.

Example 1: View alarm generation status for all sensors when there is no NPS group.

```
apc> tempAlGen all
E000: Success
1: Enabled
2: Enabled
3: Enabled
```

Example 2: View and disable alarm generation for sensor 1 on guest Rack PDU 3.

```
apc> tempAlGen 3:1
E000: Success
1: Enabled

apc> tempAlGen 3:1 disable
E000: Success

apc> tempAlGen 3:1
E000: Success
1: Disabled
```

Error Messages: E000, E102

tempHigh

Access: Super User, Administrator, Device User

Description: Set or view the high-temperature threshold in either Fahrenheit or Celsius.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	<p>all = all sensors</p> <p>sensor name = the name configured for a specific sensor</p> <p>sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges</p>
<F C>	F = Fahrenheit. C = Celsius.
<temperature>	New high-temperature threshold

Example 1: View the threshold in Celsius for all sensors when there is no NPS group.

```
apc> tempHigh all C
E000: Success
1: 59 C
2: 59 C
3: 59 C
```

Example 2: View and set the threshold for sensor 1 on guest Rack PDU 3.

```
apc> tempHigh 3:1 C
E000: Success
1: 59 C

apc> tempHigh 3:1 C 60
E000: Success

apc> tempHigh 3:1 C
E000: Success
1: 60 C
```

Error Messages: E000, E102

tempHyst

Access: Super User, Administrator, Device User

Description: Set and read the hysteresis for the temperature thresholds.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	all = all sensors sensor name = the name configured for a specific sensor sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges
<F C>	F = Fahrenheit. C = Celsius.
<hysteresis>	New hysteresis value

Example 1: View the hysteresis in Celsius for all sensors when there is no NPS group.

```
apc> tempHyst all
E000: Success
1: 1 C
2: 1 C
3: 1 C
```

Example 2: View and set the hysteresis for sensor 1 on guest Rack PDU 3.

```
apc> tempHyst 3:1 C
E000: Success
1: 1 C

apc> tempHyst 3:1 C 2
E000: Success

apc> tempHyst 3:1 C
E000: Success
1: 2 C
```

Error Messages: E000, E102

tempMax

Access: Super User, Administrator, Device User

Description: Set or view the maximum-temperature threshold in either Fahrenheit or Celsius.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	all = all sensors sensor name = the name configured for a specific sensor sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges
< F C >	F = Fahrenheit C = Celsius
<temperature>	New maximum temperature threshold.

Example 1: View the threshold in Celsius for all sensors when there is no NPS group.

```
apc> tempMax all C
E000: Success
1: 60 C
2: 60 C
3: 60 C
```

Example 2: View and set the threshold for sensor 1 on guest Rack PDU 3.

```
apc> tempMax 3:1 C
E000: Success
1: 60 C

apc> tempMax 3:1 C 62
E000: Success

apc> tempMax 3:1 C
E000: Success
1: 62 C
```

Error Messages: E000, E102

tempReading

Access: Super User, Administrator, Device User, Outlet User

Description: View the temperature readings attached Temperature/Humidity sensors in either Fahrenheit or Celsius.

NOTE: You must connect at least one Temperature/Humidity sensor (EPDU-TH3) to the Rack PDU to use this command.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	all = all sensors sensor name = the name configured for a specific sensor sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges
< F C >	F = Fahrenheit C = Celsius

Example 1: View the temperature in Celsius for all sensors when there is no NPS group.

```
apc> tempReading all C
E000: Success
1: 23.5 C
2: 22.6 C
3: 23.3 C
```

Example 2: View the temperature for sensor 1 on guest Rack PDU 3.

```
apc> tempReading 3:1 F
E000: Success
1: 51.1 F
```

Error Messages: E000, E102, E201

tempStatus

Access: Super User, Administrator, Device User

Description: Displays the status of the Temperature/Humidity sensor.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–8 depending on the group size)
<all sensor name sensor#>	<p>all = all sensors</p> <p>sensor name = the name configured for a specific sensor</p> <p>sensor# = a single number, a range of numbers separated with a dash, or a comma-separated list of single sensor numbers and/or number ranges</p>

Example 1: View the status for all sensors when there is no NPS group.

```
apc> tempStatus all
E000: Success
1: Normal
2: Normal
3: Normal
```

Example 2: View the status for sensor 1 on guest Rack PDU 3.

```
apc> tempStatus 3:1
E000: Success
1: Normal
```

Error Messages: None.

Web User Interface (Web UI)

You can use Microsoft® Edge or Google® Chrome® or Mozilla® Firefox® to access the Rack PDU through its web User Interface (web UI). Other commonly available browsers may work but have not been fully tested by APC.

Log On to the Web UI

You can use the System IP address of the Rack PDU for the URL address of the web UI. Use your case-sensitive username and password to log on.

The default username and password for the **Admin** are both “apc”. The **Admin** can create **General Users**. **General Users** define their own usernames and passwords.

On first use, you will be forced to change the default **Admin** account password. The password will require at least one lowercase character, one uppercase character, one number, and one symbol.

DHCP is enabled by default. The auto-assigned IP address can be requested from the **Network Status** page in the LCD display of the Rack PDU. On your computer, type the IP address of the Rack PDU in your web browser’s URL address field (e. g., <https://192.168.0.162> or <http://192.168.0.16> if HTTP is your access protocol) and press ENTER.

If needed, you can assign a static IP address to the Rack PDU using a serial connection to the CLI or Web UI.

URL Address Formats

Type the DNS name or IP address of the Rack PDU in the web browser's URL address field and press ENTER. Until HTTP is enabled, you must include `https://` in the URL. When you specify a non-default Web server port in Internet Explorer, you must include `http://` or `https://` in the URL.

Common Browser Error Messages at Log On

Error Message	Browser	Cause of the Error
"This page cannot be displayed."	Internet Explorer	Web access is disabled, or the URL was not correct.
"Unable to connect."	Firefox	

URL Format Examples

NOTE: HTTP is disabled by default, and HTTPS is enabled by default.

- For a DNS name of Web1:
`http://Web1` if HTTP is your access mode
`https://Web1` if HTTPS (HTTP with SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133 and the default Web server port (80):
`http://139.225.6.133` if HTTP is your access mode
`https://139.225.6.133` if HTTPS (HTTP with SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133 and a non-default Web server port (5000):
`http://139.225.6.133:5000` if HTTP is your access mode
`https://139.225.6.133:5000` if HTTPS (HTTP with SSL/TLS) is your access mode
- For a System IPv6 address of 2001:db8:1::2c0:b7ff:fe00:1100 and a non-default Web server port (5000):
`http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` if HTTP is your access mode
`https://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` if HTTPS (HTTP with SSL/TLS) is your access mode

First Log On

When you log on to the Rack PDU for the first time, you will be prompted to change the default Super User account password (**apc**). After you log in, you will be directed to the **Configuration Summary** screen. This screen is an overview of all system protocols, and their current values (for example, enabled or disabled). You can access this screen at any time afterwards by following the path: **Configuration > Network > Summary**.

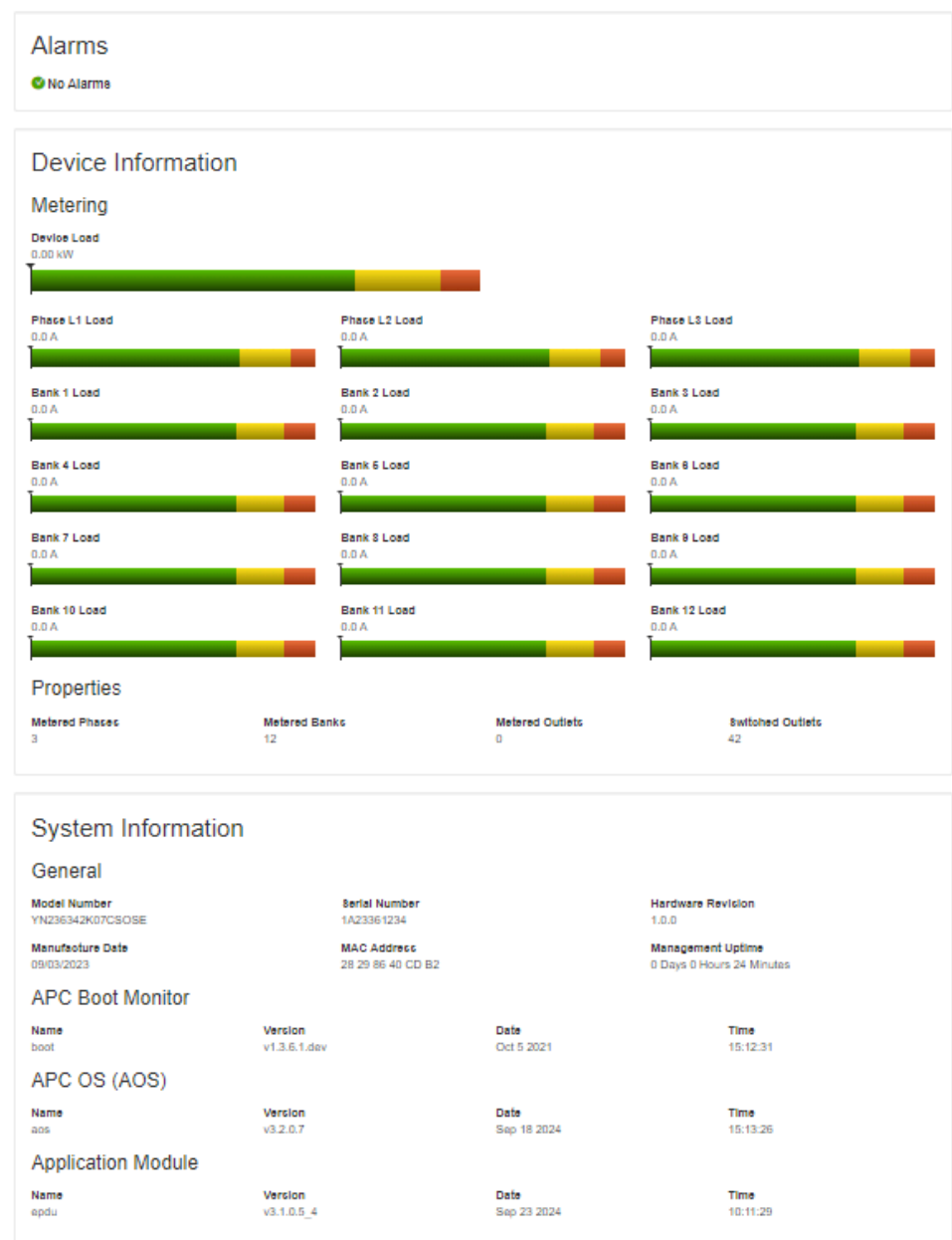
Limited Status Page

The **Limited Status** page provides limited information about the Rack PDU without requiring you to log on. Using a web browser, access the Rack PDU's IP address to view the log on page. When enabled, there is a **Limited Status** hyperlink toward the lower right corner of the frame.

The screenshot shows a web interface for logging into an EcoStruxure IT device. The page has a white background with a grey border. At the top left, the word "Login" is displayed in green. Below it, there are two input fields: "User Name" and "Password". The "User Name" field has a green border and a small icon of a person. The "Password" field has a grey border and a small icon of a key. To the right of the "Password" field, there are two buttons: "Log On" (green) and "Reset" (grey). Below the "Log On" button, there is a green link labeled "Limited Status" with a mouse cursor pointing at it. At the bottom left, the "EcoStruxure IT" logo is shown, with the tagline "Innovation At Every Level" and the text "Monitor your devices and get alarms wherever you go" and "Activate your EcoStruxure IT Expert free 30-day trial". At the bottom right, the "Schneider Electric" logo is displayed.

When you click **Limited Status** instead of the regular user name / password fields, a limited summary of device and system information is shown. A **Log On** hyper link provides access to the standard **Log On** page.

Limited Status



© 2024, Schneider Electric. All rights reserved.
Updated: 04/05/2019 at 19:05

You can enable or disable the Limited Status page under **Configuration > Network > Web > Access**.

Web UI Features

Read this section to get familiar with basic web UI features for your Rack PDU.




Tabs

The following tabs are available:

- **Home:** This is the default tab when you log on. View active alarms, the load status of the Rack PDU.
- **Status:** This tab shows the status of the Rack PDU. The **RPDU** sub-tab covers the status of alarms, bank and outlets. The **Network** sub-tab covers just the network.
- **Control:** This tab covers two topics: **Outlet** and **Reset/Reboot**.
- **Configuration:** This tab covers **RPDU**, **Outlet Group**, **Email**, **Thresholds**, **Network**, **SNMP**, **Date/Time**, **File Upgrade**, and **User**.
- **Tests:** The Tests tab allows you to blink the display LCD and the Network LED for a set amount of time.
- **Logs:** This tab covers more information which will be further discussed later in the Logs section of the document.
- **About:** The About tab will be further discussed later in the About section of the document.

Device Status Icons

One or more icons and accompanying text indicate the current operating status of the Rack PDU.

Icon	Description
	No Alarms: No alarms are present, and the Rack PDU and NMC are operating normally.
	Warning: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
	Critical: A critical alarm exists, which requires immediate action.

At the upper right corner of every page, the quick status area displays the same icons currently displayed on the Home page to report the Rack PDU status:

- The **No Alarms** icon is displayed if no alarms exist.
- One or both of the other icons (**Critical** and **Warning**) are displayed if any alarms exist. After each icon, the number of active alarms of that severity is also displayed.

You can click any icon in the quick status area to navigate to the **Home** screen.

Quick Links

There are three configurable links at the lower-left corner of each Web UI page. By default, the links access these Web pages:

- Link 1: The home page of APC website
- Link 2: The Frequently Asked Questions (FAQ) page of the APC website
- Link 3: Additional information on EcoStruxure IT

The following links are located in the upper-right corner of each Web UI page:

- Your user name: Select this link to change user preferences.
- The current UI language: Only English is supported at this time.
- **Log Off:** Select this link to log the current user off of the Web UI.
- **Help:** Select this link to view context-sensitive information.

Network Port Sharing (NPS) On the Web UI

The Web UI of the Rack PDU will have additional capabilities if the Rack PDU is part of an NPS group. This includes an NPS Group Status Web page and an NPS Group Configuration page. In addition, for Web pages that support NPS Rack PDUs, the user can select a different Rack PDU in the group to view by selecting the Rack PDU Display ID of the unit he or she would like to view.

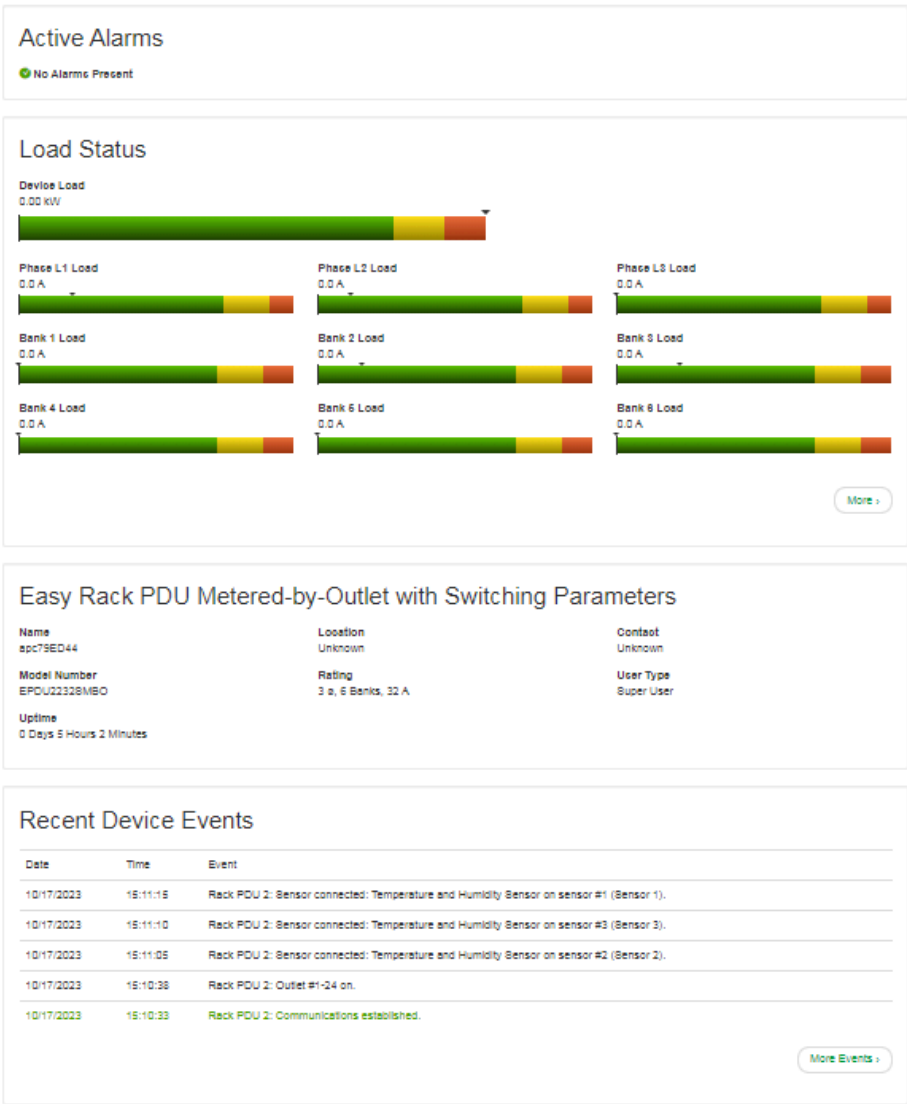
Each Rack PDU in the NPS group is denoted with a Rack PDU icon followed by its Display ID (1 to 16). The Rack PDU that the user is logged into is displayed with an additional asterisk (*) following the Display ID.

