User Guide

Rack Power Distribution Units and In-Line Current Meters

AP7XXXB

990-5848B-001

Publication Date: August 2019

by Schneider Electric

APC by Schneider Electric Legal Disclaimer

The information presented in this manual is not warranted by the APC by Schneider Electric to be authoritative, error free, or complete. This publication is not meant to be a substitute for a detailed operational and site specific development plan. Therefore, APC by Schneider Electric assumes no liability for damages, violations of codes, improper installation, system failures, or any other problems that could arise based on the use of this Publication.

The information contained in this Publication is provided as is and has been prepared solely for the purpose of evaluating data center design and construction. This Publication has been compiled in good faith by APC by Schneider Electric. However, no representation is made or warranty given, either express or implied, as to the completeness or accuracy of the information this Publication contains.

IN NO EVENT SHALL APC BY SCHNEIDER ELECTRIC, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF APC BY SCHNEIDER ELECTRIC OR THEIR RESPECTIVE OFFICERS, DIRECTORS, OR EMPLOYEES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF APC BY SCHNEIDER ELECTRIC HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. APC BY SCHNEIDER ELECTRIC RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

Copyright, intellectual, and all other proprietary rights in the content (including but not limited to software, audio, video, text, and photographs) rests with APC by Schneider Electric or its licensors. All rights in the content not expressly granted herein are reserved. No rights of any kind are licensed or assigned or shall otherwise pass to persons accessing this information.

This Publication shall not be for resale in whole or in part.

Table of Contents

Introduction 1

Product Features 1

Types of User Accounts 2

Watchdog Features 2

Overview 2

Network interface watchdog mechanism 2

Resetting the network timer 2

EnergyWise 3

Getting Started 3

Establish Network Settings 4

IPv4 initial setup 4

IPv6 initial setup 4

TCP/IP configuration methods 4

.ini file utility 4

DHCP and BOOTP configuration 4

Network Management with Other Applications 5

Command Line Interface (CLI) 5

Recovering from a Lost Password 6

Device Display Panels 7

Display Panel Description 8

Network Status LED 9

10/100 LED 9

Load indicator LED 9

Command Line Interface..... 10

About the Command Line Interface (CLI) 10

Log on to the CLI 10

Local access to the Command Line Interface 10

Remote access to the Command Line Interface 11

About the Main Screen. 12

Using the CLI 14

Command Syntax. 14

Command Response Codes 15

CLI Commands for Rack PDUs by SKU/type 16

Network Management Card Command Descriptions 18
? or help 18
about 19
alarmcount 19
boot 20
cd 20
cipher 21
clrrst 23
console 23
date 24
delete 24
dir 25
dns 26
eapol 27
email 28
eventlog 29
exit, quit, or bye 30
firewall 30
format 31
ftp 31
lang 32
lastrst 32
ledblink 32
logzip 32
netstat 33
ntp 33
ping 34
portSpeed 34
prompt 35
pwd 35
radius 36
reboot 37
resetToDef 37
session 38
smtp 38
snmp 39
snmpv3 40
snmptrap 42
system 43
tcpip 44
tcpip6 45
user 46
userdflt 47
web 49
whoami 49
xferINI 50
xferStatus 50

Device Command Descriptions 51
bkLowLoad 51
bkNearOver 51
bkOverLoad 52
bkPeakCurr 52
bkReading 53
bkRestrictn 53
devStartDly 54
energyWise 55
olAssignUsr 56
olCancelCmd 56
olDlyOff 57
olDlyOn 57
olDlyReboot 58
olGroups 59
olName 60
olOff 60
olOn 61
olOffDelay 61
olOnDelay 62
olRbootTime 63
olReboot 63
olStatus 64
olUnasgnUsr 64
phBal 65
phBalAlGen 65
phLowLoad 66
phNearOver 66
phOverLoad 67
phPeakCurr 67
phReading 68
phRestrictn 68
prodInfo 69
userAdd 69
userDelete 70
userPasswd 70
userList 71
Web User Interface 72
Supported Web Browsers 72
Log On to the Web User Interface 72
Overview 72
URL address formats 73
First log on 73
Limited Status Access 73
Web User Interface Features 74
Tabs 74
Device status icons 74
Quick Links 75
About Home 76
The Overview view 76

Status Tab 77
About the Status Tab 77
View the Load Status and Peak Load 78
View the Network Status 78
Current IPv4 Settings 78
Current IPv6 Settings 78
Domain Name System Status 78
Ethernet Port Speed 78
Control 79
Controlling Device Outlets 80
To control the outlets on your device 80
Control actions you can select 80
Managing User Sessions 81
Resetting the Network Interface 81
Configuration 82
About the Configuration Tab 82
Configure Load Thresholds 82
To configure load thresholds 82
Configure Device Name and Location 82
Set the Coldstart Delay for the Device 83
Set the Overload Outlet Restrictions 83
To set Overload Outlet Restrictions: 83
Configure Phase Load Balance 83
Configure and Control Outlet Groups 84
Outlet group terminology 84
Purpose and benefits of outlet groups 84
System requirements for outlet groups 84
Rules for configuring outlet groups 85
Enable outlet groups 85
Create a local outlet group 86
Create a global outlet group 86
Edit or delete an outlet group 86
Typical outlet group configurations 87
Verify your setup and configuration for global outlet groups 88
Outlet Settings 89
Configure outlet settings and the outlet name 89
Schedule Outlet Actions 90
Actions you can schedule 90
Schedule an outlet event 90
Edit, disable, enable, or delete a scheduled outlet event 91
Outlet User Manager 91
Configure an outlet user 91

Security 92
Session Management screen 92
Ping Response 92
Local Users 92
Remote Users 94
Configure the RADIUS Server 95
Supported RADIUS servers 95
Firewall Menus 96
802.1X Security Configuration 98
Network Features 99
Protocol Configuration Summary 99
TCP/IP and Communication Settings 100
Port Speed 102
DNS 103
Web 104
Console 106
SNMP 107
SNMPv1 107
SNMPv3 108
FTP Server 109
Notifications 110
Event Actions 110
Configure event actions 110
E-mail notification screens 112
SNMP trap receiver screen 114
SNMP traps test screen 114
General Menu 115
Identification screen 115
Date/Time screen 115
Creating and importing settings with the config file 116
Configure Links 116
Logs in the Configuration Menu 117
Identifying Syslog servers 117
Syslog settings 117
Syslog test and format example 118
Tests Tab 119
Setting the Network Status LED to Blink 119
Logs Tab 120
Event, Data and Firewall Logs 120
Event log 120
Data log 122
Firewall Logs 124
Use FTP or SCP to retrieve log files 124
About Tab 126
About the Rack PDU 126
Support Screen 126

Device IP Configuration Wizard 127
Capabilities, Requirements, and Installation 127
How to use the Wizard to configure TCP/IP settings 127
System requirements 127
Installation 127
How to Export Configuration Settings 128
Retrieving and Exporting the .ini File 128
Summary of the procedure 128
Contents of the .ini file 128
Detailed procedures 129
The Upload Event and Error Messages 131
The event and its error messages 131
Messages in config.ini 131
Errors generated by overridden values 131
Related Topics 131
File Transfers 132
Upgrading Firmware 132
Benefits of upgrading firmware 132
Firmware module files (device) 132
Firmware File Transfer Methods 133
Using the Firmware Upgrade Utility 133
Use FTP or SCP to upgrade one Rack PDU 134
Use XMODEM to upgrade one device 135
How to upgrade multiple devices 135
Using the Firmware Upgrade Utility for multiple upgrades 136
Verifying Upgrades and Updates 137
Verify the success or failure of the transfer 137
Last Transfer Result codes 137
Verify the version numbers of installed firmware. 137
Troubleshooting 138
Access Problems 138
SNMP Issues 139
Source Code Copyright Notice 140

Introduction

Product Features

The AP7XXXB Series covered in this manual includes the following equipment:

AP78XXB Metered Rack PDU
AP79XXB Switched Rack PDU
AP71XXB In-Line Current Meter

NOTE: Depending on the features of your device, some of the information in this manual will not apply.

The APC by Schneider Electric Rack PDU and In-Line Current Meter provides real-time remote monitoring of connected loads. User-defined alarms warn of potential circuit overloads. The device provides full control over outlets through remote commands and user interface settings.

You can manage a Rack PDU or In-Line Current Meter through its Web User Interface (UI), its Command Line Interface (CLI), StruxureWare, 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**.) The devices have these additional features:

- Phase current, peak current
- 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, Outlet User, 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.
- Individual outlet control (AP79XXB Switched only).
- Configurable power delays (AP79XXB Switched only).
- 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.
- E-mail notifications for device and Network Management Card (NMC) system events.
- SNMP traps, Syslog messages, and e-mail notifications based on the severity level or category of the device and NMC system event.
- Security protocols for authentication and encryption.
- Cisco EnergyWise certified.

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

Types of User Accounts

The device has various levels of access (Super User, Administrator, Device User, Read-Only User, Outlet User, and Network-Only User), which are protected by user name and password requirements. Up to four users are allowed to login to the same device simultaneously (available in AOS version 6.1.3 or later).

NOTE: You will be prompted to enter a new password the first time you connect to the RPDU with the Super User account. The Administrator, Device User, Read-Only User, and Network-Only user accounts are disabled by default, and cannot be enabled until the Super User default password (`apc`) is changed.

- An **Administrator** or the **Super User** can use all of the menus in the UI and all of the commands in the CLI. Administrator user types can be deleted, but the **Super User** cannot be deleted. The default user name and password for the **Super User** are both **apc**.
  - The **Super User** or **Administrator** can manage another Administrator's account (enable, disable, change password, etc).
- A **Device User** has read and write access to device-related screens. Administrative functions like session management under the Security menu and Firewall under Logs appear grayed out.
- A **Read-Only User** has the following restricted access:
  - Access to the same menus as a Device User, but without the capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled. The event and data logs display no button to clear the log.
- An **Outlet User** has the following restricted access:
  - Access through the Web User Interface and Command Line Interface.
  - Access to the same menus as a Device User, but with limited capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but are disabled. The Outlet User has access to the **Outlet Control** menu option that allows the user to control only the outlets assigned by the Administrator. Outlet Users cannot clear the event or data logs. The **user name** and **password** are defined by the Administrator during the process of adding a new Outlet User.
- A **Network-Only User** (remote user) can only log on using the Web UI and CLI (Telnet or SSH). A user with network-only access has read/write permission to the network related menus only.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the device 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 device implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the device 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 device that discovers an active network interface connection at start-up.

Resetting the network timer

To ensure that the device does not restart if the network is quiet for 9.5 minutes, the device attempts to contact the default gateway every 4.5 minutes. If the gateway is present, it responds to the device 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 will restart the 9.5-minute time frequently enough to prevent the device from restarting.

EnergyWise

The device has the capability of becoming a Cisco EnergyWise Entity. This entity reports power usage and alarms in the EnergyWise Domain.

To exercise this capability, plug the device network port into a Cisco switch/router that supports the EnergyWise Domain. Log into the Web User Interface of the device and navigate to the **Configuration**/**RPDU**/**EnergyWise** web page. Click on the enable radio button to initiate the task. The task will generate unique parent and children names, default roles, keywords and importance values that comply with EnergyWise requirements. Customization of the aforementioned is supported by clicking on any of the underlined entities to navigate to a configuration web page.

The EnergyWise port, domain name and shared secret may also be modified, but must be coordinated with the same parameters in the Cisco gear.

The device implementation supports a single parent, multiple children hierarchy. The parent may exist as a standalone device. The parent usage reports the power consumed by the devices themselves. The children report either inlet power or, in the case of monitored outlets, the power consumed at the outlet. Both parent and children report a usage level (0-10 scale). The parent and inlet usage are always reported as 10 or “On”. In the case of switched outlets the actual state of the switch is reported and may also be altered by the Cisco device.

The remaining configurable items are string variables that may be modified as needed and are retained across power cycles or reboots.

For more information see: **www.cisco.com/en/us/products/ps10195/index.html**.

Getting Started

To start using the device:

1. Install the device using the *Installation Instructions* that were shipped with your product.
2. Apply power and connect to your network. Follow the directions in the *Installation Instructions*.
3. Establish network settings
4. Begin using the device by way of one of the following:
   - “Web User Interface” on page 72
   - “Command Line Interface” on page 10
   - “Device Display Panels” on page 7

Establish Network Settings

IPv4 initial setup

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

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

NOTE: Do **NOT** use the loopback address (127.0.0.1) as the default gateway. Doing so disables the Network Management Card. To enable 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, see.“DHCP response options” on page 101

IPv6 initial 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 manually, automatically, or using DHCP.

TCP/IP configuration methods

Use one of the following methods to define the TCP/IP settings needed by the device:

- “Device IP Configuration Wizard” on page 127
- “DHCP and BOOTP configuration”
- “Command Line Interface” on page 10

.ini file utility

You can use the .ini file export utility to export .ini file settings from configured units to one or more unconfigured units. For more information, see “Creating and importing settings with the config file” on page 116.

DHCP and BOOTP configuration

The default TCP/IP configuration setting, **DHCP**, assumes that a properly configured DHCP server is available to provide TCP/IP settings to Rack PDU. You can also configure the setting for BOOTP.

A user configuration (INI) file can function as a BOOTP or DHCP boot file. For more information, see “Creating and importing settings with the config file” on page 116.

If neither of these servers is available, see “Device IP Configuration Wizard” on page 127.

BOOTP: For the product to use a BOOTP server to configure its TCP/IP settings, it must find a properly configured RFC951-compliant BOOTP server.In the BOOTPTAB file of the BOOTP server, enter the product’s 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 product or on the Quality Assurance slip included in the package.