NOTE:

The **Reset/Reboot** page has many additional reset/reboot options for Rack PDU groups. These include individual Rack PDU reset to defaults, individual Rack PDU rebooting, and clearing of guest PDU lost communication alarms by removing the guests from the group.

About the Home Page

Home



The **Home** page contains the information about **Active Alarms**, **Load Status**, device information (**Rack PDU Parameters**), and **Recent Device Events**.

Active Alarms will show if any alarms exist. If no alarms exist, a green check mark with the words **No Alarms Present** will show.

The **Load Status** area shows the load for the Rack PDU in kW. The load for the phases and banks is shown in amps, as applicable. The green, yellow, and red meter shows the current load status: normal, near overload, or overload, respectively. If a low load threshold is configured, the meter will also include a blue section for low load conditions. To see the device status, select the **More >** link at the bottom of the list.

The **Parameters** show the **Name**, **Location**, **Contact**, **Model Number**, **Rating**, **User** (type of user account accessing the Rack PDU), and **Uptime** (the amount of time the Rack PDU has been operating since the last reboot from either a power cycle or a reboot of the network management Interface).

The **Recent Device Events** area shows the events which have occurred most recently and the dates and times they occurred. A maximum of five events are shown at one time. Click **More Events** to view the entire event log.

Status


The **Status** menu allows you to view information about the Rack PDU.

View Alarms, NPS Groups, and Load Status

Path: Status > RPDU > Alarms

Status

Device Alarm Status

 No Alarms Present

View the alarm status of the Rack PDU.

Path: Status > RPDU > Group

Network Port sharing Group Status. List the Properties, Metering and firmware version information. You can access the **Change Host RPDU** link at the bottom of the page.

Path: Status > RPDU > Device

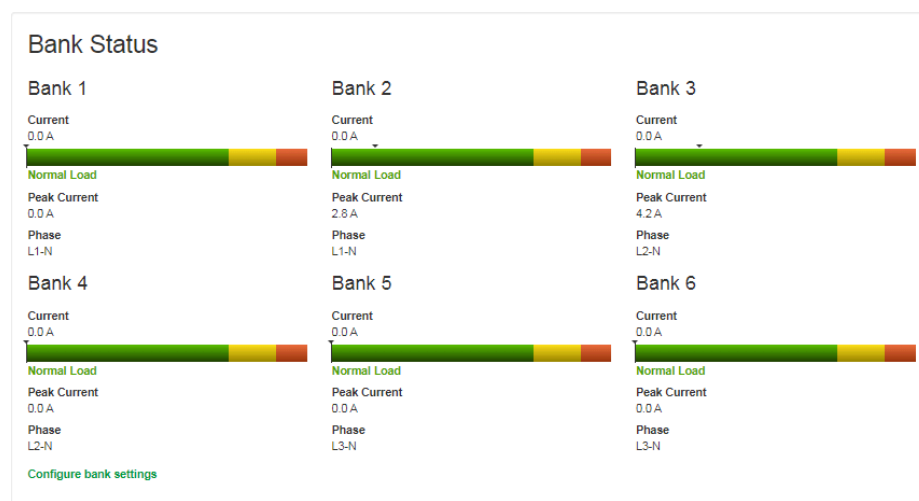
Shows status of device. Lists Status, Properties and Configuration information.

Path: Status > RPDU > Phase

Shows Phase Status. Delta values for Phase Load Balance are displayed for models with two or more metered phases. The phase settings can also be configured via a **Configure Phase Settings** link at the bottom of the page. Configuration can be changed as well.

Path: Status > RPDU > Bank

Status



View the status of each outlet bank. Click **Configure bank settings** to go to the threshold configuration page.

Path: Status > RPDU > Outlet

Status

Outlet Status

#	Outlet Name	[P]	B	State	Current	Energy	Power	Graph Peak Loads
1	Outlet 1	[1]	1	On	0.0 A	428154686.2 kWh	0 W	<div><div></div></div> Normal Load
2	Outlet 2	[1]	1	On	0.0 A	428070668.2 kWh	0 W	<div><div></div></div> Normal Load
3	Outlet 3	[1]	1	On	0.0 A	428339839.5 kWh	0 W	<div><div></div></div> Normal Load
4	Outlet 4	[1]	1	On	0.0 A	1493827.5 kWh	0 W	<div><div></div></div> Normal Load

Click the outlet number or name to see more details for that outlet. From the individual outlet page, you can click **Control** to go to the outlet control page (see) or click **Configuration** to open the configuration page (see).

Path: Status > RPDU > Switched Outlet > Outlet Groups

View outlet groups from this page. If no outlet groups are configured, click **Configure outlet groups** to open the configuration page (see for more information). If outlet groups are disabled, you must first enable them from **Configuration > RPDU > Switched Outlet > Outlet Group Settings**.

Path: Status > RPDU > Environment

Status

Temperature & Humidity Status

Name Sensor 1	Temperature 24.4 °C	Peak Temperature 1685.4 °C (At 06/27/2023 01:15:40)	Humidity 60 %RH
Name Sensor 2	Temperature 24.2 °C	Peak Temperature 48.8 °C (At 06/26/2023 16:16:51)	Humidity 60 %RH
Name Sensor 3	Temperature 24.5 °C	Peak Temperature 1685.4 °C (At 06/27/2023 01:15:40)	Humidity 59 %RH

Alarm Status

No Alarms Present

Configure environment settings

Click **Configure environment settings** to open the configuration page (Configure Temperature and Humidity Sensors, page 121).

View Network Information

Path: Status > Network > Network

Status

Current IPv4 Settings

System IP 10.179.228.66	Subnet Mask 255.255.252.0	Default Gateway 10.179.228.1	MAC Address 28 29 86 79 ED 44
Mode DHCP	DHCP Server: 10.179.228.10	Lease Acquired 10/17/2023 15:11	Lease Expires 10/19/2023 01:11

Current IPv6 Settings

Type	IP Address	Prefix Length
Auto	FE80::2A29:86FF:FE79:ED44	64
Auto	2001:112:1:3:2A29:86FF:FE79:ED44	64

Domain Name System Status

Active Primary DNS Server 10.179.90.251	Active Secondary DNS Server 10.179.51.251	Active Host Name apc79ED44
Active Domain Name (IPv4/IPv6) apa.gsd.schneider-electric.com	Active Domain Name (IPv6) example.com	

Port Speed

Current Speed
100 Full-Duplex

Current IPv4 Settings

Setting	Description
System IP	The IP address of the unit.
Subnet Mask	The IP address of the sub-network.
Default Gateway	The IP address of the router used to connect to the network.
MAC Address	The MAC address of the unit.
Mode	How the IPv4 settings are assigned: Manual , DHCP , or BOOTP .
DHCP Server	The IP address of the DHCP server. This is only displayed if Mode is DHCP .
Lease Acquired	The date/time that the IP address was accepted from the DHCP server.
Lease Expires	The date/time that the IP address accepted from the DHCP server expires and will need to be renewed.

Current IPv6 Settings

Setting	Description
Type	How the IPv6 settings are assigned.
IP Address	The IP address of the unit.
Prefix Length	The range of addresses for the sub-network.

Domain Name System Status

Setting	Description
Active Primary DNS Server	The IP address of the primary DNS server.
Active Secondary DNS Server	The IP address of the secondary DNS server.
Active Host Name	The host name of the active DNS server.
Active Domain Name (IPv4/IPv6)	The IPv4/IPv6 domain name that is currently in use.
Active Domain Name (IPv6)	The IPv6 domain name that is currently in use.

Ethernet Port Speed

Setting	Description
Current Speed	The current speed assigned to the Ethernet port.

Control

The **Control** menu enables you to take immediate actions affecting active user management and the security of your network.

Manage User Sessions

Path: Control > Security > Session Management

Current Sessions

Session Management			
User	Interface	Address	Logged In Time
apc	Web	10.171.241.174	00:36:41

The **Session Management** menu displays all active users currently connected to the Rack PDU.

You can click a **User** to display basic information about the user, including what interface they are logged-in to, their IP address, and user authentication. There is also an option to **Terminate Session** for the user.

Reset the Network Interface

Path: Control > Network > Reset/Reboot

This menu gives you the option to reset and reboot various components of the network management interface.

Reset/Reboot

Setting	Description
Reboot Management Interface	This setting only restarts the Rack PDU's Network Management Interface. It does not affect the ON/OFF status of the outlets.
Reset All	Reset all configuration values except for account information and the event log. You can select Exclude TCP/IP to reset all configuration values except the ones that determine how the PDU obtains its TCP/IP configuration. The default TCP/IP setting is DHCP .
Reset Only	Select a specific set of parameters to reset. The following parameters are only available for NPS groups: <ul style="list-style-type: none"> TCP/IP: Set the TCP/IP configuration to DHCP, its default setting. This requires that the Rack PDU receive its TCP/IP settings from a DHCP server. Event Configuration: Resets only the events to their default configuration. Any configuration changes, by event or by group, revert to their default settings. RPDU to Defaults: Resets only the Rack PDU settings to their default configurations.

Configuration

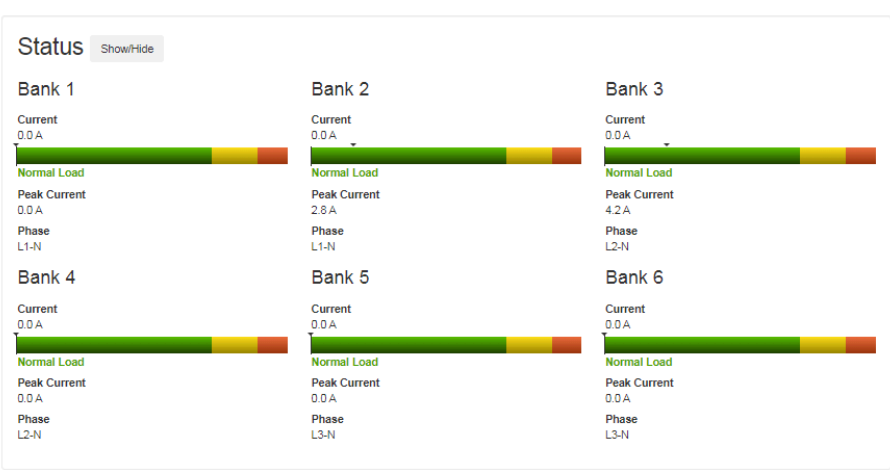
The Configuration menu allows you to

- Configure a name, location, and contact for the Rack PDU.
- Manage outlet groups.
- Configure email notifications.
- Configure Syslog server notifications.
- Configure thresholds for all connected devices, phases, banks, and outlets.
- Configure network settings.
- Configure SNMP settings.
- Configure date and time settings.
- Update the firmware, certificate, and key.
- Manage Users.

Configure Load Thresholds

You can use the configuration menu to view loads and configure thresholds for the entire rack PDU, as well as individual phases, banks, and outlets on the rack PDU. Several configuration pages display meters where green, yellow, and red areas show the configured ranges for normal, near overload, or overload statuses, respectively. If a low load threshold is configured, the meter will also include a blue section for low load conditions.

Bank Configuration



You can configure load thresholds from any of the following pages:

- Configuration > RPDU > Device
- Configuration > RPDU > Phase

By default, thresholds configured on this page do not result in alarms. Select **Enable** under **Alarm Generation** to enable alarms for phase load threshold violations.

- Configuration > RPDU > Bank

NOTE: The rack PDU generates an alarm when any bank exceeds its configured threshold. However, if a circuit breaker opens, the only indication is that the current for that bank drops. Set the bank **Low Load Warning** to 1 amp so that a warning alarm will be generated if the load drops. This creates some indication that a circuit breaker may have opened. (By default, the **Low Load Warning** is set to 0 amps, and no warning alarm is generated for low loads.)

The figure shows a configuration page for 'Bank 1' and 'Bank 2'. For each bank, there are three input fields: 'Low Load Warning [0 to 16]' (set to 0), 'Near Overload Warning [0 to 16]' (set to 13), and 'Overload Alarm [0 to 16]' (set to 16). Each field has a unit 'A' (Amps) next to it.

Set the load thresholds as needed. Click **Apply** to save your changes or click **Cancel** to discard them.

Violations of **Low Load** and **Near Overload** thresholds result in **Warning** alarms. Violations of **Overload** thresholds result in **Critical** alarms. Alarms are indicated by alarm icons throughout the web UI and recorded in the event log.

Configure Name and Location for the Rack PDU

Path: Configuration > RPDU > Device

Configuration

Name
apc79ED44

Location
Unknown

Contact
Unknown

Overload Alarm [0.0 to 32.0]
0.8 kW

Near Overload Warning [0.0 to 32.0]
0.7 kW

Low Load Warning [0.0 to 32.0]
0.0 kW

Coldstart Delay
☒ Immediate
☐ Wait
sec [1 to 300]

☐ Never

Peak Power
☐ Reset (Last reset 04/24/2023 10:58:27)

Energy
☐ Reset (Last reset 07/31/2023 14:41:59)

Apply Cancel

1. Enter a **Name**, **Location**, and **Contact** for the Rack PDU.
2. Click **Apply** to save your changes.

The **Name**, **Location** and **Contact** you enter in the **Configuration** area will appear on the **Home** tab.

Set the Coldstart Delay for the Rack PDU

Path: Configuration > RPDU > Device

The **Coldstart Delay** is the number of seconds added to each outlet's **Power On Delay** before an outlet will turn on after power is applied to the Rack PDU. You can enter values from 1–300 seconds, Immediate, or Never (never turn on). Click Apply to save your changes.

Reset Peak Load and kWh

Path: Configuration > RPDU > Device

Select the **Peak Load** and/or **Kilowatt-Hours**, then click **Apply** to save your changes.

Configure Phase Load Balance

Path: Configuration > RPDU > Phase

The Phase Load Balance alarm is only available for units with two or more metered phases.

Specify a warning threshold (in Amps) between 0 and the maximum phase current rating, then select **Enable** under **Alarm Generation**. Once this feature is enabled, the PDU will generate a Warning alarm if the phases are out of balance by more than the specified number of Amps.

Configure Temperature and Humidity Sensors

Path: Configuration > RPDU > Environment

To use this feature, you must install at least one optional temperature/humidity sensor (EPDU-TH3) to the Rack PDU.

Temperature & Humidity Configuration

Sensor #1

Name

Sensor 1

Temperature Alarm Settings

Maximum (Critical) [0 to 60]

60°C

High (Warning) [0 to 60]

59°C

Hysteresis [0 to 10]

1°C

Alarm Generation

☒ Enable

Humidity Alarm Settings

Low (Warning) [10 to 90]

15%RH

Minimum (Critical) [10 to 90]

10%RH

Hysteresis [0 to 20]

1%RH

Alarm Generation

☒ Enable

Peak Temperature

☐ Reset (Last reset 04/24/2023 10:59:26)

Sensor #2

Name

Sensor 2

Temperature Alarm Settings

Maximum (Critical) [0 to 60]

60°C

High (Warning) [0 to 60]

59°C

Hysteresis [0 to 10]

1°C

Alarm Generation

☒ Enable

Humidity Alarm Settings

Low (Warning) [10 to 90]

15%RH

Minimum (Critical) [10 to 90]

10%RH

Hysteresis [0 to 20]

1%RH

Alarm Generation

☒ Enable

Peak Temperature

☐ Reset (Last reset 04/24/2023 10:59:26)

TME63709

121

A **Sensor #** area appears for each attached sensor. Each area allows you to configure alarm settings for the sensors.

Setting	Description
Name	The name assigned to the sensor.
Temperature Alarm Settings	
Maximum (Critical)	The system generates a Critical alarm if the temperature reaches this threshold.
High (Warning)	The system generates a Warning alarm if the temperature reaches this threshold.
Hysteresis	This value specifies how far past a threshold the temperature must return to clear a threshold violation. For Maximum and High threshold violations, the clearing point is the threshold minus the hysteresis.
Alarm Generation	Select the Enable check box to enable temperature alarms for this sensor. Clear the Enable check box to disable temperature alarms for this sensor.
Humidity Alarm Settings	
Low (Warning)	The system generates a Critical alarm if the humidity reaches this threshold.
Minimum (Critical)	The system generates a Warning alarm if the humidity reaches this threshold.
Hysteresis	This value specifies how far past a threshold the humidity must return to clear a threshold violation. For Minimum and Low threshold violations, the clearing point is the threshold plus the hysteresis.
Alarm Generation	Select the Enable check box to enable humidity alarms for this sensor. Clear the Enable check box to disable humidity alarms for this sensor.
Peak Temperature	Select Reset to reset the peak temperature measurement. The date of the last peak temperature reset is shown in parenthesis.

Click **Apply** to save your changes, or click **Cancel** to discard them.

Using Hysteresis to lower alarm frequency: Temperature and humidity may repeatedly waver above and below the violation thresholds by a few degrees. If hysteresis values are too small, this will cause repeated alarms. If you experience repeated temperature or humidity alarms within a short timeframe, increase the hysteresis value to lower the alarm frequency.

Example of rising but wavering temperature: The maximum temperature threshold is 85°F, and the temperature hysteresis is 3°F. The temperature rises above 85°F, violating the threshold. It then wavers down to 84°F and then up to 86°F repeatedly, but no clearing event and no new violation occur. For the existing violation to clear, the temperature would have to drop to 82°F (3°F below the threshold).

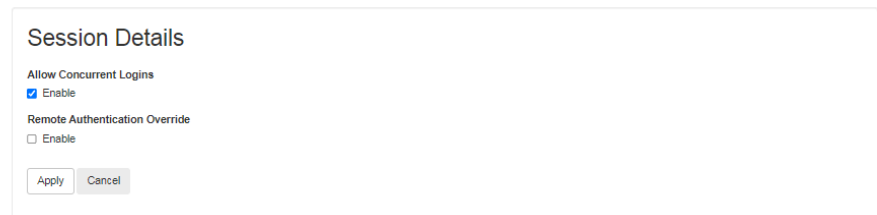
Example of falling but wavering humidity: The minimum humidity threshold is 18%, and the humidity hysteresis is 8%. The humidity falls below 18%, violating the threshold. It then wavers up to 24% and down to 13% repeatedly, but no clearing event and no new violation occur. For the existing violation to clear, the humidity would have to rise to above 26% (8% past the threshold).

Manage Security Settings

Manage Settings for User Sessions

Path: Configuration > Security > Session Management

Session Configuration



Session Details

Allow Concurrent Logins
☒ Enable

Remote Authentication Override
☐ Enable

Apply Cancel

Allow Concurrent Logins: Select **Enable** to allow two or more users to log on at the same time. Each user has equal access and each interface (HTTP, FTP, telnet, serial connection, etc.) counts as a logged-in user.

Remote Authentication Override: The Rack PDU supports RADIUS storage of passwords on a server. However, if you enable this override, the Rack PDU will allow a local user to log on using the password stored locally on the Rack PDU.

Enable Ping Response

Path: Configuration > Security > Session Management

IPv4 Ping Response: Select the **Enable** check box to allow the Rack PDU to respond to network pings. Clear the check box to disable a Rack PDU response.

This does not apply to IPv6.

Manage Local User Settings

Path: Configuration > Security > Local Users > Management

Click **Add User** to add a new user, or select a **User Name** to edit that user's configuration.

User Management Configuration

User Configuration

Access

☒ Enable

User Name

device

New Password

Confirm Password

User Type

Device

User Description

User Description

Session Timeout [1 to 60 minutes]

60

Serial Remote Authentication Override

☐ Enable

User Preferences

Event Log Color Coding

☒ Enable

Export Log Format

☒ Tab
☐ CSV

Temperature Scale

☐ US Customary
☒ Metric

Date Format

mm/dd/yyyy

Next >>

Cancel

Delete User

- **Access:** Select the **Enable** check box to allow access to the Rack PDU.
- **User Name:** Enter a new user name.
- **Current Password, New Password, Confirm Password:** Enter a new password in both the New Password and Confirm Password fields. You must enter a password for new users. Blank passwords, (passwords with no characters) are not allowed.

NOTE: The maximum length for both the name and password is 64 bytes, with less than 64 characters for multi-byte characters. Values greater than 64 bytes for **Name** and **Password** may be truncated. To change an Administrator/Super User setting, you must enter all three fields.

- **User Type:** Select the user type from the drop-down list.

Option	Description
Administrator	Read-write access to all menus.
Device	Read-write access to device-related menus. Can be enabled or disabled by Administrators.
Network-Only	Read-write access to network-related menus. Can be enabled or disabled by Administrators.

- **User Description:** Enter any additional identification details here.
- **Session Timeout:** Enter the number of minutes (3 by default) the Rack PDU waits before logging off an inactive user. If you change this value, you must log off for the change to take effect.

NOTE: If a user closes the Web UI without logging off, they are still considered logged on for the time specified in the **Session Timeout** field. This can help prevent other users from taking the place of a user who leaves the Web UI.

- **Serial Remote Authentication Override:** Select Enable to bypass RADIUS by using the serial console (CLI) connection. In order for this setting to work, you must enable it both on this page and under **Configuration > Security > Session Management > Remote Authentication Override**.

- **User Preferences:**

Option	Description
Event Log Color Coding	Mark the check box to enable color-coding of alarm text recorded in the Event Log. System event entries and configuration change entries do not change color. Red: Alarm Severity = Critical. A critical alarm exists, which requires immediate action. Orange: Alarm Severity = Warning. An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed. Green: Alarm Cleared. The conditions that caused the alarm have improved. Black: No alarms are present. The Rack PDU and all connected devices are operating normally.
Export Log Format	Configure which format the Event Log should be displayed in when exported (downloaded). Tab (default) allows fields to be tab-delimited whereas CSV is comma-separated.
Temperature scale	Select the default temperature scale, US Customary (Fahrenheit) or Metric (Celsius).
Date Format	Select the numerical format in which to display all dates in this user interface. In the selections, each letter (m for month, d for day, and y for year) represents one digit. Single digit days and months are displayed with a leading zero.

Click **Next**, and then click **Apply** to save or **Cancel** to return to the User Management Configuration page.

Configure Default User Settings

Path: Configuration > Security > Local Users > Default Settings

Determine the default values to populate in each of the fields when the Super User or Administrator-level account creates a new user. These values can be changed before the settings are applied to the system.

For remote users (user accounts not stored in the system that are remotely authenticated such as RADIUS) these are the values used for those that are not provided by the authenticating server. For example, if a RADIUS server does not provide the user with a temperature preference, the value defined in this section will be used.

- **Access:** Select the **Enable** check box to allow access to the Rack PDU.
- **User Type:** Select the user type from the drop-down list.

Option	Description
Administrator	Read-write access to all menus.
Device	Read-write access to device-related menus. Can be enabled or disabled by Administrators.
Read-Only	Read-only access. Can be enabled or disabled by Administrators.
Network-Only	Read-write access to network-related menus. Can be enabled or disabled by Administrators.

- **User Description:** Enter any additional identification details here.
- **Session Timeout:** Enter the number of minutes (3 by default) the Rack PDU waits before logging off an inactive user. If you change this value, you must log off for the change to take effect.
NOTE: If a user closes the Web UI without logging off, they are still considered logged on for the time specified in the **Session Timeout** field. This can help prevent other users from taking the place of a user who leaves the Web UI.
- **Bad Login Attempts:** Set the number of failed login attempts the user can have. Select from 0 to 99 attempts. 0 = unlimited.

- **User Preferences:**

Option	Description
Event Log Color Coding	Mark the check box to enable color-coding of alarm text recorded in the Event Log. System event entries and configuration change entries do not change color. Red: Alarm Severity = Critical. A critical alarm exists, which requires immediate action. Orange: Alarm Severity = Warning. An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed. Green: Alarm Cleared. The conditions that caused the alarm have improved. Black: No alarms are present. The Rack PDU and all connected devices are operating normally.
Export Log Format	Configure which format the Event Log should be displayed in when exported (downloaded). Tab (default) allows fields to be tab-delimited whereas CSV is comma-separated.
Temperature scale	Select the default temperature scale, US Customary (Fahrenheit) or Metric (Celsius).
Date Format	Select the numerical format in which to display all dates in this user interface. In the selections, each letter (m for month, d for day, and y for year) represents one digit. Single digit days and months are displayed with a leading zero.

- **Password Requirements:**

Option	Description
Strong Passwords	Configure whether new passwords created for user accounts will require at least one lowercase character, one uppercase character, one number, and one symbol.
Password Policy	Enter the number of days after which users will be required to change their passwords. A value of 0 days (the default) disables this feature.

Manage Remote User Settings

Path: Configuration > Security > Remote Users > Authentication

APC supports the authentication and authorization functions of RADIUS (Remote Access Dial-In User Service).

- When a user accesses a Rack PDU that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user's permission level.
- RADIUS user names used with the Rack PDU are case-sensitive, and have a 64 byte maximum, supporting up to 64 ASCII characters; less for multi-byte languages. Passwords with no characters (blank passwords) are not allowed.

Specify how you want remote users to be authenticated at logon. Select one of the following:

- **Local Authentication Only:** RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Authentication:** RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used.
- **RADIUS Only:** RADIUS is enabled. Local authentication is disabled.

NOTE: If **RADIUS Only** is selected, and the RADIUS server is unavailable or improperly configured, remote access is unavailable to all users. You must use a serial connection to the CLI and change the **access** setting to **local** or **radiusLocal** to regain access. For example, the command to change the access setting to **local** would be `radius -a local`.

For information about local authentication (not using the centralized authentication of a RADIUS server), see the *Network Management Card 3 Security Handbook* (SPD_CCON-BDYD7K_EN) on www.se.com/ww/en/download. You must select a location to view and download user manuals from the website.

Configure a RADIUS Server

Path: Configuration > Security > Remote Users > RADIUS

Use this option to do the following:

- List the RADIUS servers (a maximum of two) available to the Rack PDU and the Reply Timeout period for each.
- Select a server, and configure the parameters for authentication by a new RADIUS server.
- Select a listed RADIUS server to display and modify its parameters:

RADIUS Server Configuration

RADIUS Server

RADIUS Server
0.0.0.0

Port
1812

Secret

Reply Timeout seconds [1 to 30]
5

☒ Test Settings

User Name

Password

☐ Skip Test and Apply

Apply Cancel

Setting	Definition
RADIUS Server	The server name or IP address (IPv4 or IPv6) of the RADIUS server. Select a link to configure the server.
Port	The port the RADIUS server uses to authenticate users (1812 by default). The Rack PDU supports ports 1812, and 5000 to 32768.
Secret	The shared secret between the RADIUS server and the Rack PDU.
Reply Timeout	The time in seconds that the Rack PDU waits for a response from the RADIUS server.
Test Settings	Enter the Super User or Administrator user name and password to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path. (Not recommended)

Summary of the configuration procedure: You must configure your RADIUS server to work with the Rack PDU. For examples of the RADIUS users file with Vendor Specific Attributes (VSAs) and an example of an entry in the dictionary file on the RADIUS server, see the *Network Management Card 3 Security Handbook* (SPD_CCON-BDYD7K_EN) on www.se.com/ww/en/download. You must select a location to view and download user manuals from the website.

1. Add the IP address of the Rack PDU to the RADIUS server client list (file).
2. Users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined. If no Service-Type attributes are configured, users will have read-only access (on the Web UI only).
3. VSAs can be used instead of the Service-Type attributes provided by the RADIUS server. VSAs require a dictionary entry and a RADIUS users file. In the dictionary file, define names for ATTRIBUTE and VALUE keywords, but not for numeric values. If you change numeric values, RADIUS authentication and authorization will fail. VSAs take precedence over standard RADIUS attributes.

Configuring a RADIUS server on UNIX® with shadow passwords: If UNIX shadow password files are used (/etc/passwd) with the RADIUS dictionary files, the following two methods can be used to authenticate users:

- If all UNIX users have administrative privileges, add the following to the RADIUS “user” file. To allow only Device Users, change the APC-Service-Type to Device.

```
DEFAULTAuth-Type = System
APC-Service-Type = Admin
```

- Add user names and attributes to the RADIUS “user” file, and verify the password against /etc/ passwd. The following example is for users bconners and thawk:

```
bconnersAuth-Type = System
APC-Service-Type = Admin
thawkAuth-Type = System
APC-Service-Type = Device
```

Supported RADIUS servers: FreeRADIUS v1.x and v2.x, and Microsoft Server 2008 and 2012 Network Policy Server (NPS) are supported. Other commonly available RADIUS applications may work but may not have been fully tested.

Radius and Network Port Sharing: For RADIUS users file with VSAs, outlets on guest Rack PDUs can be associated to RADIUS users by using the method in the following example:

```
# give user access to outlets 1, 2, and 3 on unit 1,
# outlet 7 on 2, outlets 1 through 6
# on unit 3, and outlets 1,2,4 through 6,7 through 10,
# and 20 on unit 4
newOutletUser Auth-Type = Local, User-Password =
"newoutlets"
    APC-Service-Type = Outlet,
    APC-Outlets = "1[1,2,3];2[7];3[1-6];4[1,2,4-6,7-
10,20];"
```

NOTE: See the *Security Handbook* for more information on using RADIUS.

RADIUS and Network Port Sharing: For RADIUS users file with VSAs, outlets on guest Rack PDUs can be associated to RADIUS users by using the method in the following example:

```
# give user access to outlets 1, 2, and 3 on unit 1,
# outlet 7 on unit 2, outlets 1 through 6
# on unit 3, and outlets 1,2,4 through 6, 7 through 10,
# and 20 on unit 4
newOutletUser Auth-Type = Local, User-Password =
"newoutlets"
    APC-Service-Type = Outlet,
    APC-Outlets = "1[1,2,3];2[7];3[1-6];4[1,2,4-
6,7-10,20];"
```

NOTE: See the *Network Management Card 3 Security Handbook*(SPD_CCON-BDYD7K_EN) on www.se.com/ww/en/download, for more information on using RADIUS. You must select a location to view and download user manuals from the website.

Firewall Menus

Path: Configuration > Security > Firewall > Configuration

Enable or disable the firewall functionality. The configured policy is listed by default. Select the **Enable** check box to enable the firewall. The check box is unchecked by default.

- Click **Apply** to confirm a firewall policy you have selected to enable. The **Firewall Confirmation** page will open.
 - The **Confirmation** page contains a recommendation to test the firewall before enabling. It is not mandatory.
 - The first hyperlink goes to the **Firewall Policy** page.
 - The second hyperlink goes to the **Firewall Test** page.
 - Click **Apply** to enable the firewall and return to the **Configuration** page.
 - Click **Cancel** to return to the **Configuration** page without enabling the firewall.
- Click **Cancel**: No new selection will be enabled. You stay on the **Configuration** page.

Active Policy

Path: Configuration > Security > Firewall > Active Policy

Select an active policy from the **Available Policies** drop-down list, and view the validity of that policy. The current active policy is displayed by default; you can select another from the list.

- Click **Apply** to enable your changes. If a different firewall was selected and enabled, the change is effective immediately. If a newly configured firewall policy has been selected, it is recommended that you test the new firewall before enabling it. (You can test the new firewall from **Configuration > Security > Firewall > Configuration**.)
- Click **Cancel** to restore the original active policy and stay on the **Active Policy** page.

Active Rules

Path: Configuration > Security > Firewall > Active Rules

When a firewall is enabled, this read-only page lists the individual rules that are being enforced by a current active policy.

Create/Edit Policy

Path: Configuration > Security > Firewall > Create/Edit Policy

Use this page to create a new policy, or delete or edit an existing policy.

You cannot delete an active, enabled firewall policy. You can edit a running policy, but it is not recommended as changes are applied immediately. Instead, disable the firewall, edit the policy, test it, and then re-enable the policy.

Create a New Policy

Click **Add Policy**, and type in the file name for the new firewall file. The filename should have a .fwl file extension. If left without a file extension, .fwl will be appended to the name automatically.

- Click **Apply**: If the filename is legal, the empty file firewall policy file will be created. It will be located in the **/fwl** folder with the other policies on the system.
- Click **Cancel** to return to the previous page without creating a new firewall file.

Edit an Existing Policy

Select **Edit Policy** to go to the edit page. You can edit an firewall policy which is not active.

Warning page: If you attempt to edit the active enabled policy, a warning page will open. **Editing the active firewall policy will cause all changes made to be applied immediately. It is recommended to disable the firewall and test the policy before enabling it.**

- Click **Apply** to leave the Warning page and return to the **Edit Policy** page.
 - Click **Cancel** to leave the Warning page and return to the **Create/Edit Policy** page.
1. Select the policy you want to edit from the **Policy Name** drop-down list, and click **Edit Policy**.
 2. Click **Add Rule** or select the **Priority** of an existing rule to go to the **Edit Rule** page. From this page, you can change the rule settings or delete the selected rule.