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

- If you specified a bootup file name, the unit attempts to transfer that file from the BOOTP server using TFTP or FTP. The unit 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 unit remotely through its “Web User Interface” on page 72 or “Command Line Interface” on page 10; the user name and password are both **apc**, by default. To create a bootup file, see your BOOTP server documentation.

DHCP: You can use an RFC2131/RFC2132-compliant DHCP server to configure the TCP/IP settings for your device. This section summarizes the unit's communication with a DHCP server. For more detail about how a DHCP server can configure the network settings for your device, see "DHCP response options" on page 101.

1. The device 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 device)
   - A User Class Identifier (by default, the identification of the application firmware installed on the device)
   - A Host Name (by default, apcXXYYZZ with XXYYZZ being the last six digits of the device SKU). 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 product needs for network communication. The DHCP offer also includes the Vendor Specific Information option (DHCP option 43). The product can be configured to ignore DHCP offers that do not encapsulate the APC cookie in DHCP option 43 using the following hexadecimal format. (The product does not require this cookie by default.)

   ```
   Option 43 = 01 04 31 41 50 43
   ```

   Where:
   - 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 User Interface, you can require the DHCP server to provide an "APC" cookie, which supplies information to the device.

Network Management with Other Applications

These applications and utilities work with a device (Rack PDU or In-Line Current Meter) which is connected to the network.

- PowerNet® Management Information Base (MIB) with a standard MIB browser — Perform SNMP SETs and GETs and use SNMP traps
- StruxureWare — Provide enterprise-level power management and management of agents, environmental monitors, and Rack PDUs or In-Line Current Meters.
- Device IP Configuration Utility — Configure the basic settings of one or more devices (Rack PDU or In-Line Current Meter) over the network, see "Device IP Configuration Utility"
- Security Wizard — Create components needed to help with security for the units when you are using Secure Sockets Layer (SSL/TLS) or Transport Layer Security (TLS) and related protocols and encryption routines.

Command Line Interface (CLI)

1. Log on to the CLI. See "Log on to the CLI" on page 10.
2. Contact your network administrator to obtain the IP address, subnet mask, and default gateway for the product.
3. Use these three commands to configure network settings. (Text in italics indicates a variable.)

   `tcpip -i` *`yourIPaddress`*

   `tcpip -s` *`yourSubnetMask`*
   `tcpip -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, type the following command and press ENTER:
   `tcpip -i 156.205.14.141`
4. Type `exit`. The unit restarts to apply the changes.

Recovering from a Lost Password

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

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the serial cable (Schneider Electric part number 940-0144A) to the selected port on the computer and to the Serial port on the device.
3. Run a terminal program (such as Tera Term® or HyperTerminal®) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   – The serial port is not in use by another application.
   – The terminal settings are correct as specified in step 3.
   – The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The Status LED will flash alternately orange and green within 5 to 7 seconds of pressing the **Reset** button. Press the **Reset** button a second time immediately when the LED begins flashing to reset the user name and password to their defaults temporarily.
6. Press ENTER, repeatedly if necessary, to display the **User Name** prompt again, then use the default, **apc,** for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is re-displayed, you must repeat step 5 and log on again.)
7. At the Command Line Interface, use the following commands to change the **Password** setting, which is **apc** at this stage:

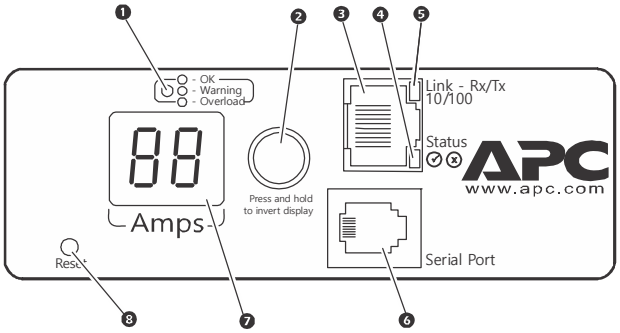
   ```
   user -n <user name> -pw <user password>
   ```

   For example, to change the **Super User** password to **XYZ** type:

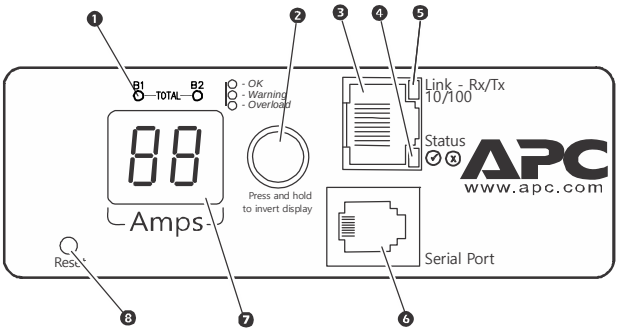
   ```
   user -n apc -cp apc -pw XYZ
   ```
8. Type `quit` or `exit` to log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Device Display Panels

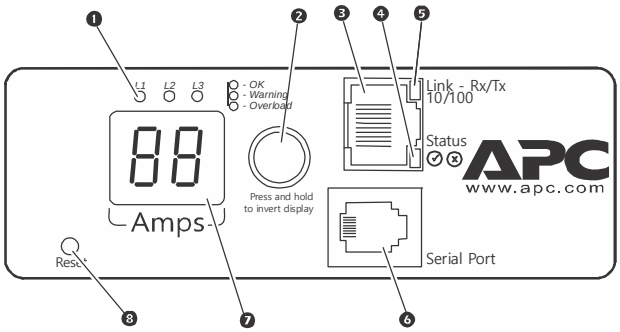
AP7152B
AP7155B
AP7800B
AP7801B
AP7820B
AP7821B
AP7900B
AP7901B
AP7920B
AP7921B



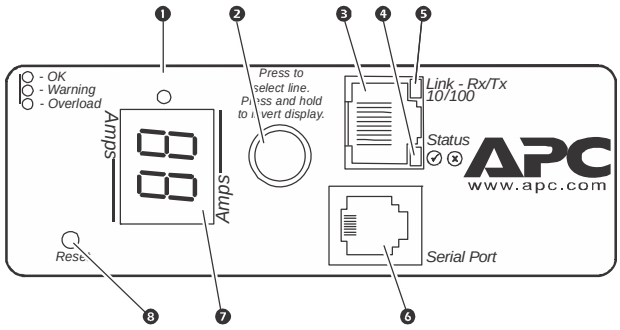
AP7802B
AP7811B
AP7822B
AP7822B
AP7902B
AP7902B
AP7911B
AP7922B



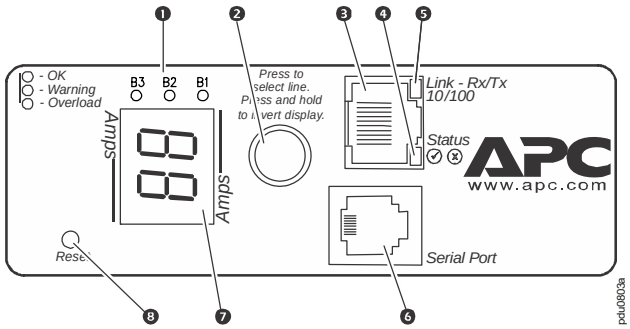
AP7175B



AP7850B
AP7950B



AP7869B
AP7899B
AP7968B
AP7998B



Display Panel Description

Item		Function
❶	Load Indicator LEDs	Indicates the status of the device load.
❷	Input Selector Main Menu button	On 3-phase models, press the input selector to monitor the current of the next phase or bank. For banked models, press the input selector to monitor the current of the next bank. For either 1- or 3-phase units, press and hold the input selector to display the IP address of the device or to invert the display. After five seconds, the IP address is displayed; after ten seconds, the displayed numbers invert. Press to view the device electrical input.
❸	10/100 Base-T Connector	Connects the device to the network.
❹	Network status LED	See “Network Status LED” on page 9.
❺	10/100 LED	See “10/100 LED” on page 9.
❻	RJ-12 Serial Port	Port for connecting the device to a terminal emulator program for local access to the Command Line Interface. Use the supplied serial cable (Schneider Electric part number 940-0144A).
❼	Display	Displays the current (amps) for the phase or bank indicated by the illuminated Load Indicator LED. On 3-phase models, the Digital Display will cycle through the phases or banks, displaying the current for each phase or bank for 3 seconds. If an internal communication failure occurs (for either a 1- or 3-phase model), the Digital Display displays Er, which you can clear by pressing the input selector.
❽	Reset button	Resets the management interface without affecting the outlet status.

Network Status LED

Condition	Description
Off	One of the following situations exists: • The device is not receiving input power. • The device is not operating properly. It may need to be repaired or replaced. Contact Customer Support.
Solid Green	The device has valid TCP/IP settings.
Solid Orange	A hardware failure has been detected in the device. Contact Customer Support.
Flashing Green	The device does not have valid TCP/IP settings.
Flashing Orange	The device is making BOOTP requests.
Alternately flashing green and orange	If the LED is flashing slowly, the device is making DHCP[2] requests[1]. If the LED is flashing rapidly, the device is starting up.
1. If you do not use a BOOTP or DHCP server, see “Establish Network Settings” on page 4 to configure the TCP/IP settings of the device. 2. To use a DHCP server, see “TCP/IP and Communication Settings” on page 100.	

10/100 LED

Condition	Description
Off	One or more of the following situations exists: • The device is not receiving input power. • The cable that connects the device to the network is disconnected or defective • The device that connects the device to the network is turned off. • The device itself is not operating properly. It may need to be repaired or replaced. Contact Customer Support.
Solid green	The device is connected to a network operating at 10 Megabits per second (Mbps).
Solid orange	The device is connected to a network operating at 100 Mbps.
Flashing green	The device is receiving or transmitting data packets at 10 Mbps.
Flashing orange	The device is receiving or transmitting data packets at 100 Mbps .

Load indicator LED

The load indicator LED identifies overload and warning conditions for the device.

Condition	Description
Solid Green	OK. No overload (critical) or near overload (warning) alarms are present.
Solid Yellow	Warning. At least one near overload warning alarm is present, but no overload critical alarms are present.
Flashing Red	Overload. At least one overload critical alarm is present.

Command Line Interface

About the Command Line Interface (CLI)

NOTE: Depending on the features of your device, some of the CLI commands will not apply.

You can use the Command Line Interface to view the status of and configure and manage the device. In addition, the Command Line Interface enables you to create scripts for automated operation. You can configure all parameters of a device (including those for which there are not specific CLI commands) by using the CLI to transfer an INI file to the device. The CLI uses XMODEM to perform the transfer, however, you cannot read the current INI file through XMODEM.

Log on to the CLI

To access the Command Line Interface, you can use either a local (serial) connection or a remote (Telnet or SSH) connection with a computer on the same network as the device.

Local access to the Command Line Interface

For local access, use a computer that connects to the device through the serial port to access the Command Line Interface:

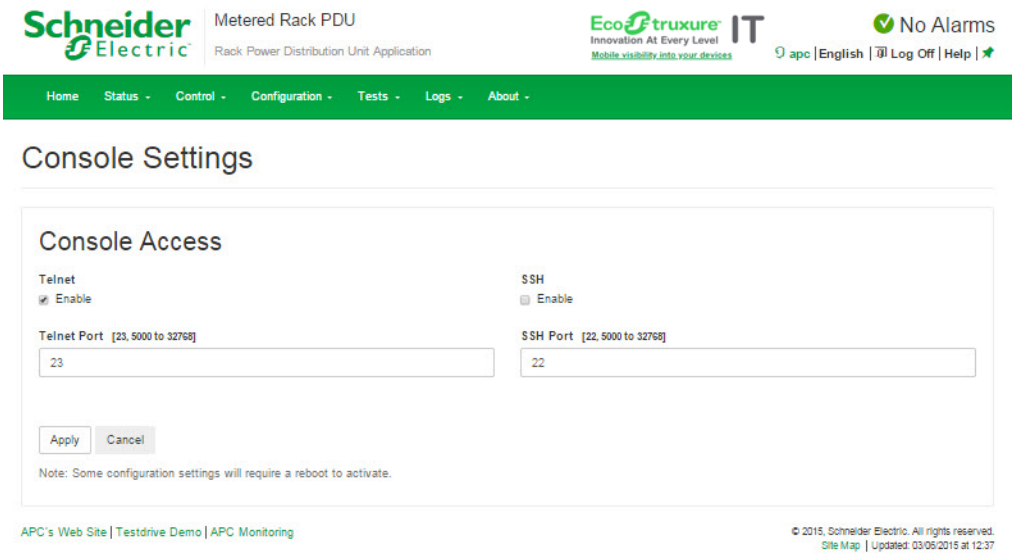
1. Select a serial port at the computer and disable any service that uses that port.
2. Connect the serial cable (Schneider Electric part number 940-0144A) from the selected serial port on the computer to the **Serial** port on the Rack PDU.
3. Run a terminal program (e.g., Tera Term or HyperTerminal) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

Press ENTER. It may take multiple (up to three) attempts to get a prompt to appear. At the prompt, enter your user name and password (by default, **apc** and **apc** for the **Super User**). If this is your first log on, you will be prompted to change the default password.

Remote access to the Command Line Interface

You can choose to access the Command Line Interface remotely through Telnet and/or SSH. SSH is enabled by default. You can use the `console` command (page 23) to enable or disable either Telnet or SSH.

If needed, you can also use the Web UI to enable or disable either Telnet or SSH. On the **Configuration** tab, select **Network** from the menu to open the **Console Access** page. Click to check the desired **Enable** box. Click **Apply** to save your changes or **Cancel** to leave the page



Telnet for basic access: Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption. Telnet is disabled by default.

To use Telnet to access the Command Line Interface:

1. From a computer that has access to the network on which the device is installed, at a command prompt, type `telnet` and the IP address for the device (for example, `telnet 139.225.6.133`, when the device uses the default Telnet port of 23), and press ENTER.