Setting	Description
Priority	If two rules conflict, the rule with the higher priority will determine what happens. The highest priority is 1; the lowest is 250.
Type	host: In the IP/any field, you will enter a single IP address. subnet: In the IP/any field, you will enter a subnet address. range: In the IP/any field, you will enter a range of IP addresses.
IP/any	Specify the IP address or range of addresses this rule applies to, or select one of the following: - any: The rule applies regardless of the IP address. - anyipv4: The rule applies for any IPv4 address. - anyipv6: The rule applies for any IPv6 address.
Port	Specify a port the rule will apply to: - None: The rule will apply to any port. - Common Configured ports: Select a standard port. - Other: Specify a non-standard port number.
Protocol	Specify which protocol the rule applies to: - any: any protocol. - tcp: used for more reliable information transfer between applications. - udp: alternative to TCP using for faster, lower bandwidth information transfer. Though it has fewer delays, UDP is less reliable than TCP. - icmp: used to report errors for troubleshooting. - icmpv6: used to report errors for troubleshooting on applications using IPv6.
Action	allow: Allow the packet that matches this rule. discard: Discard the packet that matches this rule.
Log	If this rule applied to a packet, regardless of whether the packet is blocked or allowed, this will add an entry to the Firewall Log (see Firewall Logs , page 171).

It is recommended that you add one of the following as the lowest priority rule in your firewall policy:

- To use the firewall as a white list, add
250 Dest any / Source any / protocol any / discard
- To use the firewall as a black list, add
250 Dest any / Source any / protocol any / allow

Delete a Policy

Select **Delete Policy** to open the Confirm Deletion page.

Click **Apply** to confirm and the selected firewall file is removed from the file system.

Load Policy

Path: Configuration > Security > Firewall > Load Policy

Upload a policy (with the .fwl suffix) from a source external to this device.

Test

Path: Configuration > Security > Firewall > Test

Temporarily enforce the rules of a chosen policy for a time that you specify.

802.1X Security Configuration

The NMC takes the role of a supplicant in an EAPoL (Extensible Authentication Protocol over LAN) architecture used in IEEE 802.1X port-based network access control. The NMC supports EAP-TLS as an authentication method which requires the user to upload 3 client-side certificates. The private key is stored in an encrypted format. The user needs to provide a valid passphrase to be able to enable 802.1X security access.

NOTE: The NMC supports only EAP-TLS authentication method.

Enable Access

Path: Configuration > Security > 802.1X Security > Access

EAPoL/802.1X Access

802.1X Security Access

EAPoL Access

☐ Enable

Supplicant Identifier

NMC-Supplicant-28:29:86:79:ED:44

Apply

Cancel

Setting	Description
EAPoL Access	Used to enable or disable 802.1X Security Access. NOTE: The 802.1X security access is disabled by default. You can enable it only when valid certificates and a valid passphrase for the private key are provided.
Supplicant Identifier	Allows the users to set their own supplicant identifier (up to 32 characters including whitespace). NOTE: By default, the supplicant identifier is set to "NMC-Supplicantxx: xx: xx:xx:xx:xx" where six octets of 'xx' are the MAC ID of the NMC.

Upload Certificates

Path: Configuration > Security > 802.1X Security > Configuration

EAPoL Certificate Configuration

CA Certificate

Status

File not found

Certificate Action

☒ Add or Replace

☐ Remove

Choose File

No file chosen

Uploads a new CA certificate that becomes active when a valid private key certificate, a key phrase and a user/public certificate are uploaded.

(supports .pem, .der, .PEM, .DER file extensions, in PEM or DER format.)

Removes the current certificate.

Next >>

Cancel

Setting	Description
Add or Replace	Click Choose File to Upload or replace a CA root certificate. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extensions .pem, .PEM, .der, or .DER. Click Next >> to complete the following:
Remove	Remove the current certificate.

Setting	Description
Private Key Certificate	Upload/replace or remove an encrypted private key. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extensions .key or .KEY. NOTE: Unencrypted private key is not accepted.
Private Key Passphrase	Provide the passphrase to decrypt the encrypted private key. Allows up to 64 characters including whitespace.
User/Public Certificate	Upload/replace or remove a user/public certificate. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extensions .pem, .PEM, .der, or .DER.

View Uploaded SSL Certificates

Path: Configuration > Security > SSL Certificates

You can use this page to upload CA root certificates and local device certificates.

Certificate Upload

Installed Local Device Certificates

Common Name (CN)	File Name	Status
There are no SSL certificates loaded.		

Installed CA Certificates

Common Name (CN)	File Name	Status
There are no SSL certificates loaded.		

Certificate Action

☒ Upload CA Certificate

Certificate File
 No file chosen

This uploads a new certificate authority (CA) certificate file.
 The certificate file must be either PEM or DER encoded X.509, and must have a file extension of .crt, .cer, .pem, or .der.

☐ Upload Local Device Certificate

Certificate File
 No file chosen

Private Key File
 No file chosen

Private Key Passphrase

This uploads a new local device certificate, along with its corresponding private key file.
 The certificate file must be either PEM or DER encoded X.509, and must have a file extension of .crt, .cer, .pem, or .der.
 The private key file must be either PEM or DER encoded PKCS#8, either encrypted or unencrypted, and must have a file extension of .p8, .key, .pem, or .der. If encrypted, the passphrase must also be provided.

View and all uploaded certificates. If needed, you can also upload new CA certificates on this page.

Setting	Description
Upload CA Certificate	Click Choose File to upload a CA root certificate. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extensions .pem, .PEM, .der, or .DER.
Upload Local Device Certificate	<p>The Certificate file and Private Key File are required. The Private Key Passphrase is required if the private key file is encrypted.</p> <p>Certificate file: Click Choose File to upload the local device certificate. The certificate file must be either PEM or DER encoded X.509, and must have a file extension of .crt, .cer, .pem, or .der.</p> <p>Private Key File Click Choose File to upload the private file key. The private file key must be either PEM or DER encoded PKCS#8, either encrypted or unencrypted. The file must have a file extension of .p8, .key, .pem, or .der.</p> <p>Private Key Passphrase: Provide the passphrase to decrypt the encrypted private key. Allows up to 64 characters including white space.</p> <p>NOTE: Unencrypted private key is not accepted.</p>

Configure Network Settings

The **Configuration Summary** page (**Configuration > Network > Summary**) provides a quick overview of what network settings are enabled or disabled, as well as quick links to the configuration pages for each.

Configuration Summary

IPv4	Enabled	Configure	
IPv6	Enabled	Configure	
Ping Response	Enabled	Configure	

HTTP	Enabled	Configure	
HTTPS	Enabled	Access	SSL Certificate
FTP	Disabled	Configure	
Telnet	Enabled	Configure	
SSH/SCP	Enabled	Access	SSH Host Key
SNMPv1	Read/Write	Access	Access Control
SNMPv3	Enabled	Access	Access Control User Profiles

Super User	Enabled	Configure	
RADIUS	Disabled	Authentication	RADIUS
Administrator	Disabled	Configure	
Device User	1 Enabled	Configure	
Read-Only User	Disabled	Configure	
Network-Only User	Disabled	Configure	

You can also configure network settings from the **Configuration > Network** menu options.

Configure IPv4 Network Settings

Path: Configuration > Network > TCP/IP > IPv4 Settings

The **Current IPv4 Settings** area displays the current IPv4 address, subnet mask, default gateway, MAC address, and boot mode of the Rack PDU. For information on DHCP and DHCP options, see RFC2131 and RFC2132.

IPv4 Settings

Current IPv4 Settings

System IP 10.179.228.66	Subnet Mask 255.255.252.0	Default Gateway 10.179.228.1	MAC Address 28 29 86 79 ED 44
Mode DHCP	DHCP Server: 10.179.228.10	Lease Acquired 10/17/2023 15:11	Lease Expires 10/19/2023 01:11

The **IPv4 Configuration** area displays configurable IPv4 settings.

IPv4 Configuration

IPv4

☒ Enable

Mode

☐ Manual

System IP

0.0.0.0

Subnet Mask

0.0.0.0

Default Gateway

0.0.0.0

☐ BOOTP

☒ DHCP

Vendor Cookie

☐ Require vendor specific cookie to accept DHCP Address

Vendor Class

APC

Client ID

28 29 86 79 ED 44

User Class

EPDU

Apply

Cancel

Note: Some configuration settings will require a reboot to activate.

Setting	Description
Enable	Enable or disable IPv4.
Manual	Enter the IPv4 System IP (the IP address), Subnet Mask , and Default Gateway to manually configure a static IP address.

Setting	Description
BOOTP	<p>A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Rack PDU requests network assignment from any BOOTP server:</p> <ul style="list-style-type: none"> • If the Rack PDU receives a valid response, it starts the network services. • If the Rack PDU finds a BOOTP server, but a request to that server fails or times out, the Rack PDU stops requesting network settings until it is restarted. • By default, if previously configured network settings exist, and the Rack PDU receives no valid response after five requests (the original and four retries), it uses the previously configured settings so that it remains accessible. <p>Click Next>> to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail:</p> <ul style="list-style-type: none"> • Maximum retries: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. • If retries fail: Select Use prior settings (the default) or Stop BOOTP request.
DHCP	<p>The default setting. The Rack PDU requests network assignment from any DHCP server.</p> <ul style="list-style-type: none"> • If the Rack PDU receives a valid response, it does not (as previously) require the APC cookie from the DHCP server in order to accept the lease and start the network services. • If the Rack PDU finds a DHCP server, but the request to that server fails or times out, the Rack PDU stops requesting network settings until you restart it. <p>Require vendor specific cookie to accept DHCP Address: By selecting this check box, you can require the DHCP server to provide a cookie which supplies information to the Rack PDU.</p> <p>The default values for these settings generally do not need to be changed:</p> <ul style="list-style-type: none"> • Vendor Class: APC • Client ID: The MAC address of the Rack PDU, which uniquely identifies it on the local area network (LAN) • User Class: The name of the application firmware module

DHCP response options: Each valid DHCP response contains options that provide the TCP/IP settings that the Rack PDU needs to operate on a network, and other information that affects the operation of the Rack PDU.

Vendor Specific Information (option 43): The Rack PDU uses this option in a DHCP response to determine whether the DHCP response is valid. This option contains an APC-specific option in a TAG/LEN/DATA format, called the APC Cookie. This is disabled by default. For example,
APC Cookie. Tag 1, Len 4, Data "1APC"

Option 43 communicates to the Rack PDU that a DHCP server is configured to service devices. Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie: Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43

TCP/IP options: The Rack PDU uses the following options within a valid DHCP response to define its TCP/IP settings. All of these options except the first are described in RFC2132.

- **IP Address** (from the yiaddr field of the DHCP response, described in RFC2131): The IP address that the DHCP server is leasing to the Rack PDU.
- **Subnet Mask** (option 1): The Subnet Mask value that the Rack PDU needs to operate on the network.
- **Router**, i.e., Default Gateway (option 3): The default gateway address that the Rack PDU needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the Rack PDU.
- **Renewal Time, T1** (option 58): The time that the Rack PDU must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): The time that the Rack PDU must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other options: The Rack PDU also uses these options within a valid DHCP response. All of these options except the last are described in RFC2132.

- **Network Time Protocol Servers** (option 42): One NTP server that the Rack PDU can use.
- **Time Offset** (option 2): The offset of the Rack PDU's subnet, in seconds, from Coordinated Universal Time (UTC).
- **Domain Name Server** (option 6): One Domain Name System (DNS) server that the Rack PDU can use.
- **Host Name** (option 12): The host name that the Rack PDU will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the Rack PDU will use (64-character maximum length).
- **Boot File Name** (from the file field of the DHCP response, described in RFC2131): The fully qualified directory-path to a user configuration file (.ini file) to download. The siaddr field of the DHCP response specifies the IP address of the server from which the Rack PDU will download the .ini file. After the download, the .ini file is used as a boot file to reconfigure the settings.

Configure IPv6 Network Settings

Path: Configuration > Network > TCP/IP > IPv6 Settings

The **Current IPv6 Settings** area displays the current IPv6 addresses. The **IPv6 Configuration** area displays configurable IP settings.

IPv6 Settings

Current IPv6 Settings

Type	IP Address	Prefix Length
Auto	FE80::2A29:86FF:FE79:ED44	64
Auto	2001:112:1:3:2A29:86FF:FE79:ED44	64

IPv6 Configuration

IPv6

☒ Enable

Manual Configuration

☐ Enable

System IP

FE64

Default Gateway

::

Auto Configuration

☒ Enable

DHCPv6 Mode

☒ Router Controlled

☐ Address and Other Information

☐ Non-Address Information Only

☐ Never

Apply Cancel

Note: Some configuration settings will require a reboot to activate.

Setting	Description
Enable	Select this check box to enable IPv6. Clear the check box to disable IPv6.
Manual Configuration	Configure a static IPv6 address manually by entering the IP address (System IP) and the Default Gateway . You must select the Enable check box to enable this option.

Setting	Description
Auto Configuration	When the Enable check box is selected, the system obtains addressing prefixes from the router (if available). It uses those prefixes to automatically configure IPv6 addresses.
DHCPv6 Mode	<p>Router Controlled: Selecting this option means that DHCPv6 is controlled by the Managed (M) and Other (O) flags received in IPv6 router advertisements. When a router advertisement is received, the Rack PDU checks whether the M or the O flag is set. The Rack PDU interprets the state of the M (Managed Address Configuration Flag) and O (Other Stateful Configuration Flag) "bits" for the following cases:</p> <ul style="list-style-type: none"> • <i>Neither is set:</i> Indicates the local network has no DHCPv6 infrastructure. The Rack PDU uses router advertisements and manual configuration to get addresses that are not link-local and other settings. • <i>M, or M and O are set:</i> In this situation, full DHCPv6 address configuration occurs. DHCPv6 is used to obtain addresses AND other configuration settings. This is known as <code>DHCPv6 stateful</code>. Once the M flag has been received, the DHCPv6 address configuration stays in effect until the interface in question has been closed. This is true even if subsequent router advertisement packets are received in which the M flag is not set. <p>If an O flag is received first, then an M flag is received subsequently, the Rack PDU performs full address configuration upon receipt of the M flag.</p> <ul style="list-style-type: none"> • <i>Only O is set:</i> In this situation, the Rack PDU sends a DHCPv6 Info-Request packet. DHCPv6 will be used to configure "other" settings (such as location of DNS servers), but NOT to provide addresses. This is known as <code>DHCPv6 stateless</code>. <p>Address and Other Information: With this radio box selected, DHCPv6 is used to obtain addresses AND other configuration settings. This is known as <code>DHCPv6 stateful</code>.</p> <p>Non-Address Information Only: With this radio box selected, DHCPv6 will be used to configure "other" settings (such as location of DNS servers), but NOT to provide addresses. This is known as <code>DHCPv6 stateless</code>.</p> <p>Never: Select this to disable DHCPv6.</p>

Configure Port Speed

Path: Configuration > Network > Port Speed

Port Speed Configuration

Port Speed

Current Speed
100 Full-Duplex

Configure Port Speed

Port Speed

☒ Auto-negotiation

☐ 10 Half-Duplex

☐ 10 Full-Duplex

☐ 100 Half-Duplex

☐ 100 Full-Duplex

Note: Some configuration settings will require a reboot to activate.

This setting controls the speed of the TCP/IP port.

Setting	Description
Auto-negotiation	The default setting. Ethernet devices negotiate to transmit at the highest possible speed, but if the supported speeds of two devices are unmatched, the slower speed is used.
10 Half-Duplex	10/100 = speed in megabits per second (Mbps) Half-Duplex = communication in only one direction at a time Full-Duplex = communication in both directions on the same channel simultaneously
10 Full-Duplex	
100 Half-Duplex	
100 Full-Duplex	

Configure the Domain Name System

Path: Configuration > Network > DNS > Configuration

DNS Configuration

Domain Name System Status

Active Primary DNS Server 10.179.90.251	Active Secondary DNS Server 10.179.51.251	Active Host Name apc79ED44
Active Domain Name (IPv4/IPv6) apa.gad.schneider-electric.com	Active Domain Name (IPv6) example.com	

Manual Domain Name System Settings

Override Manual DNS Settings
☒ Enable

Primary DNS Server

Secondary DNS Server

System Name Synchronization
☐ Enable

Host Name

Domain Name (IPv4/IPv6)

Domain Name (IPv6)

Setting	Description
Override Manual DNS Settings:	When enabled, configuration data from other sources (typically DHCP) takes precedence over the manual configurations set here.
Primary DNS Server / Secondary DNS Server	<p>Select one of these to specify the IPv4 or IPv6 addresses of the primary and optional secondary DNS server. For the Rack PDU to send e-mail, you must at least define the IP address of the primary DNS server.</p> <ul style="list-style-type: none"> The Rack PDU waits up to 15 seconds for a response from the primary DNS server or secondary DNS server (if specified). If the Rack PDU does not receive a response within that time, e-mail cannot be sent. Use DNS servers on the same segment as the Rack PDU or on a nearby segment (but not across a wide-area network [WAN]). Define the IP addresses of the DNS servers, then enter the DNS name of a computer on your network to look up the IP address for that computer to verify correct operation.
System Name Synchronization	<p>Allow the system name to be synchronized with the host name so both fields automatically contain the same value.</p> <p>NOTE: When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the Host Name field).</p>

Setting	Description
Host Name	Configure a host name here and a domain name in the Domain Name field. Users can then enter a host name in any field in the NMC interface (except e-mail addresses) that accepts a domain name.
Domain Name IPv4 / Domain Name IPv6	Configure the domain name here only. In all other fields in the NMC interface (except e-mail addresses) that accept domain names, the Rack PDU adds this domain name when only a host name is entered. <ul style="list-style-type: none"> To override all instances of the expansion of a specified host name by the addition of the domain name, set the domain name field to its default, <code>example.com</code>, or to <code>0.0.0.0</code>. To override the expansion of a specific host name entry, include a trailing period. The NMC recognizes a host name with a trailing period (such as <code>mySnmpServer.</code>) as if it were a fullyqualified domain name and does not append the domain name.

Test the Domain Name System

Path: Configuration > Network > DNS > Test

DNS Test

Send DNS Query

Last Query Response

No last query.

Query Type

by Host

Query Question

www.apc.com

Apply

Cancel

Use this option to send a DNS query that tests the setup of your DNS server by looking up the IP address. View the result of a test in the **Last Query Response** field, or identify the value to be used for the selected query type:

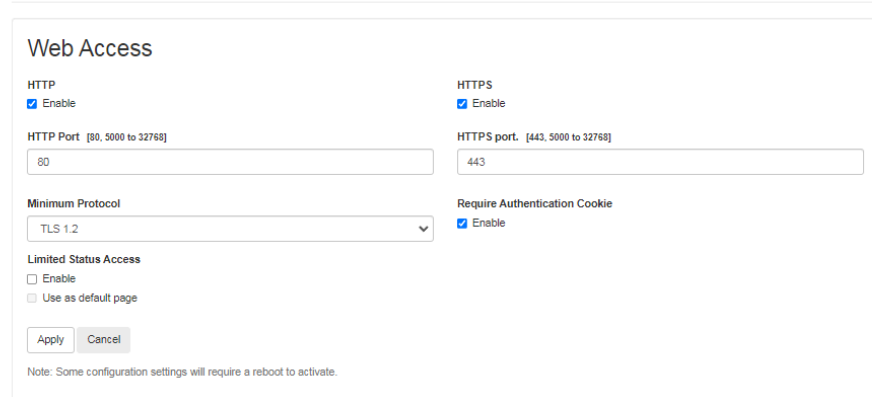
Query Type Selected	Query Question to Use
by Host	The URL name of the server
by FQDN	The fully qualified domain name of the server, <code>my_server.my_domain</code>
by IP	The IP address of the server
by MX	The mail exchange address of the server

Configure Access to the Web UI

Enable Access Protocols

Path: Configuration > Network > Web > Access

Web Settings



Web Access

HTTP
☒ Enable
 HTTP Port [80, 5000 to 32768]
 80
 Minimum Protocol
 TLS 1.2
☐ Limited Status Access
☐ Use as default page
 Apply Cancel

HTTPS
☒ Enable
 HTTPS port. [443, 5000 to 32768]
 443
☒ Require Authentication Cookie
 Note: Some configuration settings will require a reboot to activate.

To activate changes to any of these selections, log off from the Rack PDU.

Setting	Description
HTTP	Select Enable to enable Hypertext Transfer Protocol (HTTP), which provides web access by user name and password, but does not encrypt user names, passwords, and data during transmission. HTTP is disabled by default.
HTTPS	Select Enable to enable Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL). SSL encrypts user names, passwords, and data during transmission, and authenticates the Rack PDU by digital certificate. When HTTPS is enabled, your browser displays a small lock icon. HTTPS is enabled by default.
HTTP Port	The TCP/IP port (80 by default) used to communicate by HTTP with the Rack PDU.
HTTPS Port	The TCP/IP port (443 by default) used to communicate by HTTPS with the Rack PDU.
Minimum Protocol	Choose the minimum security protocol.

Upload SSL Certificates

Path: Configuration > Network > Web > SSL Certificate

Add, replace, or remove a security certificate.

If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the Rack PDU generates a default certificate. You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on.

Setting	Description
Add or Replace	Click Choose File to add or replace certificate file. New certificates become active immediately.
Remove	Delete the current certificate.

Configure Access to the CLI

Enable Access Protocols

Path: Configuration > Network > Console > Access

Console Settings

Console Access

Telnet
☒ Enable

SSH/SCP
☒ Enable

Telnet Port [23, 5000 to 32768]

SSH Port [22, 5000 to 32768]

Note: Some configuration settings will require a reboot to activate.

Setting	Description
Telnet	Telnet transmits user names, passwords, and data without encryption. Select Enable to allow access to the CLI via Telnet. Telnet is disabled by default.
SSH/SCP	SSH transmits user names, passwords, and data in encrypted form, providing protection from attempts to intercept, forge, or alter data during transmission. Select Enable to allow access to the CLI via SSH. SSH is enabled by default.
Telnet Port:	The Telnet port used to communicate with the NMC (23 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) or a space, as required by your Telnet client program, to specify the non-default port. For example, for port 5000 and an IP address of 152.214.12.114, your Telnet client requires one of the these commands: telnet 152.214.12.114:5000 telnet 152.214.12.114 5000
SSH Port	The SSH port used to communicate with the NMC (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port.

Upload SSH Host Key

Path: Configuration > Network > Console > SSH Host Key

Setting	Description
Status	<p>Indicates the status of the current host key (private key).</p> <p>SSH Disabled: No host key in use: When disabled, SSH cannot use a host key.</p> <p>Generating: The NMC is creating a host key because no valid host key was found.</p> <p>Loading: A host key is being activated on the NMC.</p> <p>Valid: One of the following valid host keys is in the <code>/ssh</code> directory (the required location on the NMC): A 1024-bit or 2048-bit host key created by the Security Wizard A 2048-bit RSA host key generated by the NMC</p>
Add or Replace	<p>Click Choose File to upload a host key file created by the Security Wizard.</p> <p>To use the Security Wizard, see the <i>Network Management Card 3 Security Handbook</i>(SPD_CCON-BDYD7K_EN) on www.se.com/ww/en/download. You must select a location to view and download user manuals from the website.</p> <p>NOTE: To reduce the time required to enable SSH, create and upload a host key in advance. If you enable SSH with no host key loaded, the NMC takes up to one minute to create a host key, and the SSH server is not accessible during that time.</p>
Remove	Remove the current host key.

Configure SNMP Settings

All usernames, passwords, and community names for SNMP are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMP access or set the access for each community to Read. (A community with Read access can receive status information and use SNMP traps.)

When using Data Center Expert™ to manage a Rack PDU on the public network, you must have SNMP enabled in the Rack PDU interface. Read access will allow Data Center Expert to receive traps from the Rack PDU, but Write access is required while you use the interface of the Rack PDU to set the Data Center Expert as a trap receiver.

Network Port Sharing

All Rack PDUs in a group can be accessed through the Host Rack PDU via SNMP **rPDU2** OIDs available in our PowerNet-MIB.

The full path to these OIDs is

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).apc(318).products(1).hardware(1).rPDU2(26)

Individual Rack PDUs can be identified in the SNMP MIB tables by viewing the corresponding "Module" OIDs in each table. These Module OIDs will return the Display ID of the Rack PDU.

Example Module OIDs:

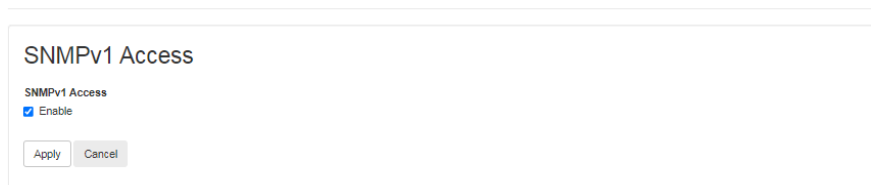
- rPDU2IdentModule
- rPDU2DeviceConfigModule
- rPDU2SensorTempHumidityConfigModule

In order to be backwards compatible with previous versions, the Host Rack PDU will always be the first index in any table that supports multiple Rack PDUs.

Enable SNMPv1/SNMPv2C Access

Path: Configuration > Network > SNMPv1 > Access

Configure SNMPv1 Access



Select **Enable** and click **Apply** to allow access via SNMPv1.

NOTE: This configuration also supports SNMPv2c.

Configure SNMPv1/SNMPv2C Access Control

Path: Configuration > Network > SNMPv1 > Access Control

You can configure up to four access control entries to specify which Network Management Systems (NMSs) have access to this device. The opening page for access control, by default, assigns one entry to each of the four available SNMPv1 communities, but you can edit these settings to apply more than one entry to any community to grant access by several specific IPv4 and IPv6 addresses, host names, or IP address masks. To edit the access control settings for a community, select its community name.

Configure SNMPv1 Community

Access Control

Community Name

NMS IP/Host Name

Access Type

Read

Apply

Cancel

Setting	Description
Community Name	The name that an NMS must use to access the community. The maximum length is 16 ASCII characters.
NMS IP/Host Name	The IPv4 or IPv6 address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows: <ul style="list-style-type: none"> - 149.225.12.255: Access only by an NMS on the 149.225.12 segment. - 149.225.255.255: Access only by an NMS on the 149.225 segment. - 149.255.255.255: Access only by an NMS on the 149 segment. - 0.0.0.0 (the default) or 255.255.255.255: Access by any NMS on any segment.
Access Type	The actions an NMS can perform through the community. <ul style="list-style-type: none"> - Read: GETs only, at any time - Write: GETs at any time, and SETs when no user is logged onto the Web UI or CLI. - Write+: GETs and SETs at any time. - Disable: No GETs or SETs at any time.

NOTE: If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network.

NOTE: If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device.

Enable SNMPv3 Access

Path: Configuration > Network > SNMPv3 > Access

Select **Enable** and click **Apply** to allow access via SNMPv1.

NOTE: This configuration also supports SNMPv2c.

Configure SNMPv3 User Profiles

Path: Configuration > Network > SNMPv3 > User Profiles

By default, this page lists the settings of four user profiles, configured with the user names **apc snmp profile1** through **apc snmp profile4**, and no authentication and no privacy (no encryption). To edit the following settings for a user profile, click a user name in the list.

Configure User Profile

Setting	Description
User Name	The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters.
Authentication Passphrase	A phrase of 15 to 32 ASCII characters that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time.
Privacy Passphrase	A phrase of 15 to 32 ASCII characters that ensures the privacy of the data (by means of encryption) that an NMS is sending to this device or receiving from this device through SNMPv3.
Authentication Protocol	The APC implementation of SNMPv3 supports SHA and MD5 authentication. Authentication will not occur unless an authentication protocol is selected.
Privacy Protocol:	<p>The implementation of SNMPv3 supports AES and DES as the protocols for encrypting and decrypting data. Privacy of transmitted data requires that a privacy protocol is selected and that a privacy passphrase is provided in the request from the NMS. When a privacy protocol is enabled but the NMS does not provide a privacy passphrase, the SNMP request is not encrypted.</p> <p>NOTE: You cannot select the privacy protocol if no authentication protocol is selected.</p>

Configure SNMPv3 Access Control

Path: Configuration > Network > SNMPv3 > Access Control

You can configure up to four access control entries to specify which Network Management Systems (NMSs) have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles, but you can edit these settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks.

NOTE: If you leave the default access control entry unchanged for a user profile, all Network Management Systems using that profile have access to this device.

NOTE: If you configure multiple access entries for one user profile, the limit of four entries requires that one or more of the other user profiles must have no access control entry. If no access control entry is listed for a user profile, no NMS that uses that profile has any access to this device.

To edit the access control settings for a user profile, select its user name.

Configure SNMPv3 Access Control

Setting	Description
Access	Select Enable to activate the access control specified by the parameters in this access control entry.
User Name	Select the user profile to which this access control entry will apply. The choices available are the four user names that you configure on the user profiles page (under Configuration > Network > SNMPv3 > User Profiles).
NMS IP/Host Name	The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows: <ul style="list-style-type: none"> - 149.225.12.255: Access only by an NMS on the 149.225.12 segment. - 149.225.255.255: Access only by an NMS on the 149.225 segment. - 149.255.255.255: Access only by an NMS on the 149 segment. - 0.0.0.0 (the default) or 255.255.255.255: Access by any NMS on any segment.

Configure Modbus TCP

Enable Modbus to allow a Building Management System to monitor the Rack PDU through Modbus TCP.

Path: Configuration > Network > Modbus > TCP

Configuration

Modbus TCP

Access

☒ Enable

Port [502, 5000 to 32768]

502

Communication Timeout

☐ Never

☒ Time
(secs) [1 to 64800, 0 - never]

5

Keep-Alive

☒ Enable

Apply

Cancel

[Knowledge Base](#) | [Schneider Electric Product Center](#) | [Product Information](#)

© 2024, Schneider Electric. All rights reserved.
[Site Map](#) | Updated: 04/12/2024 at 18:19 (2001:112:1:3:2C0:87FF:FEDD:37E4)

Access: Select **Enable** to enable Modbus TCP.

Port: Specify the port for the TCP connection (502 by default, or 5000 to 32768).

Communication Timeout: Enter the number of seconds the Rack PDU waits before disconnecting from the Modbus Poll software.

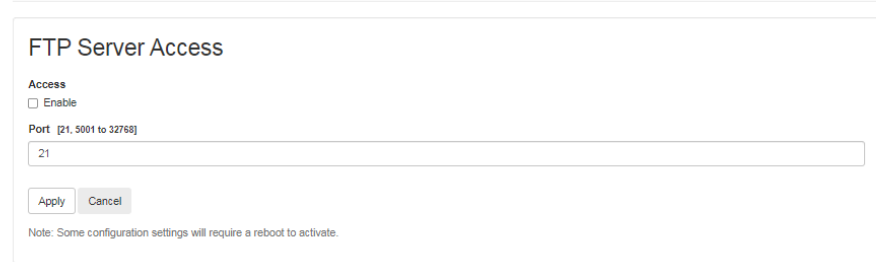
Keep-Alive: When you select **Enable**, the Rack PDU sends a packet to the server every two hours and 75 seconds if there is no other communication detected. This helps prevent a communication timeout when **Communication Timeout** is set to 7,275 seconds or more.

You must log off for the changes to take effect.

Configure an FTP Server

Path: Configuration > Network > FTP Server

Configure FTP Server Access



The FTP Server settings enable or disable access to the FTP server. FTP is disabled by default.

By default, the FTP server communicates with the Rack PDU through TCP/IP port 21. The FTP server uses both the specified port and the port one number lower than the specified port.

You can change the **Port** setting to the number of any unused port from 5001 to 32768 for added security. Users must then use a colon (:) to specify the non-default port number.

For example, for port 5001 and IP address 152.214.12.114, the command would be `ftp 152.214.12.114:5001`.

NOTE: FTP transfers files without encryption. For higher security, transfer files with Secure CoPy (SCP). Secure SHell (SSH) is enabled by default, and enables SCP automatically. However, SCP will not allow a file transfer until the Super User default password (**apc**) is changed. At any time that you want a Rack PDU to be accessible for management by Data Center Expert, FTP server access must be enabled in the Rack PDU interface.

NOTE: You can use FTP or SCP to configure and update the Rack PDU with Data Center Expert or EcoStruxure IT as long as the same protocol is enabled on both the Rack PDU and Data Center Expert or EcoStruxure IT. See your Data Center Expert or EcoStruxure IT documentation for details.

For detailed information on enhancing and managing the security of your system, see the *Network Management Card 3 Security Handbook*(SPD_CCON-BDYD7K_EN) on www.se.com/ww/en/download. You must select a location to view and download user manuals from the website.

Configure Notifications

You can configure event actions to occur in response to an event or group of events. These actions notify users of the event in any of several ways:

- Active, automatic notification. The specified users or monitoring devices are contacted directly.
 - E-mail notification
 - SNMP traps
 - Syslog notification
- Indirect notification
 - Event log. If no direct notification is configured, users must check the log to determine which events have occurred.
 - Queries (SNMP GETs).

SNMP enables an NMS to perform informational queries. For SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without the risk of allowing remote configuration changes. You can configure the access type under

For more information on SNMP, see [Configure SNMP Settings](#), page 147.

Configure Event Actions

Configure Individual Events

Path: Configuration > Notification > Event Actions > By Event

Event Actions for Individual Events

To list all events in a main category by severity level, click the main category name. To list all events in a sub-category by severity level, click the sub-category name.

System

Mass Configuration
Security

RPDU

Communications
Device
Phase Load
Bank Load
Outlet Load
Outlet Control
Sensor

Device

Management

1. To find an event, click on a column heading (**System**, **RPDU**, or **Device**) to see the lists under each category. Alternatively, you can click on a sub-category under these headings (for example, **Outlet Load**).

Outlet Load

Critical	Event Log	E-mail	Trap
Rack PDU: Outlet overload.	*	*	
Warning	Event Log	E-mail	Trap
Rack PDU: Outlet low load.	*	*	
Rack PDU: Outlet near overload.	*	*	
Informational	Event Log	E-mail	Trap
Rack PDU: Outlet configuration change.	*	*	X

2. Click an event name (for example, **Rack PDU: Outlet overload**) to view or change the current configuration. Configuration details may include the following:
- whether or not to include the event in the **Event Log**. This feature is always enabled by default.
 - recipients to be notified by email
 - Network Management Systems (NMSs) to be notified by SNMP traps

If no Syslog server is configured, items related to Syslog configuration are not displayed.