   If the device 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 usage: Some clients do not allow you to specify the port as an argument and some types of Linux might want extra commands).
2. Enter the user name and password (by default, **apc** and **apc** for the **Super User**).

   If you cannot remember your user name or password, see “Recovering from a Lost Password” on page 6.

SSH for high-security access: If you use the high security of SSL/TLS for the Web User Interface, use SSH for access to the Command Line Interface. SSH encrypts user names, passwords, and transmitted data. The interface, user accounts, and user access rights are the same whether you access the Command Line Interface through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer. SSH is enabled by default.

About the Main Screen

Following is an example of the main screen, which is displayed when you log on to the Command Line Interface of a device.

```
Schneider Electric                        Network Management Card AOS   vx.x.x
(c) Copyright 2019 All Rights Reserved    RPDU 2g APP                   vx.x.x
-------------------------------------------------------------------------------
Name       : Test Lab                                 Date      : 8/28/19
Contact    : Don Adams                                Time      : 5:58:30
Location   : Building 3                               User      : Administrator
Up Time    : 0 Days 21 Hours 21 Minutes               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)


apc>
```

- 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. In the example above, the application firmware for the device is displayed.

  ```
  Network Management Card AOS   vx.x.x
  RPDU 2g                       vx.x.x
  ```

- Three fields identify the system name, contact person, and location of the device.

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

- An **Up Time** field reports how long the 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: 8/28/19
  Time: 5:58:30
  ```

- The **User** field identifies whether you logged in through the **Super User**, **Administrator** or **Device Manager** 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 Schneider Electric Customer Care Center at **www.apc.com.**

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

Using the CLI

At the Command Line Interface, you can use commands to configure the device. To use a command, type the command and press ENTER. Commands and arguments are valid in lowercase, uppercase, or mixed case. Options are case-sensitive.

While using the Command Line Interface, you can also do the following:

- Type ? and press ENTER to view a list of available commands, based on your account type.
- To obtain information about the purpose and syntax of a specified command, type the command, a space, and ? or the word `help`. For example, to view RADIUS configuration options, type:

  `radius ?`

  or

  `radius help`
- Press the UP arrow key to view the command that was entered most recently in the session. Use the UP and DOWN arrow keys to scroll through a list of up to ten previous commands.
- Type at least one letter of a command and press the TAB key to scroll through a list of valid commands that match the text you typed in the command line.
- Type `exit` or `quit` to close the connection to the Command Line Interface.

Command Syntax

Item	Description
-	Options are preceded by a hyphen.
< >	Definitions of options are enclosed in angle brackets. For example: `-dp <device password>`
[]	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:

`ftp [-p <port number>] [-S <enable | disable>]`

In this example, the `ftp` command accepts the option `-p`, which defines the port number, and the option `-S`, which enables or disables the FTP feature.

To change the FTP port number to 5010, and enable FTP:

1. Type the ftp command, the port option, and the argument `5010`:
   `ftp -p 5010`
2. After the first command succeeds, type the ftp command, the enable/disable option, and the `enable` selection:
   `ftp -S enable`

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

`alarmcount -p [all | warning | critical]`

In this example, the option -p accepts only three arguments: all, warning, or critical. For example, to view the number of active critical alarms, type:

`alarmcount -p critical`

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:
The CLI reports all command operations with the following format:

```
E [0-9] [0-9] [0-9] : Error message
```

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.		

CLI Commands for Rack PDUs by SKU/type

❶ AP71XXB: InLine Current Meter

❷ AP78XXB: Metered Rack PDU (horizontal)

❸ AP79XXB: Switched Rack PDU (horizontal)

❹ AP88XX: Metered Rack PDU (vertical)
APF88XX Configurable Metered Rack PDU

❺ AP86XX: MBO with Switching (vertical)
APF86XX: Configurable MBO with Switching

❻ AP84XX: MBO Rack PDU (vertical)
APF84XX: Configurable MBO Rack PDU

❼ AP89XX: Switched Rack PDU
APF89XX: Configurable Switched Rack PDU

Command	Description	❶	❷	❸	❹	❺	❻	❼
alarmList	Display the alarms that are present on the device or another device in a Network Port Sharing group.	x	x	x	x	x	x	x
bkLowLoad	Set or read the bank low load threshold.		x	x	x	x	x	x
bkNearOver	Set or read the bank near overload threshold.		x	x	x	x	x	x
bkOverLoad	Set or read the bank overload threshold		x	x	x	x	x	x
bkPeakCurr	Read the bank peak current.		x	x	x	x	x	x
bkReading	Displays a reading/measurement from a bank(s).		x	x	x	x	x	x
bkRestrictn	Set or read the overload restriction feature to prevent outlets from turning on when the overload alarm threshold is violated.			x		x		x
devLowLoad	Set or read the device low load warning threshold.				x	x	x	x
devNearOver	Set or read the device near overload threshold.				x	x	x	x
devOverLoad	Set or read the device overload threshold.				x	x	x	x
devPeakLoad	Display the device peak load.				x	x	x	x
devReading	Displays the total power or energy the device is drawing.				x	x	x	x
devStartDly	Set or read the device cold start delay.			x		x		x
dispID	Set or read the Display ID.				x	x	x	x
energyWise	Configuration Options	x	x	x	x	x	x	x
humAlGen	Set or read whether humidity alarms are enabled or disabled.				x	x	x	x
humHyst	Set or read the humidity hysteresis value.				x	x	x	x
humLow	Set or read the low humidity threshold.				x	x	x	x
humMin	Set or read the minimum humidity threshold.				x	x	x	x
humReading	Display the humidity reading from the sensor.				x	x	x	x
lcd	Control the LCD Display.				x	x	x	x
lcdBlink	Blink the LCD Display.				x	x	x	x
logToFlash	Backup log files to USB flash.				x	x	x	x
olAssignUsr	Assign outlets to a user that exists in the local database.			x		x	x	x
olCancelCmd	Cancel all pending commands for an outlet or group of outlets.			x		x		x
olDlyOff	Turns off an outlet or group of outlets after power off delay.			x		x		x
olDlyOn	Turns on an outlet or group of outlets after power on delay.			x		x		x
olDlyReboot	Delayed Cycle power to an outlet or a group of outlets.			x		x		x
olGroups	List the outlet synchronization groups defined on the switched rack PDU.			x		x		x
olLowLoad	Set or view the outlet low-load threshold in kilowatts.					x	x	
olName	Set or display a name assigned to an outlet.			x		x	x	x

Command	Description	❶	❷	❸	❹	❺	❻	❼
olNearOver	Set or view the outlet near-overload threshold in kilowatts.					x	x	
olOff	Turn an outlet or group of outlets off.			x		x		x
olOffDelay	Set or read the power off delay time.			x		x		x
olOn	Turn an outlet or group of outlets on.			x		x		x
olOnDelay	Set or read the power on delay time.			x		x		x
olOverLoad	Set or view the outlet overload threshold in kilowatts.					x	x	
olPeakLoad	Display the peak current measurement from a bank(s).					x	x	
olRbootTime	Set or read the outlet reboot duration time.			x		x		x
olReading	Displays a reading/measurement from an outlet or a group of outlets.					x	x	
olReboot	Cycles power to an outlet or group of outlets.			x		x		x
olStatus	Display the status of selected outlets.			x		x		x
olType	Displays the type and rating of selected outlets.					x	x	x
olUnasgnUsr	Unassign outlets to a user that exists in the local database.			x		x	x	x
phBal	*Set or read the phase load balance threshold.			x		x	x	x
phBalAlGen	*Set or read whether phase load balance alarms are enabled or disabled.			x		x	x	x
phLowLoad	Set or read the phase low load threshold.	x	x	x	x	x	x	x
phNearOver	Set or read the phase near overload threshold.	x	x	x	x	x	x	x
phOverLoad	Set or read the phase overload threshold.	x	x	x	x	x	x	x
phPeakCurr	Read the peak current reading/measurement from a phase(s).	x	x	x	x	x	x	x
phReading	View the current, voltage, or power for a phase.	x	x	x	x	x	x	x
phRestrictn	Set or read the overload restriction feature to prevent outlets from turning on when the overload alarm threshold is violated.			x		x		x
phTophVolts	Read the phase-to-phase voltage on 3-phase devices.				x	x	x	x
prodInfo	Displays information about the rack PDU	x	x	x	x	x	x	x
sensorName	Set or display the name assigned to the temperature or temperature/ humidity sensor.				x	x	x	x
tempAlGen	Set or read whether temperature alarms are enabled or disabled.				x	x	x	x
tempHigh	Set or read the temperature high threshold.				x	x	x	x
tempMax	Set or read the temperature max threshold.				x	x	x	x
tempHyst	Set or read the temperature threshold hysteresis value.				x	x	x	x
tempPeak	Display the peak temperature reading of the sensor.				x	x	x	x
tempReading	Display the temperature reading from the sensor.				x	x	x	x
tempStatus	Display the status of the sensor.				x	x	x	x
userAdd	Add an outlet user to the local user database.			x		x	x	x
userDelete	Remove an outlet user from the local user database.			x		x	x	x
userList	List the users and outlets assigned to them.			x		x	x	x
userPasswd	Set a user password.			x		x	x	x

*Phase balance commands only applies to models with two or more metered phases.

Network Management Card Command Descriptions

? or help

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

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.

Parameters: `[<command>]`

Example 1:

```
apc> ?
System Commands:
-----------------------------------------------------------------------
 For command help: command ?

 ?          about      alarmcount  boot       bye        cd
 cipher     clrrst     console     date       delete     dir
 dns        eapos      email       eventlog   exit       firewall
 format     ftp        hhelp       lang       lastrst    ledblink
 pwd        quit       radius      reboot     resetToDef session
 smtp       snmp       snmptrap    snmpv3     system     tcpip
 tcpip6     user       userdflt    web        whoami     xferINI
 xferstatus
```

Example 2:

```
apc> help boot
Usage: boot -- Configuration Options
   boot  [-b <dhcpBootp | dhcp | bootp | manual>] (Boot Mode)
         [-a <remainDhcpBootp | gotoDhcpOrBootp>] (After IP
Assignment)
         [-o <stop | prevSettings>] (On Retry Fail)
         [-c <enable | disable>]    (Require DHCP Cookie)
         [-s <retry then stop #>]   (Note: 0 = never)
         [-f <retry then fail #>]   (Note: 0 = never)
         [-v <vendor class>]
         [-i <client id>]
         [-u <user class>]
```

Error Message: `E000, E102`

about

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

Description: Displays system information (Model Number, Serial Number, Manufacture Dates, etc.)

Parameters: None

Example: `apc> about`

```
E000: Success
Hardware Factory
---------------
Model Number:           AP7XXXB
Serial Number:          ST0913012345
Hardware Revision:      HW05
Manufacture Date:       1/4/2018
MAC Address:            00 05 A2 18 00 01
Management Uptime:      0 Days 1 Hour 42 Minutes
```

Error Message: `E000`

alarmcount

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

Description: Displays alarms present in the system.

Parameters:

Option	Argument	Description
`-p`	`all`	View the number of active alarms reported by the device. 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.

Example: To view all active warning alarms, type:

```
apc> alarmcount
E000: Success
AlarmCount: 0
```

Error Message: `E000, E102`

boot

Access: Super User, Administrator

Description: Allows the user to get/set the network startup configuration of the device, such as setting boot mode (DHCP vs BOOTP vs MANUAL).

Parameters:

Option	Argument	Description
`-b <boot mode>`	`dhcp | bootp | manual`	Define how the TCP/IP settings will be configured when the device turns on, resets, or restarts. See “TCP/IP and Communication Settings” on page 100 for information about each boot mode setting.
`-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.
`-v`	`[<vendor class>]`	Vendor Class is APC
`-i`	`[<client id>]`	The MAC address of the device’s NMC, Which uniquely identifies it on the network.
`-u`	`[<user class>]`	The name of the application firmware module.

Example: Using a DHCP server to obtain network settings:

```
apc> boot
E000: Success
Boot Mode:              manual
Non-Manual Mode Shared Settings
-------------------------------
Vendor class:           <device class>
Client id:              XX XX XX XX XX XX
User class:             <user class>
After IP assignment:    gotoDhcpOrBootp

DHCP Settings
-------------
Retry then stop:        4
DHCP cookie is:         enable

BOOTP Settings
--------------
Retry then fail:        never
On retry failure:       prevSettings
```

Error Message: `E000, E102`

cd

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

Description: Allows the user to set the working directory of the file system. The working directory is set back to the root directory ‘/’ when the user logs out of the CLI.

Parameters: `<dicrectory name>`

Example:

```
apc> cd logs
E000: Success

apc> cd /
E000: Success
```

Error Message: `E000, E102`

cipher

Access: Super User, Administrator

Description: Enable or disable cryptographic algorithms for Web UI sessions. You cannot enable or disable these algorithms directly from the Web UI. You must reboot your appliance after enabling or disabling algorithms for changes to take effect.

There are three categories of algorithms: Authentication algorithms, Block Cipher algorithms, and MAC algorithms. Available and Blocked Cipher Suites are also listed.

NOTE: Disabling the only algorithm will block all SSL/TLS sessions.

Parameters:

Option	Argument	Description
`-3des`	`<enable | disable>`	Triple-DES
`-aes`	`<enable | disable>`	AES
`-dh`	`<enable | disable>`	DH
`-rsake`	`<enable | disable>`	RSA Key Exchange
-rsaau	`<enable | disable>`	RSA Authentication
-sha1	`<enable | disable>`	SHA
-sha2	`<enable | disable>`	SHA256
-ecdhe	`<enable | disable>`	ECDHE

Example 1: Disable the triple-DES block cipher.

```
apc> cipher -3des disable
E002: Success
Reboot required for change to take effect.
```

Example 2: Retrieve a list of each available cryptographic algorithm and its status.