Event Detail

Rack PDU: Outlet overload.[0x3426]

Category
RPDU | Outlet Load

Clearing Event
Rack PDU: Outlet overload cleared. [0x3426]

Log
☒ Event Log

E-mail

Recipient	Delay	Repeat	Interval	Duration
<input checked="" type="checkbox"/> example@se.com	Disabled	yes	2 minutes	until cleared
<input checked="" type="checkbox"/> example@se.com	Disabled	yes	2 minutes	until cleared

Trap [750]

Recipient	Delay	Repeat	Interval	Duration
There are no receivers configured.				

Apply

Cancel

Restore Defaults

NOTE: When viewing details of an event configuration, you can enable or disable event logging or Syslog, or disable notification for specific email recipients or trap receivers, but you cannot add or remove recipients or receivers.

Configure a Group of Events

Path: Configuration > Notification > Event Actions > By Group

Configure Event Actions for Groups of Events

1. Select how to group events for configuration:
 - You can select events by **Severity**, and then select one or more severity levels. You cannot change the severity of an event.
 - You can select events by **Category**, and then select events in one or more pre-defined categories.
2. Click **Next** to select an event action.
 To select any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
3. Click **Next** to do one of the following:
 - If you selected **Logging** on the previous screen and have not configured a Syslog server, select **Configure Event Log**.
 - If you selected **Logging** on the previous screen and have configured a Syslog server, select **Event Log** or **Syslog**.
 - If you selected **Email Recipients** on the previous screen, select the e-mail recipients to configure.
 - If you selected **Trap Receivers** on the previous screen, select the trap receiver to configure.
4. Click **Next** to configure notification parameters. These configuration fields define e-mail parameters to send notifications:
 - If you are configuring **Logging** settings, select **Enable Notification** or **Disable Notification**.
 - If you are configuring **Email Recipients** or **Trap Receivers**, select **Enable Notification** or **Disable Notification** and set the notification parameters.
5. Click **Next** to view pending actions and do one of the following:
 - Click **Apply** to accept the changes.
 - Click **Cancel** to revert to the previous settings.

Email Notification Parameters: These configuration fields define e-mail parameters for sending notifications of events. You can access notification parameters by selecting the receiver or recipient name.

Field	Description
Delay n time before sending	If the event persists for the specified time, the notification is sent. If the condition clears before the time expires, no notification is sent.
Repeat at an interval of n	The notification is sent repeatedly at the specified interval (the default is every two minutes until the condition clears).
Up to n times or Until condition clears	During an active event, the notification repeats for this number of times. The notification is sent repeatedly until the condition clears or is resolved.

NOTE: You can also set notification parameters for events that have an associated clearing event.

Configure Email Notifications

You can optionally use Simple Mail transfer Protocol (SMTP) to send email notifications when an event occurs. To set up email notifications, you must configure an email server and email recipients. You can optionally upload an SSL certificate to increase security.

Configure an Email Server

Path: Configuration > Notification > Email > Server

E-mail Server Settings

Active Primary DNS Server
10.179.90.251

Active Secondary DNS Server
10.179.51.251

Outgoing Mail Configuration

From Address
address@example.com

SMTP Server
10.179.230.222

Port [25, 465, 587, 2525, 5000 to 32768]
25

Authentication
☐ Enable

User Name
User

Password

Confirm Password

Advanced

Use SSL/TLS
Never

Require CA Root Certificate
☐ Enable

File Name
There are no SSL certificates loaded.

Apply Cancel

You can use Simple Mail Transfer Protocol (SMTP) to send an email to a single recipient when an event occurs. To use the email feature, you must define the following settings:

Setting	Description
From Address	The IP addresses of the Domain Name System (DNS).
SMTP Server	The IPv4 address or DNS name of the local SMTP server. NOTE: This definition is required when the SMTP server is set to Local .
Port	The SMTP port number, with a default of 25. The range is 25, 465, 587, 5000 to 32768.
Authentication	Enable this if the SMTP server requires authentication.
User Name, Password, and Confirm Password	If your mail server requires authentication, enter your user name and password here.
Use SSL/TLS	Never: The SMTP server does not require nor support encryption. If Supported: The SMTP server advertises support for STARTTLS but doesn't require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given. Always: The SMTP server requires the STARTTLS command to be sent on connection to it. Implicitly: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.
Require CA Root Certificate	Select Enable if the security policy of your organization does not allow for implicit trust of SSL/TLS connections. When this setting is enabled, a valid root CA certificate must be loaded onto the Rack PDU for encrypted emails to be sent.

Configure Email Recipients

Path: Configuration > Notification > Email > Recipients

Click **Add Recipient** to specify up to four email recipients.

Click the **To Address** of an email recipient to edit settings for that recipient.

E-mail Recipient

Generation
☒ Enable

To Address

Format
☒ Long
☐ Short

Server

Custom E-mail Server Settings

From Address

SMTP Server

User Name

Password

Confirm Password

Advanced

Use SSL/TLS

Require CA Root Certificate
☐ Enable

File Name
 There are no SSL certificates loaded.

Setting	Description
E-mail Recipient	
Generation	Enables (default) or disables sending email to the recipient.
To Address	<p>The user and domain names of the recipient. To use email for paging, use the email address for the recipient's pager gateway account (for example, myacct100@skytel.com). The pager gateway will generate the page.</p> <p>To bypass the DNS lookup of the IP address of the mail server, use the IP address in brackets instead of the email domain name. For example, use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.</p>
Format	The Long format contains name, location, contact, IP address, serial number of the device, date and time, event code, and event description. The Short format provides only the event description.
Server	<p>The email routing method.</p> <p>Local: The recommended setting. Email is sent using the site-local SMTP server. This setting limits delays and network outages and retries sending email for many hours. When choosing the Local setting, you must also enable forwarding at the SMTP server of your device and set up a special external email account to receive the forwarded email. Check with your SMTP server administrator before making these changes.</p>

Setting	Description
	<p>Recipient: This is the SMTP server of the recipient. The Rack PDU performs an MX record look-up on the recipients email address and uses that as its SMTP server. The email is only sent once so it could easily be lost.</p> <p>Custom: This setting enables each email recipient to have their own server settings. These settings are independent of the SMTP Server setting under Configuration > Notification > Email > Server.</p>
Custom E-mail Server Settings	
From Address	The IP addresses of the Domain Name System (DNS).
SMTP Server	<p>The IPv4 address or DNS name of the local SMTP server.</p> <p>NOTE: This definition is required when the SMTP server is set to Local.</p>
Port	The SMTP port number, with a default of 25. The range is 25, 465, 587, 5000 to 32768.
Authentication	Enable this if the SMTP server requires authentication.
User Name, Password, and Confirm Password	If your mail server requires authentication, enter your user name and password here.
Advanced	
Use SSL/TLS	<p>Never: The SMTP server does not require nor support encryption.</p> <p>If Supported: The SMTP server advertises support for STARTTLS but doesn't require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given.</p> <p>Always: The SMTP server requires the STARTTLS command to be sent on connection to it.</p> <p>Implicitly: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.</p>
Require CA Root Certificate	Select Enable if the security policy of your organization does not allow for implicit trust of SSL/TLS connections. When this setting is enabled, a valid root CA certificate must be loaded onto the Rack PDU for encrypted emails to be sent.

Load an SSL Certificate

Path: Configuration > Notification > Email > SSL Certificates

Email Certificate Upload

Certificate

File Name	Size	Status
There are no SSL certificates loaded.		

Certificate File

Choose File

No file chosen

Add

Load a mail SSL/TLS certificate on the Rack PDU for greater security. The file must have an extension of .crt or .cer. Up to five files can be loaded at any given time. When installed, the certificate details also display on this page. An invalid certificate will display “n/a” for all fields except **File Name**.

You can also delete certificates from this screen. After a certificate is deleted, you must manually remove reference to this certificate from any of the email recipients using the certificate.

Send a Test Email

Path: Configuration > Notification > Email > Test

E-mail Test

Initiate Test

Last Test Result

No test performed.

Last Server Response

To

testaccount@se.com

Apply

Cancel

Send a test message to a configured recipient.

Configure SNMP Traps

With Simple Network Management Protocol (SNMP) traps, you can automatically get notifications for significant Rack PDU events. They are a useful tool for monitoring devices on your network.

Configure SNMP Trap Receivers

Path: Configuration > Notification > SNMP Traps > Trap Receivers

The trap receivers are displayed by **NMS IP/Host Name**, (NMS stands for Network Management System). You can configure up to six trap receivers. To configure a new trap receiver, click **Add Trap Receiver**. To edit (or delete) a trap receiver, select its IP address/host name.

SNMP Traps

The screenshot shows the 'Trap Receiver' configuration form. It has the following fields and options:

- Trap Generation:** ☒ Enable
- NMS IP/Host Name:** Text input field containing '0.0.0.0'.
- Port:** Text input field containing '162'.
- SNMPv1:** ☒ Selected.
- Community Name:** Text input field.
- Authenticate Traps:** ☒ Enable
- SNMPv3:** ☐ Not selected.
- User Name:** Dropdown menu showing 'Apc@123'.
- Buttons:** 'Apply' and 'Cancel' at the bottom.

Setting	Description
Trap Generation	Enable (the default) or disable trap generation for this trap receiver.
NMS IP/Host Name	The IPv4/ IPv6 address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.
Port	Enter the port for the trap receiver.
Select either SNMPv1 or SNMPv3 to specify the trap type. For an NMS to receive both types of traps, you must separately configure two trap receivers for that NMS, one for each trap type.	
SNMPv1	<p>Community Name: The name used as an identifier when SNMPv1 traps are sent to this trap receiver.</p> <p>Authenticate Traps: When this option is enabled (the default), the NMS identified by the NMS IP/ Host Name setting will receive authentication traps (traps generated by invalid attempts to log on to this device).</p>
SNMPv3	User Name: Enter the identifier of the user profile for this trap receiver.

If you delete a trap receiver, all notification settings configured under “Configuring event actions” for the deleted trap receiver are set to their default values.

Test SNMP Traps

Path: Configuration > Notification > SNMP Traps > Test

Last Test Result: The result of the most recent SNMP trap test. A successful SNMP trap test verifies only that a trap was sent; it does not verify that the trap was received by the selected trap receiver. A trap test succeeds if all of the following are true:

- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver itself is enabled.
- If a host name is selected for the **To** address, that host name can be mapped to an valid IP address.

To: Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver is configured, a link to the **Trap Receiver** configuration screen (**snmp receiver**) is displayed.

Configure Syslog Servers and Notifications

You can optionally send messages to a Syslog server. To set up Syslog notifications, first configure at least one Syslog Server. Then configure Syslog notification settings and complete a test to ensure your configuration works as intended.

Configure a Syslog Server

Path: Configuration > Logs > Syslog > Servers

Click **Add Server** to configure a new Syslog server.

Syslog Server

Syslog Server: Uses IPv4/ IPv6 addresses or host names to identify from one to four servers to receive Syslog messages sent by the Rack PDU.

Port: The port that the Rack PDU will use to send Syslog messages. The default UDP port assigned to Syslog is 514.

Protocol: Select either **UDP**, **TCP**, or **TLS**.

Client Certificate: Choose a client certificate to use with TLS mutual authentication. You must upload the client certificates separately apcapunder **Configuration > Security > SSL Certificates**.

Click **Apply** to save or **Cancel** to leave without saving.

Configure Syslog Notification Settings

Path: Configuration > Logs > Syslog > Settings

Message Generation: Enable the generation and the logging of Syslog messages for events that have Syslog configured as a notification method.

Facility Code: Selects the facility code assigned to the Syslog messages of the Rack PDU (User, by default).

NOTE: User best defines the Syslog messages sent by the Rack PDU. Do not change this selection unless advised to do so by the Syslog network or system administrator.

Severity Mapping: This section maps each severity level of the Rack PDU or environment events to available Syslog priorities. The local options are **Critical**, **Warning**, and **Informational**. You should not need to change the mappings.

- **Emergency:** The system is unusable
- **Alert:** Action must be taken immediately
- **Critical:** Critical conditions
- **Error:** Error conditions
- **Warning:** Warning conditions
- **Notice:** Normal but significant conditions
- **Info:** Informational messages
- **Debug:** Debug-level messages

The following are the default settings for **Local Priority**:

- **Critical** is mapped to **Critical**
- **Warning** is mapped to **Warning**
- **Informational** is mapped to **Info**

Test Syslog Notifications

Path: Configuration > Logs > Syslog > Test

Send a test message to the Syslog servers. The result will be sent to all configured Syslog servers.

Select a **Severity** to assign to the test message and then define the test message. Format the message to consist of the event type (for example, **APC**, **System**, or **Device**) followed by a colon, a space, and the event text. The message can have a maximum of 50 characters.

- The priority (PRI): the Syslog priority assigned to the message event, and the facility code of messages sent by the Rack PDU.
- The Header: a time stamp and the IP address of the Rack PDU.
- The message (MSG) part.
 - The **TAG** field, followed by a colon and space, identifies the event type.
 - The **CONTENT** field is the event text, followed (optionally) by a space and the event code.

Example: APC: Test Syslog is valid.

Configure Identification

Path: Configuration > General > Identification

General

Identification

Host Name Synchronization
☐ Enable

Name

apc79ED44

Contact

Unknown

Location

Unknown

System Message

1024 characters left

Apply

Cancel

Setting	Description
Host Name Synchronization	<p>Allows the host name to be synchronized with the system name so both fields automatically contain the same value.</p> <p>NOTE: When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the host name field).</p>
Name Contact Location	<p>Define the Name, the Contact (the person responsible for the device), and the Location (the physical location), used by the SNMP agent of the Rack PDU and Data Center Expert.</p> <p>Specifically, the name field is used by the sysName, sysContact, and sysLocation object identifiers (OIDs) in the SNMP agent of the Rack PDU. For more information about MIB-II OIDs, see the PowerNet® <i>SNMP Management Information Base (MIB) Reference Guide</i>, available at www.apc.com.</p>
System Message	<p>When defined, a custom message will appear on the log on screen for all users.</p>

Configure Date and Time Settings

Path: Configuration > General > Date/Time > Mode

Set the time and date used by the Rack PDU. You can change the current settings manually or through a Network Time Protocol (NTP) Server. With both methods, you must select the **Time Zone**. This is your local time difference with Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT).

Date/Time Mode

Current Settings

Date 10/17/2023	Time 22:24:42	Daylight Saving Time Disabled
Active Primary NTP Server 0.0.0.0	Active Secondary NTP Server 0.0.0.0	

System Time Configuration

Time Zone
-05:00 hours (Eastern Time) ▼

☒ Manual

Date mm/dd/yyyy
10/17/2023

Time hh:mm:ss
22:24:42

☐ Apply local computer time.

☐ Synchronize with NTP Server

☐ Override Manual NTP Settings

Primary NTP Server
0.0.0.0

Secondary NTP Server
0.0.0.0

Update Interval [1 to 8760]
336 hours

☐ Update using NTP now.

Apply Cancel

Setting	Description
Manual	Do one of the following: <ul style="list-style-type: none"> Enter the current Date and Time. Select the Apply Local Computer Time to apply the date and time settings of the computer you are using.
Synchronize with NTP Server	Have an NTP (Network Time Protocol) Server define the date and time for the Rack PDU. <ul style="list-style-type: none"> Override Manual NTP Settings: If you select this, data from other sources (typically DHCP) take precedence over the NTP configurations you set here. NTP Server: Enter the IP address or domain name of the NTP server. Update Interval: Define, in hours, how often the Rack PDU accesses the NTP Server for an update. Minimum = 1; Maximum = 8760 (1 year). Update Using NTP Now: Initiate an immediate update of the date and time by the NTP Server.

Configure Daylight Savings

Path: Configuration > General > Date/Time > Daylight Savings

Daylight Savings Configuration

Daylight Saving Time

☐ Disable DST
☐ Traditional US DST (Second Sunday in March to First Sunday in November)
☒ Custom DST Definition (Adds 1 hour at start, subtracts 1 hour at end)

Start

Date
 First Sunday of January

Time
 00 : 00

End

Date
 First Sunday of January

Time
 00 : 00

Note: Custom DST end time must be one hour or greater from the start time.

Daylight Saving Time (DST) is disabled by default. You can enable traditional United States DST, or enable and configure a customized daylight saving time to match how Daylight Saving Time is implemented in your local area.

When customizing DST, the system puts the clock forward by an hour when the time and date you specify under **Start** is reached and puts the clock back an hour when the time and date you specify under **End** is reached.

- If your local DST always starts or ends on the fourth occurrence of a specific weekday of a month (e.g., the fourth Sunday), choose Fourth/Last. If a fifth Sunday occurs in that month, you should still choose Fourth/Last.
- If your local DST always starts or ends on the last occurrence of a specific weekday of a month, whether it is the fourth or the fifth occurrence, choose Fifth/Last.

How to Create and Import Settings With the User Config File

Path: Configuration > General > User Config File

Uploading Configuration INI File

From this page, you can use the settings from one Rack PDU to configure another. Retrieve the config.ini file from the configured Rack PDU, customize that file (e.g., change the IP address), and upload the customized file to the new Rack PDU. The file name can be up to 64 characters, and must have the .ini suffix.