```
apc> cipher
E000: Success
Key Exchange Algorithms
-----------------------

         DH                    enabled
         RSA Key Exchange      enabled
         ECDHE                 enabled


Authentication Algorithms
-------------------------

         RSA Authentication    enabled

Cipher Algorithms
-----------------

         triple-DES            enabled
         AES                   enabled

MAC Algorithms
--------------
         SHA                   enabled
         SHA256                enabled

Available Cipher Suites
-----------------------

1        TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
2        TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
3        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
4        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
5        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
6        TLS_DHE_RSA_WITH_AES_128_CBC_SHA
7        TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
8        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
9        TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
10       SSL_RSA_WITH_3DES_EDE_CBC_SHA
11       TLS_RSA_WITH_AES_128_CBC_SHA
12       TLS_RSA_WITH_AES_256_CBC_SHA
13       TLS_RSA_WITH_AES_128_CBC_SHA256
14       TLS_RSA_WITH_AES_256_CBC_SHA256

Blocked Cipher Suites
---------------------
(the settings above disable the suites listed here)

None
```

Error Message: `E000, E102`

clrrst

Access: Super User, Administrator

Description: Clear 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 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> (ssh)`	Enable or Disable SSH access to the device. Enabling SSH enables SCP.
-t	`<enable | disable> (telnet)`	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 serial port connection (9600 bps by default).

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

```
console -S ssh
```

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

```
apc> console
E000: Success
Telnet:      enabled
SSH:         disabled
Telnet Port: 23
SSH Port:    22
Baud Rate:   9600
```

Error Message: `E000, E102`

date

Access: Super User, Administrator

Definition: Get and set the date and time of the system.

To configure an NTP server to define the date and time for the device, see “Date/Time screen” on page 115.

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 January 30, 2019, using the format configured in the preceding example, type:

```
date -d “2019-01-30”
```

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.

Parameters:

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

Example:

```
apc> delete /db/prefs.dat
E000: Success
```

Error Messages: `E000, E102`

dir

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

Description: Displays the content of the working directory.

Parameters: None

Example:

```
apc> dir
E000: Success
--wx-wx-wx  1 apc      apc      3145728 Jan 3  2019 aos.bin
--wx-wx-wx  1 apc      apc      3145728 Jan 4  2019 app.bin
-rw-rw-rw-  1 apc      apc        45000 Jan 6  2019 config.ini
drwxrwxrwx  1 apc      apc            0 Jan 3  2019 db/
drwxrwxrwx  1 apc      apc            0 Jan 3  2019 ssl/
drwxrwxrwx  1 apc      apc            0 Jan 3  2019 ssh/
drwxrwxrwx  1 apc      apc            0 Jan 3  2019 logs/
drwxrwxrwx  1 apc      apc            0 Jan 3  2019 sec/
drwxrwxrwx  1 apc      apc            0 Jan 3  2019 dbg/
drwxrwxrwx  1 apc      apc            0 Jan 3  2019 pdu/
```

Error Messages: `E000`

dns

Access: Super User, Administrator

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

Parameters:

Parameter	Argument	Description
`-OM`	`enable | disable`	Override the manual DNS.
`-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.
-y	`<enable | disable>`	System-hostname sync

Example:

```
apc> dns
E000: Success
Active Primary DNS Server:      x.x.x.x
Active Secondary DNS Server:    x.x.x.x

Override Manual DNS Settings:   enabled
Primary DNS Server:             x.x.x.x
Secondary DNS Server:           x.x.x.x
Domain Name:                    example.com
Domain Name IPv6:               example.com
System Name Sync:               Enabled
Host Name:                      ExampleHostName
```

Error Message: `E000, E102`

eapol

Access: Super User, Administrator, User

Description: Configure EAPoL (802.1X Security) settings.

Parameters:

Option	Argument	Definition
`-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 Name:NMC-Supplicant
  Passphrase:<hidden>
  CA file Status:Valid Certificate
  Private Key Status:Valid Certificate
  Public Key Status:Valid Certificate
  Result:Success
```

Example 2: To enable EAPoL:

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

Example 3: To change the supplicant name:

```
apc>eapol -n "NMC-Supplicant"
E000: Success
```

Example 4: To set the passphrase:

```
apc> eapol -p "client_password"
E000: Success
```

email

Access: Super User, Administrator

Description: View email

Parameters:

Parameters	Argument
-g[n]	<enable | disable> (Generation)
-t[n]	<To Address>
-o[n]	<long | short> (Format)
-l[n]	<Language Code>
-r [n]	<Local | recipient | custom> (Route)
Custom Route Option	
-f[n]	<From Address>
-s{n}	<SMTP Server>
-p[n]	<Port>
-a[n]	<enable | disable> (Authentication)
-u[n]	<User Name>
-w[n]	<Password>
-e[n]	<none | ifsupported | always | implicit> (Encryption)
-c[n]	<enable | disable > (Required Certificate)
-i[n]	<Certificate File Name>
n=	Email Recipient Number 1,2,3 or 4)

Example:

```
apc> email
E000: Success

  Recipient:    1
  Generation:   enabled
  Address:      example@example.com
  Format:       long
  Language:     enUs - English
  Route:        local
```

Error Message: E000, E102

eventlog

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

Description: View the date and time you retrieved the event log and the status of the device. 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: 01/06/2019 Time: 13:22:26
     ------------------------------------
     “Device Mame”: Communication Established
Date        Time      Event
     ---------------------------------------------------------------
     01/06/2019 13:17:22  System: Set Time.
     01/06/2019 13:16:57  System: Configuration change. Date format
                           preference.
     01/06/2019 13:16:49  System: Set Date.
     01/06/2019 13:16:35  System: Configuration change. Date format
                           preference.
     01/06/2019 13:16:08  System: Set Date.
     01/05/2019 13:15:30  System: Set Time.
     01/05/2019 13:15:00  System: Set Time.
     01/05/2019 13:13:58  System: Set Date.
     01/05/2019 13:12:22  System: Set Date.
     01/05/2019 13:12:08  System: Set Date.
     01/05/2019 13:11:41  System: Set Date.
<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

Error Message: `E000, E100`

exit, quit, or bye

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

Description: Exit from the CLI session. The exit, quit, and bye commands all close the CLI session.

Parameters: None

Example:

```
apc> exit
Bye
```

Error Message: None

firewall

Access: Super User, Administrator

Description: Establishes a barrier between a trusted, secure internal network and another network.

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	No argument. List only	Shows active file errors.
-te	No argument. List only	Shows test file errors.
-c	No argument.	Cancel a firewall test.
-r	No argument. List only	Shows active firewall rules.
-l	No argument. List only	Shows firewall activity log.
-Y	No argument.	Skip firewall test prompt.

Error Message: E000, E102

format

Access: Super User, Administrator

Description: Allows the user to format the FLASH file system. This will delete all configuration data (including network settings), event and data logs, certificates and keys, and reset the card to the factory defaults. See “resetToDef” on page 37.

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

Parameters: None

Example:

```
apc> format

Format FLASH file system

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

Enter 'YES' or ‘Y’ to continue or <ENTER> to cancel:
apc>
```

Error Message: None

ftp

Access: Super User, Administrator

Description: Get/set the ftp configuration data,
NOTE: The system will reboot if any configuration is changed.

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 device (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

apc> ftp
E000: Success
Service:        Enabled
Ftp Port:       5001

apc> ftp -p 21
E000: Success
```

Error Message: E000, E102

lang

Access: Super User, Administrator, Device User, Outlet 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: Last reset reason

Parameters: : None

Example:

```
apc> lastrst
00 Reset Cleared
E000: Success
```

Error Message: `E000, E102`

ledblink

Access: Super User, Administrator

Description: Sets the blink rate to the LED on the device.

Parameters: `<time>` = Number of minutes to blink the LED

Example:

```
apc> ledbllink 1
E000: Success
```

Error Message: `E000, E102`

logzip

Access: Super User, Administrator

Description: Places large logs into a zip file before sending.

Parameters:

```
[-m <email recipient>] (email recipient number (1-4))
```

Example:

```
apc> logzip
Generating files
Compressing files into /dbg/debug_ZA1023006009.tar
E000: Success
```

Error Message: `E000, E102`

netstat

Access: Super User, Administrator

Description: Displays incoming and outgoing network connections.

Parameters: None

Example: :

```
apc> netstat

Current IP Information:

Family   mHome   Type     IPAddress                      Status
IPv6     4       auto     FE80::2C0:B7FF:FE51:F304/64    configured
IPv6     0       manual   ::1/128                        configured
IPv4     0       manual   127.0.0.1/32                   configured
```

Error Message: `E000, E102`

ntp

Access: Super User, Administrator

Description: Synchronizes the time of a computer client or server.

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.

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

Description: Perform a network 'ping' to any external network device.

Parameters:

Argument	Description
`<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.

Example:

```
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

Description: Allows the user to get/set the network port speed.
NOTE: The system will reboot if any configuration is changed.

Parameters:

Option	Arguments	Description
`-s`	`auto | 10H | 10F | 100H | 100 F`	Define the communication speed of the Ethernet port. The `auto` command enables the Ethernet devices to negotiate to transmit at the highest possible speed. See "Port Speed" on page 102 for more information about the port speed settings.
`H = Half Duplex` `F = Full Duplex`		`10 = 10 Meg Bits` `100 = 100 Meg Bits`

Example:

```
apc> portspeed
E000: Success
Port Speed: 10 Half_Duplex

apc> portspeed -s 10h
E000: Success

apc> portspeed
E000: Success
Port Speed: 10 Half_Duplex

apc> portspeed -s auto
E000: Success
```

Error Message: `E000, E102`

prompt

Access: Super User, Administrator, Device User

Description: Allows the user to change the format of the prompt, either short or long.

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, Read Only

Description: Used to 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`

radius

Access: Super User, Administrator

Description: View the existing RADIUS settings, enable or disable RADIUS authentication, and configure basic authentication parameters for up to two RADIUS servers.

For a summary of RADIUS server configuration and a list of supported RADIUS servers, see “Configure the RADIUS Server” on page 95.
Additional authentication parameters for RADIUS servers are available at the Web User Interface of the device. See “RADIUS” on page 94 for more information.
For detailed information about configuring your RADIUS server, see the *Security Handbook*, available at www.apc.com.

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. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address. The device supports ports 1812, 5000 to 32768.
-s1 -s2	<server secret>	The shared secret between the primary or secondary RADIUS server and the device.
-t1 -t2	<server timeout>	The time in seconds that the device waits for a response from the primary or secondary RADIUS server.

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

Example 2: To enable RADIUS and local authentication, type:

```
apc> radius -a radiusLocal
E000: Success
```

Example 3: 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

Description: Restart the NMC interface of the device only. Forces the network device to reboot. User must confirm this operation by entering a “YES” or “Y” after the command has been entered.

Parameters: None

Example:

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

Error Message: `E000, E100`

resetToDef

Access: Super User, Administrator

Description: Reset all parameters to their default. Deletes all accounts and clears event and data logs. Resets all configuration changes, including event actions, device settings, and, optionally, TCP/IP configuration settings.

Parameters:

Option	Arguments	Description
`-p`	`all | keepip`	all = all configuration data, including the IP address. keepip = all configuration data, except the IP address. Reset all configuration changes, including event actions, device settings, and, optionally, TCP/IP configuration settings.

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

```
resetToDef -p keepip
Enter 'YES' or ‘Y’ to continue or <ENTER> to cancel : <user enters
‘YES’ or ‘Y’>
all User Names, Passwords.
Please wait...

Please reboot system for changes to take effect!
```

Error Message: `E000, E100`

session

Access: Super User, Administrator

Description: Records who is logged in, the serial, time and ID.

Parameters:

Option	Arguments
-d	[-d <session nID>] (Delete)
-M	<Enable | disable> (Multi-User Enable)
-a	<enable | disable (Remote Authentication Override)

Example:

```
apc>session
User          Interface     Address           Logged In Time    ID
-----------------------------------------------------------------------
apc           Web           x.x.x.x           00:00:08          156
apc           Telnet        x.x.x.x           00:00:02          157
E000: Success
```

Error Message: E000, E102

smtp

Access: Super User, Administrator

Description: Internet standard for electronic mail.

Parameters:

Option	Argument
-f	<From Address
-s	<SMTP Server>
-p	<Port> [1]
-a	<enable | disable> (Authentication)
-u	<User Name>
-w	<Password>
-e	<none | ifavail | always | implicit> (Encryption)
-c	<enable | disable> (Require Certificate)
-i	<Certificate File Name>
[1]Port options are 25, 465, 587, 2525, 5000 to 32768	

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

Description: Enable or disable SNMP v1.

Parameters:

Option	Arguments	Description
-c	<Community>	Identify the group of devices
-a	<read | write | writeplus | disable>	Set the access level
-n	<IP or Domain Name>	The host's name or address
-S	<enable | disable>	Enable or disable SNMPv1. SNMPv1 is disabled by default.

Example: To enable SNMP version 1, type:

```
apc> snmp
E000: Success
  SNMPv1:       enabled

Access Control summary:
Access Control #:        1
Community:               public
Access Type:             read
Address:                 0.0.0.0

Access Control #:        2
Community:               private
Access Type:             write +
Address:                 0.0.0.0

Access Control #:        3
Community:               public2
Access Type:             disabled
Address:                 0.0.0.0

Access Control #:        4
Community:               private2
Access Type:             disabled
Address:                 0.0.0.0
```

Error Message: E000, E102

snmpv3

Access: Super User, Administrator

Description: View the existing SNMPv3 settings, enable or disable SNMP, and configure basic SNMP parameters.