Status	<p>Reports the progress of the upload.</p> <ul style="list-style-type: none"> No configuration file uploaded: The Rack PDU has not been configured with a <i>config.ini</i> file. Configuration file successfully uploaded: The Rack PDU has been configured with a <i>config.ini</i> file. You may need to refresh the page to see this message. <p>NOTE: The upload succeeds even if the file contains errors, but a system event reports the errors in the Event Log.</p>
Upload	Browse to the customized file and upload it so that the current Rack PDU can use it to set its own configuration.
Download	Allows the download of the <i>config.ini</i> file directly through the Web browser to your computer.

Instead of uploading the file to one Rack PDU, you can export the file to multiple Rack PDU units by using an FTP or SCP script.

NOTE: To retrieve and customize the file of a configured Rack PDU, see [How to Export Configuration Settings](#), page 175.

Configure Quick Links

Path: Configuration > General > Quick Links

Use this page to change the URL links displayed at the bottom left of each page of the web UI.

By default, these links access the following Web pages:

- **Link 1:** The home page of the APC website
- **Link 2:** Software and firmware downloads for APC products
- **Link 3:** Information on EcoStruxure IT

Test: Blink the LCD or LEDs

Path: Tests > RPDU > LCD Blink

Path: Tests > Network > LED Blink

You can blink the LED or LCD to help locate the Rack PDU. Enter a number of minutes in the **Blink Duration** field on either page, then click **Apply**. The LCD

blink test causes the backlight of the display interface to blink. The LED blink test causes the LEDs on the Network port to blink.

Logs Tab

Event Log

Path: Logs > Events

By default, the log displays all events recorded during the last two days, starting with the latest events.


Additionally, the log records any event that sends an SNMP trap, except SNMP authentication failures, and abnormal internal system events.

You can enable color coding for events on the **Configuration > Security > Local Users Management** screen.

Filter the Event Log

Path: Logs > Events > Log

By default, the event log displays the most recent events first. To see the events listed together on a Web page, click **Launch Log in New Window**.

To open the log in a text file or to save the log to disk, click on the floppy disk icon () on the same line as the **Event Log** heading.

You can also use FTP or Secure CoPy (SCP) to view the event log. See *Use FTP or SCP to Retrieve Log Files*, page 171.

Filtering event logs: Use filtering to omit information you don't want to display.

- Filtering the log by date or time: Use the **Last** or **From** radio buttons. (The filter configuration is saved until the Rack PDU restarts.)
- Filtering the log by event severity or category:
 1. Click **Filter Log**.
 2. Clear a check box to remove it from view.
 3. After you click **Apply**, text at the upper right corner of the **Event Log** page indicates that a **Filter Is Active**. The filter is active until you clear it or until the Rack PDU restarts.
- Removing an active filter:
 1. Click **Filter Log**.
 2. Click **Clear Filter (Show All)**.
 3. As Administrator, click **Save As Default** to save this filter as the new default log view for all.

Important points on filtering:

- Events are processed through the filter using OR logic. If you apply a filter, it works regardless of the other filters.
- Events that you cleared in the **Filter By Severity** list never display in the filtered Event Log, even if selected in the **Filter by Category** list.
- Similarly, events that you clear in the **Filter by Category** list never display in the filtered Event Log.

Deleting event logs: To delete all events, click **Clear Log**. Deleted events cannot be retrieved. To disable the logging of events based on their assigned severity level or their event category, see *Configure Event Actions*, page 154.

Reverse Lookup

Path: Logs > Events > Reverse Lookup

With reverse lookup enabled, when a network-related event occurs, both the IP address and the domain name for the networked device with the event are logged in the event log. If no domain name entry exists for the device, only its IP address is logged with the event.

Since domain names generally change less frequently than IP addresses, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events.

Reverse lookup is disabled by default. You should not need to enable it if you have no DNS server configured or have poor network performance because of heavy network traffic.

Event Log Size

Path: Logs > Events > Size

Use **Event Log Size** to specify the maximum number of log entries.

NOTE: NOTE: When you resize the event log in order to specify a maximum size, all existing log entries are deleted. When the log subsequently reaches the maximum size, the older entries are deleted.

Network Port Sharing event logs and traps: Rack PDU events from guest Rack PDUs are sent to the host Rack PDU for inclusion into its log. The log entry will include the Display ID of the unit that the event occurred on. These events are then handled the same as local events from the host PDU. Therefore alarms, SNMP traps, emails, Syslog, etc., will support Rack PDU events and alarms from all Rack PDUs in a group.

Example event log:

Example event log: Rack PDU 4: Device low load.

NOTE: System events will only be logged for the host Rack PDU. System events from guest Rack PDUs will not be logged on the host PDU.

Data Log

Use the data log to display measurements about the Rack PDU, the power input to the Rack PDU, and the ambient temperature of the Rack PDU.

The steps to display and resize the data log are the same as for the event log, except that you use menu options under **Data** instead of **Events**.

Filter the Data Log

Use the data log to display measurements about the Rack PDU, the power input to the Rack PDU, and the ambient temperature of the Rack PDU.

The steps to display and resize the data log are the same as for the event log, except that you use menu options under **Data** instead of **Events**.

Path: Logs > Data > Log

Filtering data logs: Use filtering to omit information you don't want to display. Using the **Network Port Sharing Data Log**, the host Rack PDU will poll data from guest Rack PDUs so that data from all Rack PDUs in a group are available. To view data from a different Rack PDU in a group, select the desired Rack PDU from the "Filter Log" pull-down list.

Similarly for data log graphing, you can select a different Rack PDU by clicking on the **Change Data Filter** button.

- Filtering the log by date or time: Use the **Last** or **From** radio buttons. (The filter configuration is saved until the Rack PDU restarts.)
- Filtering the log by event severity or category:
 1. Click **Filter Log**.
 2. Clear a check box to remove it from view.
 3. After you click **Apply**, text at the upper right corner of the **Data Log** page indicates that a **Filter Is Active**. The filter is active until you clear it or until the Rack PDU restarts.
- Removing an active filter:
 1. Click **Filter Log**.
 2. Click **Clear Filter (Show All)**.
 3. As Administrator, click **Save As Default** to save this filter as the new default log view for all users.

Deleting data logs: To delete all data log records, click **Clear Data Log**. Deleted data log records cannot be retrieved.

Log Interval

Path: Logs > Data > Interval

Define, in the **Log Interval** setting, how frequently data is searched for and stored in the data log. When you click **Apply**, the number of possible storage days is recalculated and display at the top of the screen. When the log is full, the oldest entries are deleted.

NOTE: Because the interval specifies how often the data is recorded, the smaller the interval, the more times the data is recorded and the larger the log file.

Data Log Graphing

Data log graphing provides a graphical display of logged data and is an enhancement of the existing data log feature. How the graphing enhancement displays data and how efficiently it performs will vary depending on your computer hardware, computer operating system, and the Web browser you use to access the interface of the unit.

NOTE: JavaScript® must be enabled in your browser to use the graphing feature. Alternatively, you can use FTP or SCP to import the data log into a spreadsheet application, and graph data in the spreadsheet.

Graph Data: Select the data items that correspond to the abbreviated column headings in the data log to graph multiple data items. Hold down CTRL to select multiple items.

Graph Time: Select **Last** to graph all records or to change the number of hours, days, or weeks for which data log information is graphed. Select a time option from the drop-down menu. Select **From** to graph data logged during a specific time period.

NOTE: Enter time using the 24-hour clock format.

Apply: Click **Apply** to graph the data.

Launch Graph in New Window: Click **Launch Graph in New Window** to launch the data log graph in a new browser window that provides a larger view of the graph.

Data Log Rotation

Rotation causes the contents of the data log to be appended to the file you specify by name and location. Use this option to set up password-protection and other parameters.

- **FTP Server:** The IP address or host name of the server where the file will reside.
- **User Name/Password:** The user name with password required to send data to the repository file. This user must also be configured to have read and write access to the data repository file and the directory (folder) in which it is stored.
- **File Path:** The path to the repository file.
- **Filename:** The name of the repository file (an ASCII text file), e.g. datalog.txt. Any new data is appended to this file: it does not overwrite it.
- **Unique Filename:** Select this check box to save the log as *mmdyyy*, where filename is what you specified in the Filename field above. Any new data is appended to the file but each day has its own file.
- **Delay *n* hours between uploads:** The number of hours between uploads of data to the file (max. 24 hours).
- **Upon failure, try uploading every *n* minutes:** The number of minutes between attempts to upload data to the file after a failed upload.
 - **Up to *n* times:** The maximum number of times the upload will be attempted after it fails initially.
 - **Until upload succeeds:** Attempt to upload the file until the transfer is completed.

Data Log Size

Use **Data Log Size** to specify the maximum number of log entries.

NOTE: When you resize the data log in order to specify a maximum size, all existing log entries are deleted. When the log subsequently reaches the maximum size, the older entries are deleted.

Firewall Logs

Path: Logs > Firewall

If you create a firewall policy, firewall events will be logged here.

The information in the log can be useful to help the technical support team solve problems. Log entries contain information about the traffic and the rules action (allowed or discarded). When logged here, these events are not logged in the main Event Log (see section [Event Log](#), page 168).

A firewall log contains up to 50 of the most recent events. The firewall log is cleared when the management interface reboots.

Use FTP or SCP to Retrieve Log Files

An Administrator or Device User can use FTP or SCP to retrieve a tab-delimited Event Log file (*event.txt*) or Data Log file (*data.txt*) and import it into a spreadsheet.

- The file reports all events or data recorded since the log was last deleted or (for the data log) truncated because it reached maximum size.

- The file includes information that the Event Log or Data Log does not display.
 - The version of the file format (first field)
 - The date and time the file was retrieved
 - The **Name**, **Contact**, and **Location** values and IP address of the Rack PDU
 - The unique **Event Code** for each recorded event (*event.txt* file only)

NOTE: The Rack PDU uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits.

If you are using the encryption-based security protocols for your system, use SCP to retrieve the log file.

If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.

NOTE: By default, FTP is disabled and SCP (via SSH) is enabled.

See the *Security Handbook*, available at www.apc.com, for information on available protocols and methods to set up the type of security you need.

Use SCP to Retrieve the Files

To retrieve the *event.txt* file, use the following command:

```
scp -c <cipher> username@hostname_or_ip_address:event.txt
./event.txt
```

To use SCP to retrieve the *data.txt* file, use the following command:

```
scp -c <cipher> username@hostname_or_ip_address:data.txt
./data.txt
```

NOTE:

- This SCP command is for OpenSSH. The command may differ depending on the SSH tool used.
- When using OpenSSH, *<cipher>* can be either aes256-cbc or 3des-cbc.

Use FTP to Retrieve the event.txt or data.txt Files

1. At a command prompt, type `ftp` and the IP address of the Rack PDU, and press ENTER. If the **Port** setting for the **FTP Server** option (set through the **Network** menu of the **Administration** tab) has been changed from its default (**21**), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

```
ftp>open ip_address port_number
```

You can set a non-default port value to enhance security for the FTP Server, see “FTP Server”. You can specify any port from 5001 to 32768.

2. Use the case-sensitive **User Name** and **Password** for Administrator or Device User to log on. For Administrator, **apc** is the default for **User Name** and **Password**. For the Device User, the defaults are device for **User Name** and **apc** for **Password**.
3. Use the `get` command to transmit the text of a log to your local drive.

```
ftp>get event.txt
```

or

```
ftp>get data.txt
```
4. Type `quit` at the `ftp>` prompt to exit from FTP.

View Customer Support Information

The About tab provides information that can help Customer Support Representatives troubleshoot issues with your Rack PDU.

Path: About > RPDU

About

Easy Rack PDU Metered-by-Outlet with Switching

Name apc79ED44	Location Unknown	Contact Unknown
Model Number EPDU2232SMBO	Rating 3 ø, 6 Banks, 32 A	Serial Number 1A2320FD0034
Hardware Revision 1.0.0	Manufacture Date 05/14/2023	Present Phases 3
Metered Phases 3	Metered Banks 6	Metered Outlets 24
Switched Outlets 24	Present Outlets 24	NMC Serial Number ZA2307005645
NMC Uptime 0 Days 7 Hours 26 Minutes	Network Link Link Active	

Firmware

Rack PDU

Version 1.0.0.3	Date Sep 28 2023
---------------------------	----------------------------

APC OS (AOS)

Version 2.5.0.8	Date Sep 28 2023
---------------------------	----------------------------

Boot Monitor

Version 1.5.1.1	Date Mar 27 2023
---------------------------	----------------------------

RPDU Controller

Version 1.0.28	Date Sep 19 2023
--------------------------	----------------------------

The hardware information is useful to Schneider Electric Customer Support for troubleshooting problems with the Rack PDU. The serial number and MAC address are also available on the Rack PDU itself. **NMC Uptime** is the length of time the network management interface has been running continuously.

Path: About > Network

Factory Information

Hardware Factory

Model Number EPOU2232SMB0	Serial Number 1A2320F00034	Hardware Revision 1.0.0
Manufacture Date 05/14/2023	MAC Address 28 29 86 79 ED 44	Management Uptime 0 Days 7 Hours 27 Minutes

Network Management Card

Model Number 0N-1570	Serial Number ZA2307005645
Hardware Revision 3	Manufacture Date 02/15/2023

Application Module

Name epdu	Version v1.0.0.3
Date Sep 28 2023	Time 07:00:45

APC OS (AOS)

Name aos	Version v2.5.0.8
Date Sep 28 2023	Time 06:58:22

APC Boot Monitor

Name boot	Version v1.5.1.1
Date Mar 27 2023	Time 12:10:09

Firmware information for the Rack PDU Application Module, APC OS (AOS), Boot Monitor, and RPDU Controller indicates the firmware version the date and time each firmware module was created. This information is also useful in troubleshooting and enables you to determine if updated firmware is available at the website, www.se.com.

Path: About > Support

Troubleshooting

Support Resources

Name	URL
Knowledge Base	http://www.apc.com/site/support/index.cfm?faq/
Company Contact Information	http://www.apc.com/support/contact/index.cfm
Software & Firmware Downloads	http://www.apc.com/tools/download/index.cfm

Technical Support Debug Information Download

This feature captures an assortment of debug data into a single file and then allows the user to download that file to a local computer which is intended for technical support use.

Generate Logs

Download

Note: File generation may take awhile to complete.

On this page, you can consolidate various data in this interface into a single zipped file for troubleshooting purposes and customer support. The data includes the event log, the configuration file, and complex debugging information. Click **Generate Logs** to create the file, and then click **Download** when generation is complete. You will be asked whether you want to view or save the zipped file.

How to Export Configuration Settings

Summary of the Procedure

A Super User/Administrator can retrieve the .ini file of a Rack PDU and export it to another Rack PDU or to multiple Rack PDUs. The steps are below; see details in the sections following.

1. Configure a Rack PDU with the desired settings, and retrieve the .ini file from that Rack PDU.
2. If desired, you can edit the .ini file with any text editor before uploading it to another device. Data entries may not be moved between sections. Lines will not be processed if they start with a semicolon (;).
3. Use a file transfer protocol supported by the Rack PDU to transfer a copy to one or more other devices. For a transfer to multiple Rack PDUs, use an FTP or SCP script or the .ini file utility. Each receiving unit uses the file to re-configure its own settings and then deletes it.

NOTE: FTP is disabled by default. If needed, you can enable FTP under **Configuration > Network > FTP Server**.

NOTE: Managing Users via the config.ini - Users are no longer managed via the config.ini in any form. Users are now managed via a separate file with the .csf extension. For further information on this topic, refer to FAQ article FA156117: How can I mass configure a Network Management Card (NMC) or NMC embedded product? To find an FAQ article, go to www.apc.com, and select your location if prompted to do so. Then select **Support > Browse FAQs** and enter the article number or title of the FAQ in the Search bar.

Contents of the .ini File

The config.ini file you retrieve from an Rack PDU contains the following:

- Section headings and keywords (only those supported for the particular device from which you retrieve the file): **Section headings** are category names enclosed in brackets ([]). **Keywords**, under each section heading, are labels describing specific Rack PDU settings. Each keyword is followed by an equal sign and a value (either the default or a configured value).
- The `Override` keyword: With its default value, this keyword helps prevent the exporting of one or more keywords and their device-specific values. For example, in the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the Rack PDU) blocks the exporting of values for the `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.

.ini and Network Port Sharing

The .ini configuration utility is able to get and set values for all devices in a group. In order to be backwards compatible, the host Rack PDU will always be designated as first, "PDU_A". Any guest Rack PDUs are then designated "PDU_B", "PDU_C", and "PDU_D" based on their Display ID in ascending order up to PDU_Z. After that, further PDUs are designated PDU_AA, up to PDU_FF. Therefore, "PDU_A" will not necessarily correlate to Display ID 1, and so on.

NOTE: Because of the large number of configuration values possible in a Rack PDU group, it may take a very long time to process an INI file set. For example, a Rack PDU group of 4 units with all values changing may take 30 minutes to complete processing.