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>	User Name
`-a[n]`	`<Auth phrase>`	Authentication phrase of User profile
`-c[n]`	`<Crypt phrase>`	Crypt phrase of User profile
`-ap[n]`	`<sha | md5 | none>`	(Authentication Protocol)]
-pp[n]	<aes | des | none>	(Privacy Protocol)]
-ac[n]	<enable | disable>	(Access)
-au[n]	<User profile name>]	Access User Profile
`-n[n]`	`<IP or Domain Name>`	The host's name or address

[n] = Access Control # = 1,2,3, or 4)

Example:

```
apc> snmpv3
E000: Success
SNMPv3 Configuration
  SNMPV3:       disabled

SNMPv3 User Profiles

  Index:                1
  User Name:            apc snmp profile1
  Authentication:       None
  Encryption:           None

  Index:                2
  User Name:            apc snmp profile2
  Authentication:       None
  Encryption:           None

  Index:                3
  User Name:            apc snmp profile3
  Authentication:       None
  Encryption:           None
```

```
  Index:                4
  User Name:            apc snmp profile4
  Authentication:       None

  Encryption:           None

SNMPv3 Access Control

  Index:                1
  User Name:            apc snmp profile1
  Access:               disabled
  NMS IP/Host Name:     0.0.0.0

  Index:                2
  User Name:            apc snmp profile2
  Access:               disabled
  NMS IP/Host Name:     0.0.0.0

  Index:                3
  User Name:            apc snmp profile3
  Access:               disabled
  NMS IP/Host Name:     0.0.0.0

  Index:                4
  User Name:            apc snmp profile4
  Access:               disabled
  NMS IP/Host Name:     0.0.0.0
```

Error Message: E000, E102

snmptrap

Access: Super User, Administrator

Description: Enable or disable SNMP trap generation

Parameters:

Option	Arguments
-c{n}	<Community>
-r[n]	<Receiver NMS IP>
-l[n]	<Language> [language code]
-t[n]	<Trap Type> [snmpV1 | snmpV3]]
-g[n]	<Generation> [enable | disable]
-a[n]	<Auth Trap> [enable | disable]
-u[n]	<profile1 | profile2 | profile3 | profile4> (User Name)
n=Trap reciever # = 1,2,3,4,5 or 6	

Example:

```
apc> snmptrap
E000: Success

SNMP Trap Configuration

  Index:        1
  Receiver IP:  x.x.x.x
  Community:    public
  Trap Type:    SNMPV1
  Generation:   disabled
  Auth Traps:   enabled
  User Name:    apc snmp profile1
  Language:     enUs - English
```

Error Message: E000, E102

system

Access: Super User, Administrator

Description: View and set the system name, the contact, the location and 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” on page 12 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 and the device’s SNMP agent.
`-c`	`<system-contact>`	
`-l`	`<system-location>`	
-m	`<system-message>`	When defined, a custom message will appear on the log on screen for all users.
-s	`<enable | disable>] (system-hostname sync)`	Allow the host name to be synchronized with the system name so both fields automatically contain the same value. **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 view the device name, type:

```
apc> system -n
E000: Success
Name:    :  Rack 2 in Room #222
```

Error Message: `E000, E102`

tcpip

Access: Super User, Administrator

Description: View and manually configure these network settings for the device:

Parameters:

Option	Argument	Description
`-i`	`<IP address>`	Type the IP address of the device, using the format *xxx.xxx.xxx.xxx*
`-s`	`<subnet mask>`	Type the subnet mask for the device.
`-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 device will use.
-S	`enable | disable`	Enable or disable IPv4.

Example 1: To view the network settings of the device, type `tcpip` and press ENTER.

```
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 view the IP address of the device, type:

```
apc> tcpip -i
E000: Success
IP Address:     192.168.1.50
```

Example 3: To manually configure an IP address of `192.168.1.49` for the device, 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 and view and manually configure these network settings for the device:

Parameters:

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

Example: To view the network settings of the device, 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
```

Error Message: `E000, E102`

user

Access: Super User, Administrator

Description: Configure the user name, password, and inactivity timeout for each account type. You can't edit a user name, you must delete it and then create a new user. For information on the permissions granted to each account type, see "Types of User Accounts" on page 2.

Parameters:

Option	Argument	Description
-n	<user>	Specify these options for a user.
-pw	<user password>	
-pe	<user permission>	
-d	<user description>	
-e	enable | disable	Enable overall access.
-st	<session timeout>	Specify how long a session lasts waits before logging off a user when the keyboard is idle.
-sr	enable | disable	Bypass RADIUS by using the serial console (CLI) connection, also known as Serial Remote Authentication Override
-el	enable | disable	Indicate the Event Log color coding.
-lf	tab | csv	Indicate the format for exporting a log file.
-ts	us | metric	Indicate the temperature scale, Fahrenheit or Celsius.
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd>	Specify a date format.
-lg	<language code (e.g. enUs)>	Specify a user language.
-del	<user name>	Delete a user.
-l		Display the current user list.

Example:

```
apc> user -n apc
E000: Success
Access: Enabled
User Name: apc
Password: <hidden>
User Permission: Super User
User Description: User Description
Session Timeout: 3 minutes
Serial Remote Authentication Override: Disabled
Event Log Color Coding: Enabled
Export Log Format: Tab
Temperature Scale: Metric
Date Format: mm/dd/yyyy
Language: English (enUs)
Outlets: All
```

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> (Enable)	By default, user will be enabled or disabled upon creation. Remove (Enable) from the end
-pe	<Administrator | Device | Read-Only | Network-Only> (user permission)	Specify the user's permission level and account type.
-d	<user description>	Provide a user description.
-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
-sp	<enable | disable>	Strong password
-pp	<interval in days>	Required password change interval

Example:

```
apc> userdflt
E000: Success
Access: Disabled
User Permission: Administrator
User Description: User Description
Session Timeout: 3 minutes
Bad Login Attempts: 0
Event Log Color Coding: Enabled
Export Log Format: Tab
Temperature Scale: Metric
Date Format: mm/dd/yyyy
Language: English (enUs)
Strong Passwords: Disabled
Require Password Change: 0 day(s) (Disabled)
```

Error Message: E000, E102

web

Access: Super User, Administrator

Description: Enable access to the Web User Interface 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.
-ph	<http port #>	Specify the TCP/IP port used by HTTP to communicate with the device (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 device (443 by default). The other available range is 5000–32768.
-mp	<minimum protocol>	Choices are: SSL3.0 | TLS1.0 | TLS1.1 | TLS1.2

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

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

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

```
apc> web
E000: Success
HttP:              enabled
Https:             disabled
Http Port:         80
Https Port:        443
Minimum Protocol:  TLS1.1

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

Error Message: E000, E102

whoami

Access: Super User, Administrator, Device Only, Read Only

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 device, you must reset the baud rate to the default to reestablish communication with the device.

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. See “Verifying Upgrades and Updates” on page 137 for descriptions of the transfer result codes.

Parameters: None

Example:

```
apc> xferStatus
E000: Success
Result of last file transfer: Failure unknown
```

Error Message: `E000`

Device Command Descriptions

NOTE: Depending on the features of your device, some of the information in this manual will not apply.

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:

```
<all | bank#> [current]
```

`bank#` = A single number or 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 set the low-load threshold for all banks to 1A, type:

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

Example 2: To view the low-load threshold setting for banks 1 through 3, type:

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

Error Messages: `E000, E102`:

bkNearOver

Access: Super User, Administrator, Device User

Description: Set or view the bank near-overload 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:

```
<all | bank#> [current]
```

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

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

Example 2: To view the near-overload threshold setting for banks 1 through 3, type:

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

Error Messages: `E000, E102`:

bkOverLoad

Access: Super User, Administrator, Device User

Description: Set or view the bank overload 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:

```
<all | bank#> [current]
```

Example 1: To set the bank overload threshold for all banks to 13A, type:

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

Example 2: To view the bank overload threshold setting for banks 1 through 3, type:

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

Error Messages: `E000, E102`

bkPeakCurr

Access: Super User, Administrator, Device User

Description: Display the peak current measurement from a bank(s)

Parameters: : `<"all" | bank#>`

Example:

```
apc> bkPeakCurr 2
E000: Success
2: 0.0 A

apc> bkPeakCurr all
E000: Success
1: 0.0 A
2: 0.0 A
```

Error Messages: `E000, E102`

bkReading

Access: Super User, Administrator, Device User, Read Only

Description: View the current reading (measurement) in amps for a bank. You can specify all banks, a single bank, a range, or a comma-separated list of single banks and/or ranges.

Parameters:

```
<all | bank#> [current]
```

Example 1: To view the current reading for bank 3, type:

```
apc> bkReading 3
E000: Success
3: 4.2 A
```

Example 2: To view the current reading for all banks, type:

```
apc> bkReading all
E000: Success
1: 6.3 A
2: 5.1 A
3: 4.2 A
```

Error Messages: `E000, E102`

bkRestrictn

Access: Super User, Administrator, Device User

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

Parameters: : `<“all” | phase#> [<“none” | “near” | “over”>`

Acceptable arguments are `none`, `near`, and `over`.
To specify phases, choose from the following options.
Type: `all`, a single phase, a range, or a comma-separated list of phases.
`phase#` = A single number or a range of numbers separated with a dash or a comma separated list of single phase number and/or number ranges.

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

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

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

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

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: `[time | never]`

Argument	Definition
`[time	"never"]`	time = Cold start delay time in whole seconds or "never"; case insensitive.

Example 1: To view the cold start delay, type:

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

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

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

Error Messages: `E000, E102`

energyWise

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

Description: Cisco IOS® software for monitoring, controlling, and reporting the energy use of information technology (IT).

Parameters:

Option	Argument
-e	<enable | disable>] (Enable)
-p	<Port>
-d	<Domain>]
-m	<enable | disable>] (Secure Mode)
-s	<Shared Secret>
-v	(Toolkit Version)
-n	[outlet #] <Name>] (0 for Parent)
-r	[outlet #] <Role>] (0 for Parent)
-k	[outlet #] <Keywords>] (0 for Parent)
-i	[outlet #] <1-100>] (0 for Parent) (Importance)

Example:

```
Enable:                 Disabled
  Port:                   43440
  Domain Name:
  Secure Mode:            Shared Secret
  Shared Secret:          <hidden>
  Toolkit Version:        (rel2_7)1.2.0
  Name (P):               apc51F304
  Name (C1):              apc51F304.1.Outlet1
  Name (C2):              apc51F304.1.Outlet2
  Name (C3):              apc51F304.1.Outlet3
  Name (C4):              apc51F304.1.Outlet4
  Name (C5):              apc51F304.1.Outlet5
  Name (C6):              apc51F304.1.Outlet6
  Name (C7):              apc51F304.1.Outlet7
  Name (C8):              apc51F304.1.Outlet8
  Role (P):               Rack Power Distribution Unit
  Role (C1):              Outlet
  Role (C2):              Outlet
  Role (C3):              Outlet
  Role (C4):              Outlet
  Role (C5):              Outlet
  Role (C6):              Outlet
  Role (C7):              Outlet
  Role (C8):              Outlet
  Keywords (P):           apc,pdu,rackpdu
  Keywords (C1):          apc,pdu,rackpdu,outlet
  Keywords (C2):          apc,pdu,rackpdu,outlet
  Keywords (C3):          apc,pdu,rackpdu,outlet
  Keywords (C4):          apc,pdu,rackpdu,outlet
  Keywords (C5):          apc,pdu,rackpdu,outlet
  Keywords (C6):          apc,pdu,rackpdu,outlet
  Keywords (C7):          apc,pdu,rackpdu,outlet
  Keywords (C8):          apc,pdu,rackpdu,outlet
  Importance (P):         1
  Importance (C1):        1
  Importance (C2):        1
  Importance (C3):        1
  Importance (C4):        1
  Importance (C5):        1
  Importance (C6):        1
  Importance (C7):        1
  Importance (C8):        1
```

Error Message: None

olAssignUsr

Access: Super User, Administrator

Description: Assign control of outlets to an outlet user that exists in the local database.

Parameters: `<all | outlet name | outlet#> <user>`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.
`<user>`	A user that exists in the local database. (See “userAdd” on page 69.)

Example 1: To assign a user named Bobby to outlets 3, 5 through 7, and 10, type:

```
apc> olAssignUsr 3,5-7,10 bobby
E000: Success
```

Example 2: To assign a user named Billy to all outlets, type:

```
apc> olAssignUsr all billy
E000: Success
```

Error Message: `E000, E102`

olCancelCmd

Access: Super User, Administrator, Device User, and Outlet User, but only for outlets to which the user is assigned.

Description: Cancels all pending commands for an outlet or group of outlets.

Parameters: `<all | outlet name | outlet#>`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.

Example: To cancel all commands for outlet 3, type:

```
apc> olCancelCmd 3
E000: Success
```

Error Message: `E000, E102, E104`

olDlyOff

Access: Super User, Administrator, Device User, and Outlet User, but only for outlets to which the user is assigned.

Description: Turns off an outlet or group of outlets after the Power Off Delay (see “olOffDelay” on page 61).

Parameters: `<all | outlet name | outlet#>`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.

Example 1: To turn off outlets 3, 5 through 7, and 10, type:

```
apc> olDlyOff 3,5-7,10
E000: Success
```

Example 2: To turn off all outlets, type:

```
apc> olDlyOff all
E000: Success
```

Error Message: `E000, E102, E104`

olDlyOn

Access: Super User, Administrator, Device User, and Outlet User, but only for outlets to which the user is assigned.

Description: Turns on an outlet or group of outlets after the Power On Delay (see “olOnDelay” on page 62).

Parameters: `<all | outlet name | outlet#>`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.

Example 1: To turn on outlets 3, 5 through 7, and 10, type:

```
apc> olDlyOn 3,5-7,10
E000: Success
```

Example 2: To turn on an outlet with the configured name of Outlet1, type:

```
apc> olDlyOn outlet1
E000: Success
```

Error Message: `E000, E102, E104`

olDlyReboot

Access: Super User, Administrator, Device User, and Outlet User, but only for outlets to which the user is assigned.

Description: Cycles power to an outlet or a group of outlets. The specified outlets will be turned off based on the configured Power Off Delay (see “olOffDelay” on page 61). After the longest Reboot Duration (see “E000, E102, E104” on page 62) of the selected outlets, the outlets will then begin to turn on based on the configured Power On Delays (see “olOnDelay” on page 62) set for the specified outlets.

Parameters: `<all | outlet name | outlet#>`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.

Example 1: To cycle power to outlets 3, 5 through 7, and 10, type:

```
apc> olDlyReboot 3,5-7,10
E000: Success
```

Example 2: To cycle power to an outlet with the configured name of Outlet1, type:

```
apc> olDlyReboot outlet1
E000: Success
```

Error Message: `E000, E102, E104`

olGroups

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

Description: The device's CLI will not allow outlet synchronization groups to be assigned or managed, except via an INI file put/get. However, outlet group information can be retrieved using this command. Outlet synchronization groups can also be assigned and managed via the Web User Interface. An Outlet User can perform control commands on all outlets defined in an outlet synchronization group as long as one of the outlets has been assigned to them. Outlet synchronization can occur locally on one device or across the network with multiple devices depending on configuration. When an outlet is part of a synchronization group it will always be synchronized with the other members of the group.

Lists the outlet synchronization groups defined on the device. If synchronization of outlets between devices is enabled, information of those devices is also listed.

Parameters: `None`

Example: To list outlet synchronization groups on the device, type:

```
apc> olGroups
Outlet Group Method: Enabled via Network
Outlet Group A:
159.215.6.141Outlets: 2,4-7,9
159.215.6.143Outlets: 2,7,8
Outlet Group B:
159.215.6.141Outlets: 1
159.215.6.166Outlets: 1
E000: Success
```

Error Message: `E000, E102, E104`

olName

Access: Super User, Administrator, Device User, Read Only, and Outlet User, but only for outlets to which the user is assigned.

Description: Set or view the name configured for an outlet.

Parameters: `<all | outlet#> [newname]`

Argument	Definition
`all`	All device outlets.
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.
`<newname>`	The name for a specific outlet. Use only letters and numbers.

Example: To configure the name for outlet 3 to BobbysServer, type:

```
apc> olName 3 BobbysServer
E000: Success
```

Error Message: `E000, E102, E104`

olOff

Access: Super User, Administrator, Device User, and Outlet User, but only for outlets to which the user is assigned.

Description: Turn off an outlet or group of outlets without any delay.

Parameters: `<all | outlet name | outlet#>`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.

Example: To turn off outlets 3 and 5 through 7, type:

```
apc> olOff 3,5-7
E000: Success
```

Error Message: `E000, E102, E104`

olOn

Access: Super User, Administrator, Device User, and Outlet User, but only for outlets to which the user is assigned.

Description: Turn on an outlet or group of outlets without any delay.

Parameters: `<all | outlet name | outlet#>`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.

Example: To turn on outlets 3 and 5 through 7, type:

```
apc> olOn 3,5-7
E000: Success
```

Error Message: `E000, E102, E104`

olOffDelay

Access: Super User, Administrator, Device User, and Outlet User, but only for outlets to which the user is assigned.

Description: Set or view the time delay for the Off Delayed command (see “olDlyOff” on page 57) and for a Reboot Delayed command (see “olDlyReboot” on page 58).

Parameters: `<all | outlet name | outlet#> [time]`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.
`<time>`	A time for the delay within the range of 1 to 7200 seconds (2 hours).

Example 1: To set a 9-second delay for turning off outlets 3 and 5 through 7, type:

```
apc> olOffDelay 3,5-7 9
E000: Success
```

Example 2: To view the delay for the Off Delayed command for outlets 3 and 5 through 7, type:

```
apc> olOffDelay 3,5-7
E000: Success
3: BobbysServer: 9 sec
5: BillysServer: 9 sec
6: JoesServer: 9 sec
7: JacksServer: 9 sec
```

Error Message: `E000, E102, E104`

olOnDelay

Access: Super User, Administrator, Device User, and Outlet User, but only for outlets to which the user is assigned.

Description: Set or view the time delay for the On Delayed command (see “olDlyOn” on page 57) and for or a Reboot Delayed command (see “olDlyReboot” on page 58).

Parameters: `<all | outlet name | outlet#> [time]`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.
`<time>`	A time for the delay within the range of 1 to 7200 seconds (2 hours).

Example 1: To set a 6-second delay for turning on outlets 3 and 5 through 7, type:

```
apc> olOnDelay 3,5-7 6
E000: Success
```

Example 2: To view the delay for On Delayed command for outlets 3 and 5 through 7, type:

```
apc> olOnDelay 3,5-7
E000: Success
3: BobbysServer: 6 sec
5: BillysServer: 6 sec
6: JoesServer: 6 sec
7: JacksServer: 6 sec
```

Error Message: `E000, E102, E104`

olRbootTime

Access: : Super User, Administrator, Device User, and Outlet User, but only for outlets to which the user is assigned.

Description: Set or view the amount of time an outlet will remain off for a Reboot Delayed command (see “olDlyReboot” on page 58).

Parameters: `<all | outlet name | outlet#> [time]`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.
`<time>`	A time for the delay within the range of 1 to 7200 seconds (2 hours).

Example 1: To view the time set for outlets 3 and 5 through 7, type:

```
apc> olRbootTime 3,5-7
E000: Success
3: Bobby’s Server: 4 sec
5: Billy’s Server: 5 sec
6: Joe’s Server:   7 sec
7: Jack’s Server:  2 sec
```

Example 2: To set the time for outlets 3 and 5 through 7 to remain off during a reboot, type:

```
apc> olRbootTime 3,5-7 10
E000: Success
3: Bobby’s Server: 10 sec
5: Billy’s Server: 10 sec
6: Joe’s Server:   10 sec
7: Jack’s Server:  10 sec
```

Error Message: `E000, E102, E104`

olReboot

Access: Super User, Administrator, Device User, and Outlet User, but only for outlets to which the user is assigned.

Description: Cycle power to an outlet or group of outlets without any delays. If more than one outlet is specified, then those outlets will be cycled together.

Parameters: `<all | outlet name | outlet#>`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.

Example: To reboot outlets 3 and 5 through 7, type:

```
apc> olReboot 3,5-7
E000: Success
```

Error Message: `E000, E102, E104`

olStatus

Access: Super User, Administrator, Device User, and Read Only. Outlet Users also have access, but only for outlets to which the user is assigned.

Description: View the status of specified outlets.

Parameters: `<all | outlet name | outlet#>`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.

Example: To view the status for outlets 3 and 5 through 7, type:

```
apc> olStatus 3,5-7
E000: Success
3: BobbysServer: On
5: BillysServer: Off
6: JoesServer: Off
7: JacksServer: On
```

Error Messages: `E000, E102, E104`

olUnasgnUsr

Access: Super User, Administrator

Description: Unassign outlets to a user that exists in the local database. Outlet permissions for RADIUS defined users can only be set at the RADIUS server. This command is only available to the administrator. If an outlet is specified that is not assigned to a user, no error is generated.

Parameters: : `<all | outlet name | outlet#> <user>`

Argument	Definition
`all`	All device outlets.
`<outlet name>`	The name configured for a specific outlet. (See “olName” on page 60.)
`<outlet#>`	A single number or a range of numbers separated with a dash, or a comma-separated list of single outlet numbers and number ranges.
`<user>`	A user that exists in the local database.

Example 1: To remove a user named Bobby from control of outlets 3, 5 through 7, and 10, type:

```
apc> olUnasgnUsr 3,5-7,10 bobby
E000: Success
```

Example 2: To remove a user named Billy from control of all outlets, type:

```
apc> olUnasgnUsr all billy
E000: Success
```

Error Message: `E000, E102`

phBal

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

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

Parameters: `[id#:] [current]`= The new phase threshold (Amps).

Example:

```
apc> phBal 13
E000: Success

apc> phBal
E000: Success

13A
```

Error Message: `E000, E102`

phBalAlGen

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

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

Parameters: `[id#:] [<enable/disable>]`

`enable` = enable phase load balance alarms

`disable` = disable phase load balance alarms

Example 1:

```
apc> phBalAlGen enable
E000: Success

apc> phBalAlGen disable
E000: Success
```

Error Message: `E000, E102`

phLowLoad

Access: Super User, Administrator, Device User

Description: Set or view the phase low-load threshold. To specify phases, choose from the following options. Type: `all`, a single phase, a range, or a comma-separated list of phases.

Parameters: `<all | phase#> [current]`

`phase#` = A single number or a range of numbers separated with a dash or a comma; separated list of single bank number and/or number ranges.

`current` = The new phase threshold (Amps).

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

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

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

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

Error Message: `E000, E102`

phNearOver

Access: Super User, Administrator, Device User

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

Parameters: `<all | phase#> [current]`

`phase#` = A single number or a range of numbers separated with a dash or a comma; separated list of single bank number and/or number ranges.

`current` = The new phase threshold (Amps).

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

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

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

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

Error Message: `E000, E102`

phOverLoad

Access: Super User, Administrator, Device User

Description: Set or view the phase overload threshold.

Parameters: `<all | phase#> [current]`

`phase#` = A single number or a range of numbers separated with a dash or a comma; separated list of single bank number and/or number ranges.

`current` = The new phase threshold (Amps).

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

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

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

```
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 a phase(s).

Parameters: `<all | phase#>`

`phase#` = A single number or a range of numbers separated with a dash or a comma; separated list of single bank number and/or 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, Read Only

Description: View the current for a phase. You can specify all phases, a single phase, a range, or a comma-separated list of phases.

Parameters: `< all | phase# > < current >`

Example: To view the measurement for current for phase 3, type:

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

Error Message: `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. Acceptable arguments are `none`, `near`, and `over`. To specify phases, choose from the following options. Type: `all`, a single phase, a range, or a comma-separated list of phases.

Parameters: `< all | phase#> [none | near | over]`

`phase#` = A single number or a range of numbers separated with a dash or a comma; separated list of single bank number and/or number ranges.

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

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

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

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

Error Message: `E000, E102`

prodInfo

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

Description: View information about the device.

Parameters: `<all>`

Example: To view the product information for this device, type:

```
apc> prodInfo
E000: Success
AOS X.X.X
Metered Rack PDU  X.X.X
Model:            AP7XXXB
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 0 Hours 0 Minutes
Network Link:     Link Active
```

Error Messages: `E000`

userAdd

Access: Super User, Administrator

Description: Add an outlet user to the local user database.

The password for the new user will be the same as the user name. To change the password of the user, use the ‘`userPasswd`’ command.

Parameters: `<user>`

`user` = A user that does NOT exists in the local database.

Example: **:** To add a user named Bobby, type:

```
apc> userAdd Bobby
E000: Success
```

Error Message: `E000, E102, E202`

userDelete

Access: Super User, Administrator

Description: Remove an outlet user from the local user database.

Parameters: `<user>`

`user` = A user that exists in the local database.

Example: **:** To remove a user named Bobby, type:

```
apc> userDelete Bobby
E000: Success
```

Error Message: `E000, E102, E202`

userPasswd

Access: Super User, Administrator.

Description: Set an outlet User password.The administrator user can change passwords for all users.

Parameters: `<user> <password1> <password2>` = User name that will have its password changed. Password 2 is a confirmation and must be identical to password 1.

Example: To set dobby's password to "riddle" type:

```
apc> userPasswd dobby riddle riddle
E000: Success
```

Error Messages: `E000, E102, E104`

userList

Access: Super User, Administrator, Device User, Read Only, and Outlet User, but only for outlets to which the user is assigned.

Description: List the users and the outlets assigned to them.

When used by the administrator, it lists the users in the local database and the outlet numbers assigned to them. When used by an outlet user, it lists only that user and their outlets. If the active user was authenticated via RADIUS, then the user and the outlet permissions are displayed based on logged user type.

Parameters: None

Example 1: : When logged in as the Administrator, type:

```
apc> userList
E000: Success
Name                User Type           Status    Outlets
----                ---------           ------    -------
apc                 Super               ******    1-24
device              Device              Enabled   1-24
readonly            ReadOnly            Enabled   1-24
network             NetworkOnly         Enabled   1-24
dobby               Outlet              Enabled   1-12
```

Example 2: : If outlet user ‘dobby’ is logged in:

```
apc> userList
E000: Success
Name                User Type           Status    Outlets
----                ---------           ------    -------
dobby               Outlet              Enabled   1-12
```

Example 3: : If a radius outlet user ‘RadOutlet’ is logged in:

```
apc> userList
E000: Success
Name                User Type           Status    Outlets
----                ---------           ------    -------
RadOutlet           Outlet(Radius)     ******    1[1,3,5]
```

Example 4: : If a radius device user ‘RadDevice’ is logged in:

```
apc> userList
E000: Success
Name                User Type           Status    Outlets
----                ---------           ------    -------
raddev              Device(Radius)      ******    1-24
readonly            ReadOnly            Enabled   1-24
network             NetworkOnly         Enabled   1-24
dobby               Outlet              Enabled   1-12
```

Error Message: `E000`

Web User Interface

Supported Web Browsers

NOTE: Depending on the features of your device, some of the Web User Interface (Web UI) pages described will not apply.

You can use the latest version of Microsoft Internet Explorer® (IE) or Edge®, Google Chrome®, Apple Safari®, or Mozilla Firefox® to access the Rack PDU through its Web UI. Other commonly available browsers and versions may work but have not been fully tested.

The device cannot work with a proxy server. Before you can use a Web browser to access the Web User Interface of the device, you must do one of the following:

- Configure the Web browser to disable the use of a proxy server for the device.
- Configure the proxy server so that it does not proxy the specific IP address of the device.