Detailed Procedures

Retrieve .ini File

If possible, use the interface of a Rack PDU to configure it with the settings to export. (Directly editing the .ini file risks introducing errors).

Then retrieve *config.ini* from the configured Rack PDU via FTP, SCP, or the Web UI:

To use FTP

1. Open a connection to the Rack PDU using its IP address:
2. Log on using the Super User/Administrator user name and password.
3. Retrieve the *config.ini* file containing the settings of the Rack PDU:

```
ftp> get config.ini
```

The file is written to the folder from which you launched FTP.

To export configuration settings to multiple Rack PDUs, see FAQ article FA156117: *How can I mass configure a Network Management Card (NMC) or NMC embedded product?* To find an FAQ article on www.se.com, enter the title or number of the article in the search bar. On the resulting page, select **Faq** to narrow your search results to only FAQ articles.

To use SCP

Use the following command:

```
scp -c <cipher> username@hostname_or_ip_address:config.ini  
./config.ini
```

Then enter the correct password.

NOTE:

- This SCP command is for OpenSSH. The command may differ depending on the SSH tool used.
- When using OpenSSH, <cipher> can be either aes256-cbc or 3des-cbc. Aes256 is more secure.

To use the Web UI:

Navigate to **Configuration > General > User Config File** and select **Download**.

Edit .ini File

Edit the file carefully before you transfer it to other Rack PDUs.

1. Use a text editor to make your changes.
 - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
 - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
 - Enclose in quotation marks any values that contain leading or trailing spaces or are already enclosed in quotation marks.
 - To export scheduled events, configure the values directly in the .ini file.
 - To export a system time with the greatest accuracy, if the receiving Rack PDUs can access a Network Time Protocol server, configure `enabled` for `NTPEnable`:

```
NTPEnable=enabled
```

Alternatively, reduce transmission time by exporting the `[SystemDate/Time]` section as a separate .ini file.
 - To add comments, start each comment line with a semicolon (;).
2. Copy the customized file to another file name in the same folder:
 - The file name can have up to 64 characters and must have the .ini suffix.
 - Retain the original customized file for future use. **The file that you retain is the only record of your comments.**

Transfer the File To a Single Rack PDU

To transfer the .ini file to another Rack PDU, do either of the following:

- From the Web UI of the receiving Rack PDU, select **Configuration > General > User Config File**. Enter the full path of the file, or use Browse on your local PC.
- Use any file transfer protocol supported by Rack PDUs, i.e., FTP, FTP Client, SCP, or TFTP. The following example uses FTP:
 1. From the folder containing the copy of the customized .ini file, use FTP to log in to the Rack PDU to which you are exporting the .ini file:

```
ftp> open ip_address
```
 2. Export the copy of the customized .ini file to the root directory of the receiving Rack PDU:

```
ftp> put filename.ini
```

Transfer the File To Multiple Rack PDUs

To transfer the .ini file to multiple Rack PDUs, do one of the following:

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single Rack PDU.
- Use a batch processing file and the .ini file utility.

To create the batch file and use the utility, see FAQ article FA156117: *How can I mass configure a Network Management Card (NMC) or NMC embedded product?* To find an FAQ article on www.se.com, enter the title or number of the article in the search bar. On the resulting page, select **Faq** to narrow your search results to only FAQ articles.

The Upload Event and Error Messages

The Event and Its Error Messages

The following event occurs when the receiving Rack PDU completes using the .ini file to update its settings.

Configuration file upload complete, with number valid values

If a keyword, section name, or value is invalid, the upload by the receiving Rack PDU succeeds, and additional event text states the error.

Event text	Description
Configuration file warning: Invalid keyword on line number. Configuration file warning: Invalid value on line number.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line number.	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line number.	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, an incomplete upload occurs. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in Config.ini

A Rack PDU from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the Rack PDU is not present or is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values. For example: Rack PDU not discovered

If you did not intend to export the Rack PDU configuration as part of the .ini file import, ignore these messages.

Errors Generated By Overridden Values

The `Override` keyword and its value will generate error messages in the Event Log when it blocks the exporting of values. See [Contents of the .ini File](#), page 175 for information about which values are overridden.

Because the overridden values are device-specific and not appropriate to export to other Rack PDUs, ignore these error messages. To prevent these error messages, delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Related Topics

On Windows operating systems, instead of transferring .ini files, you can use the Device IP Configuration Wizard to update the basic TCP/IP settings of the Rack PDU and configure other settings through its user interface. See [Device IP Configuration Utility](#), page 13 for instructions to download and install the Device IP Configuration Wizard.

Updating Firmware

When you update the firmware on the Rack PDU:

- You obtain the latest bug fixes and performance improvements.
- New features become available for immediate use.

Keeping the firmware versions consistent across your network helps ensure that all Rack PDUs support the same features in the same manner. Here, upgrading simply means placing the firmware file on the Rack PDU; there is no installation required. Check regularly on www.se.com for any new updates.

Firmware File Transfer Methods

To upgrade the firmware of one or more NMCs **to firmware version 3.x or later**, download the Secure NMC System Tool for your application (SU or SUCAN) from the APC website. For more information on how to use the Secure NMC System Tool, please consult the *Secure NMC System (SNS) Tool User Guide*.

NOTE: A valid Secure NMC System subscription is required to upgrade to firmware version 3.x using the Secure NMC System Tool.

NOTE: Firmware versions 3.x or later are not currently available in China or Japan. The latest firmware version available is version 2.5.0.6.

To update the firmware of one or more NMCs **to firmware version 2.5.x or earlier**, use one of these five methods:

- On a Windows operating system, use the **Firmware Update Utility** downloaded from www.apc.com. See *Use the Firmware Upgrade Utility For Multiple Upgrades*, page 183.
- On any supported operating system, use **FTP** or **SCP** to transfer the `.nmc3` file. See *Use FTP or SCP to Update One Rack PDU*, page 181.
- For a Network Management Card that is NOT on your network, use **XMODEM** through a USB virtual communication port via the boot loader to transfer the `.nmc3` file from your computer to the NMC. See *Use XMODEM To Upgrade One Rack PDU*, page 182.
- Use a **USB drive** to transfer the `.nmc3` file from your computer to the NMC. See *Use a USB Drive To Transfer and Update Files*, page 182.
- For updates to **multiple NMCs**, see *Use the Firmware Upgrade Utility For Multiple Upgrades*, page 183.

Use the Firmware Update Utility

This Firmware Update Utility is part of the firmware update package available on www.apc.com. *(Never use an Update Utility designated for one product to update the firmware of another product).*

Use the Utility for updates on Windows-based systems. On any supported Windows operating system, the Firmware Update Utility automates the firmware transfer.

Unzip the downloaded firmware update file and double-click the .exe file. Then enter the IP address, the user name, and the password in the dialog fields and click **Start Update Now**. You can use the **Ping** button to test your entered details.

Use the Utility for manual updates, primarily on Linux. On non-Windows operating systems, the Firmware Update Utility extracts the firmware file, but does not upgrade the Rack PDU.

To extract the firmware files:

1. After extracting files from the downloaded firmware upgrade file, run the **Firmware Update Utility** (the .exe file).
2. At the prompts, click **Next>**, then specify the directory location to which the files will be extracted.
3. When the **Extraction Complete** message displays, close the dialog box.

See *Firmware File Transfer Methods*, page 179 for the different upgrade methods after extraction.

Use FTP or SCP to Update One Rack PDU

FTP

To use FTP to update a Rack PDU over the network:

- The Rack PDU must be on the network with its system IP, subnet mask, and default gateway configured.
- The FTP server must be enabled at the Rack PDU. You can enable the FTP server under **Configuration > Network > FTP Server**.

To transfer the files:

1. Extract the firmware file.
2. At a computer on the network, open a command prompt window. Go to the directory that contains the firmware files, and list the files:

```
C:\>cd apc  
C:\apc>dir
```
3. Open an FTP client session: `C:\apc>ftp`
4. Type `open` with the IP address of the Rack PDU, and press ENTER. If the **port** setting for the FTP Server has changed from its default of **21**, you must use the non-default value in the FTP command.
 - For Windows FTP clients, separate a non-default port number from the IP address by a space. For example (showing a space before 21000):

```
ftp> open 150.250.6.10 21000
```
 - Some FTP clients require a colon instead before the port number.
5. Log on as the Super User or Administrator. The default username and password for the Super User are both **apc**.
6. Use the `put` command to send the .nmc3 file: `put filename.nmc3`
For example: `put apc_hw21_rpdu2g_0-0-0.nmc3`
(where 0-0-0 is the firmware version number).
7. When FTP confirms the transfer, type `quit` to close the session.

SCP

To use Secure CoPy (SCP) to update firmware for the Rack PDU, follow these steps:

NOTE: As SCP is part of SSH, enabling SSH also enables SCP. SSH is enabled by default.

1. Locate the firmware file.
2. Use an SCP command line to transfer the firmware to the Rack PDU. The following example uses 0-0-0 to represent the version number of the firmware:

```
scp -c <cipher> apc_hw21_rpdu2g_0-0-0.nmc3  
apc@158.205.6.185:apc_hw21_rpdu2g_0-0-0.nmc3
```

NOTE: This SCP command is for OpenSSH. The command may differ depending on the SSH tool used. `<cipher>` can be either `aes256-cbc` or `3des-cbc`.

Use XMODEM To Upgrade One Rack PDU

To use XMODEM to upgrade one Rack PDU that is not on the network, you must extract the firmware files from the Firmware Upgrade Utility.

To transfer the files:

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect a Micro USB cable to the selected port and to the Console port at the Rack PDU.
3. Run a terminal program such as TeraTerm or HyperTerminal, and configure the selected port for 115200 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press the **Reset** button on the Rack PDU, then immediately press ENTER twice, or until the Boot Monitor prompt displays: `BM>`
5. Type `XMODEM ()`, then press ENTER.
6. From the terminal program's menu, select **XMODEM**, then select the `.nmc3` firmware file to transfer using XMODEM. After the XMODEM transfer is complete, the Boot Monitor prompt returns.
7. Type `reset ()` or press the **Reset** button to restart the network management interface.

Use a USB Drive To Transfer and Update Files

Before starting the transfer, make sure the USB drive is formatted in FAT32.

1. Create a folder named **apcfirm** on the USB flash drive.
2. Download the firmware update files and unzip them if needed. Copy the **app.nmc3** firmware file into the **apcfirm** folder.

NOTE: Only use firmware applications intended for your device type and NMC.

3. Use a text editor to create a file named **nmc3.rcf** and save it to the **apcfirm** folder. (The file extension must be `.rcf`, not `.txt` for example.)

Add only the following text to the file: `NMC3=application_name.nmc3`, where `application_name` is filename of the firmware update file.

For example: If the update firmware file is

`apc_hw21_rpdu2g_0-0-0-xx.nmc3`, the text file should say
`NMC3=apc_hw21_rpdu2g_0-0-0-xx.nmc3`

Save the changes to the `nmc3.rcf` file.

4. Insert the flash drive into a USB port on your Rack PDU.
5. Use the Web UI, the CLI, or the **Reset** button on the front of the Rack PDU to reboot the management interface. Wait for the reboot to finish.

Check that the update was completed successfully using the procedures in [Verifying Upgrades and Updates](#), page 184.

How To Update Multiple Rack PDUs

Use one of these methods:

- **Firmware Update Utility:** Use this for multiple firmware updates in IPv4 if you have Windows. The Utility records all update steps in a log as a good reference to validate the update. The Utility is included with your firmware download. For more information, see the following:
 - Use the Firmware Update Utility, page 180, or
 - FAQ article FA156099: *How do I perform a mass firmware upgrade on APC network enabled products?* on www.se.com. To find an FAQ article on www.se.com, enter the title or number of the article in the search bar. On the resulting page, select **Faq** to narrow your search results to only FAQ articles.
- **Export configuration settings:** You can create batch files and use the .ini file utility to retrieve configuration settings from multiple Rack PDU and export them to other Rack PDUs. For more information on how to download the .ini file utility,
 - See FAQ article FA156117: *How can I mass configure a Network Management Card (NMC) or NMC embedded product?* on www.se.com. To find an FAQ article on www.se.com, enter the title or number of the article in the search bar. On the resulting page, select **Faq** to narrow your search results to only FAQ articles.
 - Read the release notes (release notes are included with the utility file).
- **Use FTP or SCP to update multiple Rack PDUs:** To update multiple Rack PDUs using an FTP client or using SCP, write a script which automatically performs the procedure.

NOTE: To find an FAQ article, go to www.apc.com, and select your location if prompted to do so. Then select **Support > Browse FAQs** and enter the article number or title of the FAQ in the Search bar.

Use the Firmware Upgrade Utility For Multiple Upgrades

After downloading the Upgrade Utility, double click on the .exe file to run the utility (which ONLY works with IPv4) and follow these steps to upgrade your Rack PDU firmware:

1. Type in an IP address, a user name, and a password.
2. Open the devices.txtfile. This should list any device IP, user name, and password.
3. Select the **Upgrade From Device List** check box to use the *iplist.txt* file.
4. Choose the **Upgrade Now** button to start the firmware version update(s).
5. Choose **View Log** to verify any upgrade.

Upgrade Firmware for Network Port Sharing (NPS) Groups

For an NPS Group, all Rack PDUs in the group must have the same firmware version. Upgrade the host Rack PDU and it will upgrade all guest Rack PDUs automatically. This may take up to 10 minutes.

Verifying Upgrades and Updates

Verify the Success Or Failure of the Transfer

To verify whether a firmware update succeeded, use the `xferStatus` command in the CLI to view the last transfer result, or use an SNMP GET to the `mfiletransferStatusLastTransferResult` OID.

Last Transfer Result Codes

Possible transfer errors include the TFTP or FTP server not being found, or the server refusing access, the server not finding or not recognizing the transfer file, or a corrupt transfer file.

SNMP Return Value	Code	Description
1	Successful	The file transfer was successful.
2	Result not available	There are no recorded file transfers.
3	Failure unknown	The last file transfer failed for an unknown reason.
4	Server inaccessible	The TFTP or FTP server could not be found on the network.
5	Server access denied	The TFTP or FTP server denied access.
6	File not found	The TFTP or FTP server could not locate the requested file.
7	File type unknown	The file was downloaded but the contents were not recognized.
8	File corrupt	The file was downloaded but at least one Cyclical Redundancy Check (CRC) failed.

Verify the Version Numbers of Installed Firmware

You can check the firmware version in the Web UI or the display interface. In the CLI, you can use the `about` command to check the firmware version.

You can also use an SNMP GET to the get the MIB II `sysDescr` OID.

Troubleshooting

For problems that persist or are not described here, contact APC Customer Care at www.apc.com.

Rack PDU Access Issues

Problem	Solution
Unable to ping the Rack PDU	<p>If the Rack PDU's Network Status LED is green, try to ping another node on the same network segment as the Rack PDU. If that fails, it is not a problem with the Rack PDU. If the Network Status LED is not green, or if the ping test succeeds, perform the following checks:</p> <ul style="list-style-type: none">• Verify all network connections.• Verify the Network Settings of the Rack PDU.
Cannot access the Web User Interface	<ul style="list-style-type: none">• Verify that HTTP or HTTPS access is enabled.• Make sure you are specifying the correct URL — one that is consistent with the security system used by the Rack PDU. SSL requires HTTPS, not HTTP, at the beginning of the URL.• Verify that you can ping the Rack PDU.• Verify that you are using a Web browser supported for the Rack PDU.• If the Rack PDU has just restarted and SSL security is being set up, the Rack PDU may be generating a server certificate. The Rack PDU can take up to several minutes to create this certificate, and the SSL server is not available during that time.

SNMP Issues

Problem	Solution
Unable to perform a GET or SET	<ul style="list-style-type: none">• Verify the community name (SNMPv1 or SNMPv2c) or the Authentication configuration (SNMPv3). See Configure SNMP Settings, page 147.• Verify the UDP port 161 of NMS is correctly opened.
Unable to receive traps at the NMS	<ul style="list-style-type: none">• Verify the Trap Proxy Server IP address configuration is correct.• Verify the UDP port 162 of NMS is correctly opened.

Download Log Files to a USB Flash Drive

1. Insert a USB Flash drive to the USB port on the Display Interface of the Rack PDU. Before starting the transfer, make sure the USB drive is formatted in FAT32.
2. Scroll to **Log to Flash** on the Display Screen and press the **Select** button.
3. Press the **Select** button again to export the Log files to your Flash drive.

You may abort the download by pressing the **Select** button at any time during the download process.

NOTE: If a debug.txt file or a dump.txt file does not exist on the Rack PDU, it cannot be downloaded to the USB Flash drive. These files are only created following an unexpected system crash or a Network Management Card (NMC) reset. The debug.txt and dump.txt files are used for technical support only.

Worldwide Customer Support

Support for this product is available at www.apc.com.

Source Code Copyright Notice

cryptlib copyright Digital Data Security New Zealand Ltd 1998.

Copyright © 1990, 1993, 1994 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Mike Olson.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

© 2025 – 2025 Schneider Electric. All rights reserved.

TME63709