Log On to the Web User Interface

Overview

You can use the DNS name or System IP address of the device for the URL address of the Web User Interface. Use your case-sensitive user name and password to log on.

The default user name and password for the **Super User** are both **apc**. For all other user types, there is no default user name or password. The **Super User** or an **Administrator** created by the **Super User**, must define the user name and password and other account characteristics for these users.

NOTE: If you are using HTTPS (SSL/TLS) as your access protocol, your login credentials are compared with information in a server certificate. If the certificate was created with the Security Wizard, and an IP address was specified as the common name in the certificate, you must use an IP address to log on to the device. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

You may receive a message that the Web page is not secure. This is normal, and you can continue to the Web UI. The warning is generated because your Web browser does not recognize the default certificate used for encryption over HTTPS. However, information transmitted over HTTPS is still encrypted. See the *Security Handbook* on **www.apc.com** for more details on HTTPS and instructions to resolve the warning.

URL address formats

Type the DNS name or IP address of the device in the Web browser's URL address field and press ENTER. 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

First log on

When you log on to the NMC 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 (e.g. enabled/disabled). You can access this screen at any time afterwards by following the path: **Configuration > Network > Summary**.

Limited Status Access

The RPDU Limited Status (**Configuration > Network > Web > Access**) page provides limited information, without requiring you to log on. Using a Web browser, access the RPDU'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. Clicking on "Limited Status," instead of the regular user name / password fields, a limited summary of Device and System Information is made available to viewing. A "Log On" hyper link, as seen immediately above, allows for easy access to the standard Log In page.

Web User Interface Features

Read the following to familiarize yourself with basic Web User Interface features for your device.

Tabs

The following tabs are available:

- **Home:** Appears when you log on (This is the default tab when you log on. To change the login page to a different page, click on the green pushpin at the top right side of the browser window while on the desired page). View active alarms, the load status of the device, and the most recent device events. For more information, see “About Home” on page 76.
- **Status:** Gives the user the status of the device and **Network**. The **RPDU** tab covers the status of alarms, groups, device, phase, bank, and environment. **Network** tab covers just the network. See “Status Tab” on page 77.
- **Control:** The **Control** tab covers three topics: **RPDU**, **Security** and **Network**. Much more information is covered under each of these tabs and will be described in the **Control** tab section.
- **Configuration**: The **Configuration** tab covers **RPDU**, **Security**, **Network**, **Notification**, **General** and **Logs**. Much more information is covered under each of these tabs and will be described in the **Configuration** tab section.
- **Tests:** The **Tests** tab covers **RPDU** and **Network**. The **Network** tab covers LED Blink. This will be further described later in the **Tests** section of the document.
- **Logs:** The **Logs** section covers: **Event**, **Data** and **Firewall**. The **Event** and **Data** tabs cover more information which will be further discussed later in the **Logs** section of the document.
- **About:** The **About** section covers **RPDU** and **Network**, which 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 device:

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

At the upper right corner of every page, the Web User Interface displays the same icons currently displayed on the **Home** page to report device status:

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

Quick Links

At the lower left on each page of the interface, there are three configurable links. By default, the links access the URLs for these Web pages:

- **Link 1**: The home page of the APC by Schneider Electric website
- **Link 2**: Demonstrations of APC by Schneider Electric web-enabled products
- **Link 3:** Information on **EcoStruxure IT**

Located in the upper right hand corner of each page:

- User name (click to change user preferences)
- Language (if available, click to change language preference)
- Log Off (click to log the current user off of the Web User Interface)
- Help (click to view help contents)
- (click to set the current web page to be the log in home page)
  Example:
  Log In Home: To make any screen the “home” screen (i.e., the screen that displays first when you log on), go to that screen, and click the icon in the top right corner.
  Click to revert to displaying the Home screen when you log on.

About Home

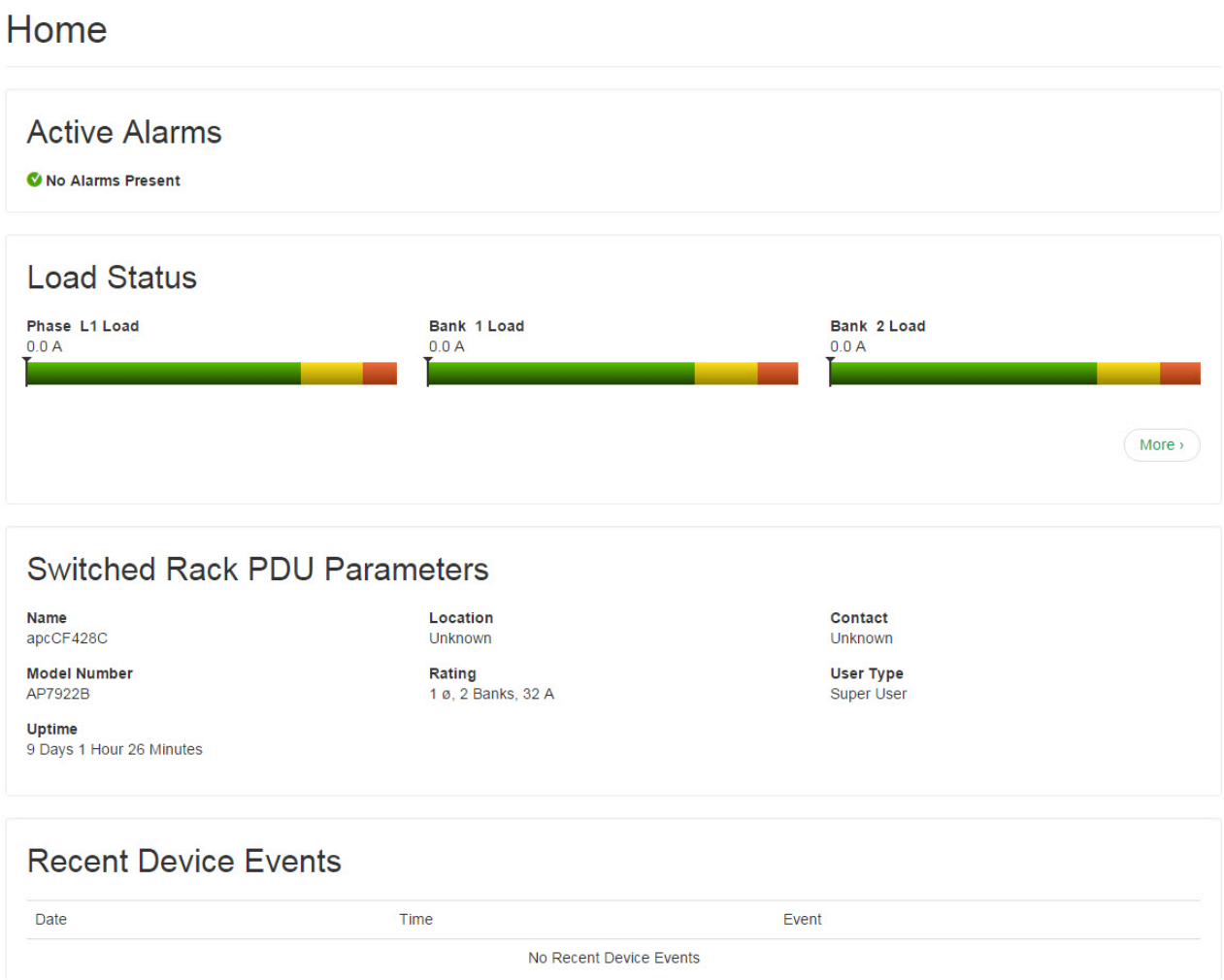
The **Home** page contains the following information: Active Alarms, Load Status and Recent Device Events. Active Alarms will show if any alarms exist. If no alarms exist, a green check mark with the words ”**No Alarms Present**” will show. The Load Status shows a colored bar demonstrating the level of the Bank, Phase and Device loads. To see the Device Status select the **More** link at the bottom of the list.The Recent Device Events box will list the five most recent device Events by the device by Date, Time and Event.

The Overview view

In the **Load Status** area, view the load for the phases and banks in amps, as applicable.

In the **Rack PDU Parameters** box, you will find the **Name**, **Location**, **Contact**, **Model Number**, **Rating**, **User** (type of user account accessing the device) and **Uptime** (the amount of time the device has been operating since the last reboot from either a power cycle or a reboot of the Management Interface).

In the **Recent Device Events** box are 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 go to the **Logs** tab to view the entire event log.

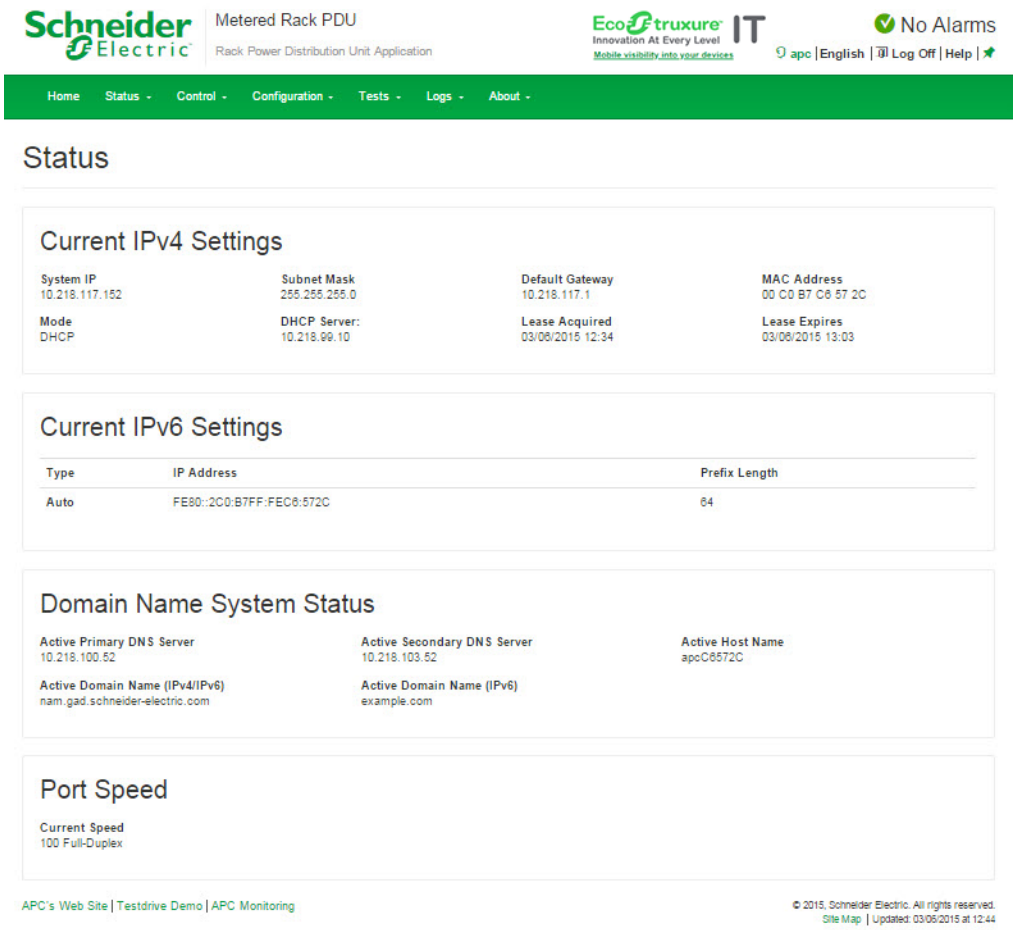


Status Tab

About the Status Tab

Use the **Status** tab to:

- View the status for the device or the network
- Under the device option, users can access the following: Alarms, Device, Phase, Bank, Outlets and Environment.
- Select Network to view the current IPv4 and IPv6 settings.



View the Load Status and Peak Load

Path: Status > RPDU

Alarms: Lists Device Alarm Status.

Device: Shows status of device. Lists Properties and Configuration information.

Phase: Shows phase status (only on units with this feature). 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.

Bank: Shows bank status (only on units with this feature). The bank settings can be changed via a Configure Bank status link at the bottom of the page.

Outlet: Shows: Outlet Name, Phase, and State.

Switched Outlet: Choose from the following options:

- **Scheduling:** Shows Scheduled outlet actions.
- **Outlet Groups:** Shows outlet groups as either enabled or disabled and can also configure.

View the Network Status

Path: Status > Network

The **Network** screen displays information about your network.

Current IPv4 Settings

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

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

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

Current Speed: The current speed assigned to the Ethernet port.

Control

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

Outlet Control

Control Action

No Action

Apply to Outlets

All Outlets

	#	State	Outlet Name	Phase	Bank
	1	On	Outlet 1	L1-N	1
	2	On	Outlet 2	L1-N	1
	3	On	Outlet 3	L1-N	1
	4	On	Outlet 4	L1-N	1
	5	On	Outlet 5	L1-N	1
	6	On	Outlet 6	L1-N	1
	7	On	Outlet 7	L1-N	1
	8	On	Outlet 8	L1-N	1
	9	On	Outlet 9	L1-N	2
	10	On	Outlet 10	L1-N	2
	11	On	Outlet 11	L1-N	2
	12	On	Outlet 12	L1-N	2
	13	On	Outlet 13	L1-N	2
	14	On	Outlet 14	L1-N	2
	15	On	Outlet 15	L1-N	2
	16	On	Outlet 16	L1-N	2

* Indicates a pending state change.

Next >> Cancel

Controlling Device Outlets

Path: Control > RPDU > Outlet

Shows Outlet Control, Control Action, and Selected Outlets. Inside the Select Outlet box the screen will show the Outlet's Name, its State and its Phase.

NOTE: If you apply an outlet control action to outlets or outlet groups, the following delays are used for the action:

- For an individual outlet (not in an outlet group), the action uses the delay periods and reboot duration configured for that outlet.
- For a global outlet group, the action uses the delay periods and reboot duration configured for the global outlet.
- For a local outlet group, the action uses the delay periods configured for the lowest-numbered outlet in the group.

To control the outlets on your device

Mark the checkboxes for each individual outlet or outlet group to control, or select the **All Outlets** checkbox.

Select a **Control Action** from the list, and click **Next >>**. On the confirmation page that explains the action, choose to apply or cancel it.

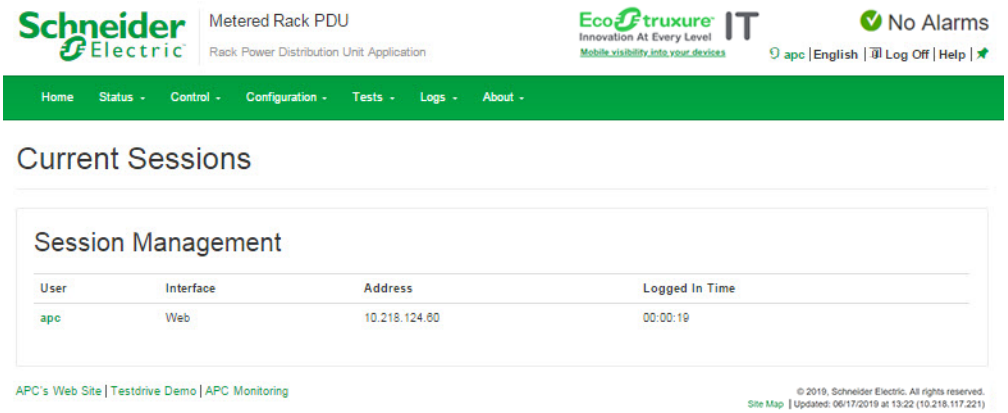
Control actions you can select

Option	Description
No Action	Do nothing.
On Immediate	Apply power to the selected outlets.
On Delayed	Apply power to each selected outlet according to its value for **Power On Delay**.†
Off Immediate	Remove power from the selected outlets.
Off Delayed	Remove power from each selected outlet according to its value for **Power Off Delay**.†
Reboot Immediate	Remove power from each selected outlet. Then apply power to each of these outlets according to its value for **Reboot Duration**.†
Reboot Delayed	Remove power from each selected outlet according to its value for **Power Off Delay**. Wait until all outlets are off (the highest value for **Reboot Duration**), and then apply power to each outlet according to its value for **Power On Delay**. †
Cancel Pending Commands	Cancel all commands pending for the selected outlets and keep them in the present state. **NOTE:** For global outlet groups, you can cancel a command only from the interface of the initiator outlet group. The action will cancel the command for the initiator outlet group and all follower outlet groups.
† If a local outlet group is selected, only the configured delays and reboot duration of the lowest-numbered outlet of the group are used. If a global outlet group is selected, only the configured delays and reboot duration of the global outlet are used.	

Managing User Sessions

Path: Control > Security > Session Management

The **Session Management** menu displays all active users currently connected to the Rack PDU. To view Information about a given user, click their user name. The **Session Details** screen displays 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.



Resetting the Network Interface

Path: Control > Network > Reset/Reboot

This menu gives you the option to reset and reboot various components of the network interface. Users have the option to **Reboot Management Interface**,

NOTE: Rebooting the Management Interface only restarts the device's Network Management Interface. It does not affect the outlet ON/OFF status.

Reset All: Clear the **Exclude TCP/IP** checkbox to reset all configuration values; mark the **Exclude TCP/IP** checkbox to reset all values except TCP/IP and EAPoL.

Reset Only: (Resetting may take up to a minute) Options include:

- **TCP/IP settings**: Set TCP/IP Configuration to **DHCP & BOOTP**, its default setting, request requiring that the device receive its TCP/IP settings from a DHCP or BOOTP server. See "View the result of the test DNS in the Last Query Response field." EAPoL is reset to disabled.
- **Event configuration**: Reset all changes to event configuration, by event and by group, to their default settings.
- **RPDU** to Defaults.

Configuration

About the Configuration Tab

Under the Configuration tab, several menu options are available to make changes to the devices:

- View the load status for the device
- Configure load thresholds for all connected phases and banks.
- Manage and control outlets
- Configure a name and location for the device
- View and manage the peak load measurement
- Click user-configurable links to open web pages for specific devices connected to the device

Configure Load Thresholds

Path: Configuration > RPDU

View the load for the phases and banks. The indicator in the green, yellow, and red meter shows the current load status: normal, near overload, or overload. If a low load threshold was configured, the meter will include a blue segment to the left of the green.

NOTE: The device generates an alarm when any bank exceeds its configured value. However, if a circuit breaker trips, there is no definitive indication that the circuit breaker is open, other than that the current for that bank will drop. Set the Low Load Warning to 1 amp for these reasons:

- The default setting for the Low Load Warning is 0 amps. This effectively disables the warning. With a setting of 0 amps for the Low Load Warning, the Web User Interface will not indicate that a circuit breaker may have tripped.
- A 1 amp detection threshold for the Low Load Warning for Bank Load Management will help to indicate that a circuit breaker may have tripped.

To configure load thresholds

1. To configure load thresholds for the device, phases, or banks, make a selection from the **Configuration > RPDU > Phase** and **Bank** drop-down menu. To configure load thresholds for outlets, click **Configuration** and then click an outlet.
2. Set Overload Alarm, Near Overload Warning, and Low Load Warning thresholds.
3. Click **Apply** to save your settings.

Configure Device Name and Location

Path: Configuration > RPDU > Device

The name and location you enter will appear on the **Home** tab.

1. Enter a name and location and contact.
2. Click **Apply** to save.

Set the Coldstart Delay for the Device

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 device. Allowed values are from 1 to 300 seconds, **Immediate**, or **Never** (never turn on).

1. Make a selection for **Coldstart Delay**.
2. Click **Apply**.

Set the Overload Outlet Restrictions

Path: Configuration > RPDU > Phase and **Bank**

Prevent users from applying power to outlets during an overload condition. You can set the following restrictions for each phase and bank:

- **None**: Users can apply power to outlets regardless of an Overload Alarm or Near Overload Warning.
- **On Warning**: Users cannot apply power to an outlet on the selected phase or bank if the current for that phase or bank has exceeded the Near Overload Warning threshold.
- **On Overload**: Users cannot apply power to an outlet on the selected phase or bank if the current for that phase or bank has exceeded the Overload Alarm threshold.

To set Overload Outlet Restrictions:

1. Click the **Configuration** tab, then **RPDU,** then **phase** or **bank** from the menu.
2. Make selections for **Overload Outlet Restriction**.
3. Click **Apply**.

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 RPDU will generate a Warning alarm if the phases are out of balance by more than the specified number of Amps.

Configure and Control Outlet Groups

Outlet group terminology

An *outlet group* consists of outlets that are logically linked together on the same device. Outlets that are in an outlet group turn on, turn off, and reboot in a synchronized manner:

- A *local outlet group* consists of two or more outlets on a device. Only the outlets in that group are synchronized.
- A *global outlet group* consists of one or more outlets on a device. One outlet is configured as a *global outlet*, which logically links the outlet group to outlet groups on up to three other devices. All outlets in the linked global outlet groups are synchronized.
  - For global outlet groups, the *initiator outlet group* is the group that issued the action.
  - For global outlet groups, a *follower outlet group* is any other outlet group that is synchronized with the initiator outlet group.

When you apply an outlet control action to outlets that are members of an outlet group, the outlets are synchronized as follows:

- For a global outlet group, use the delay periods and reboot duration configured for the global outlet of the initiator outlet group.
- For a local outlet group, the outlets use the delay periods and reboot duration of the lowest-numbered outlet in the group.

Purpose and benefits of outlet groups

By using groups of synchronized outlets on devices, you can ensure that outlets turn on, turn off, and reboot in a synchronized manner. Synchronizing control group actions through outlet groups provides the following benefits.

- Synchronized shutdown and startup of the power supplies of dual-corded servers prevents erroneous reporting of power supply failures during a planned system shutdown or reboot.
- Synchronizing outlets by using outlet groups provides more precise shutdown and restart timing than relying on the delay periods of individual outlets.
- A global outlet is visible to the user interface of any device to which it is linked.

System requirements for outlet groups

To set up and use synchronized outlet control groups:

- You need a computer that can initiate synchronized control operations through the Web User Interface or Command Line Interface of the devices or through SNMP.
- All of the Rack devices must use firmware that has the same version number for both APC by Schneider Electric's APC Operating System (AOS) module and the application module.
- All of the devices must be configured with the same "Member Name".
- If you are using Network mode, you will also need the following items.
  - You need a 10/100Base-T TCP/IP network, with an Ethernet hub or switch that has a power source not shared by the computers or other devices being synchronized.
  - All of the devices must be on the same subnet.
  - Outlet groups you synchronize must have the same Multicast IP address, outlet group port, authentication phrase, and encryption phrase. Make sure each Ethernet switch that connects devices allows Multicast network traffic for that Multicast IP address.

Rules for configuring outlet groups

For a system that uses outlet groups, the following rules apply:

- A device can have more than one outlet group, but an outlet can belong to only one outlet group.
- A local outlet group, which has no global outlet, must consist of two or more outlets.
- You can synchronize a global outlet group on one device with a global outlet group on each of three other devices.
  - In a global outlet group, you can designate only one outlet to be a global outlet, linking to outlet groups on other devices for the purpose of synchronization. That global outlet can be the only outlet in its group, or the group can consist of multiple outlets.
  - A global outlet of one outlet group must have the same physical outlet number as the global outlet of any other outlet group to which it links.
- To create and configure outlet groups, you must use the Web User Interface or export configuration file (.ini file) settings from a configured device. The Command Line Interface lets you display whether an outlet is a member of an outlet group and lets you apply control actions to an outlet group, but the Command Line Interface does not let you set up or configure an outlet group.

Enable outlet groups

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

Configure the following parameters, and click **Apply**.

Enable creation of outlet groups:

Parameters	Description
Device Level Outlet Group	To create an outlet group, you must enable the desired group method. Choices are: Disabled, Local Only, and Enabled via Network.

Enable support for global outlet groups (linked groups):

Parameters	Description
Member Name	To link outlet groups on multiple devices, you must define the same Member name on each of the devices. **NOTE:** A maximum of four devices can be configured with the same Member name

Setting parameters for outlet groups using Network mode:

Parameters	Description
Multicast IP	To link outlet groups on multiple devices, you must define the same Multicast IP address on each of the devices. **NOTE:** A maximum of four devices can be configured with the same Member name and Multicast IP address.
Authentication Phrase	A phrase of 15 to 32 ASCII characters that verifies that the device is communicating with other devices, that the message has not been changed during transmission, and that the message was communicated in a timely manner. The authentication phrase indicates that it was not delayed and that it was not copied and sent again later at an inappropriate time.
Encryption Phrase	A phrase of 15 to 32 ASCII characters that ensures the privacy of the data (by means of encryption).
Outlet Group Port	The port number on which the device will communicate with other devices. This must be the same on all devices in a group.

NOTE: Devices attempting to synchronize with Outlet Groups on other devices using network mode must all have the same Authentication Phrase and Encryption Phrase. The values are hidden to the user.

Create a local outlet group

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

1. Make sure outlet groups are enabled. (See “Typical outlet group configurations” on page 87.)
2. Click **Create Local Outlet Group**.
3. Select the checkboxes of the outlets that will be in the group and assign the group a name in the **Outlet Group Name** field. You must select at least two outlets.

Create a global outlet group

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

To set up multiple global outlet groups that link to outlet groups on other devices:

1. Make sure outlet groups are enabled. (See “Typical outlet group configurations” on page 87.)
2. Click **Create Global Outlet Groups**.
3. Select the checkboxes of the outlets that will be in the group and then click "**Apply and Select Global Outlets**" to select the global outlet for the group. If there is only one outlet in the group, it will automatically be assigned as the global outlet.
4. To add outlets to any of the global outlet groups you created, see “Edit or delete an outlet group”.

Edit or delete an outlet group

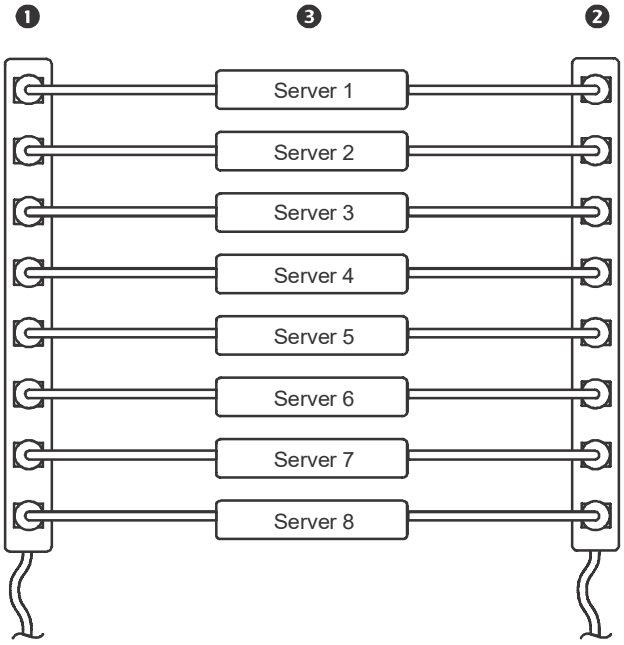
Path: Configuration > RPDU > Switched Outlet > Outlet Groups

1. In the **Configure Group** table, click on the number or name of the outlet group to edit or delete.
2. When editing an outlet group you can do any of the following:
   – Rename the outlet group.
   – Add or remove outlets by clicking the checkboxes to mark or unmark them.

   NOTE: You cannot remove an outlet from an outlet group that contains only two outlets unless the remaining outlet is a global outlet.
3. To delete the outlet group, click **Delete Outlet Group**.

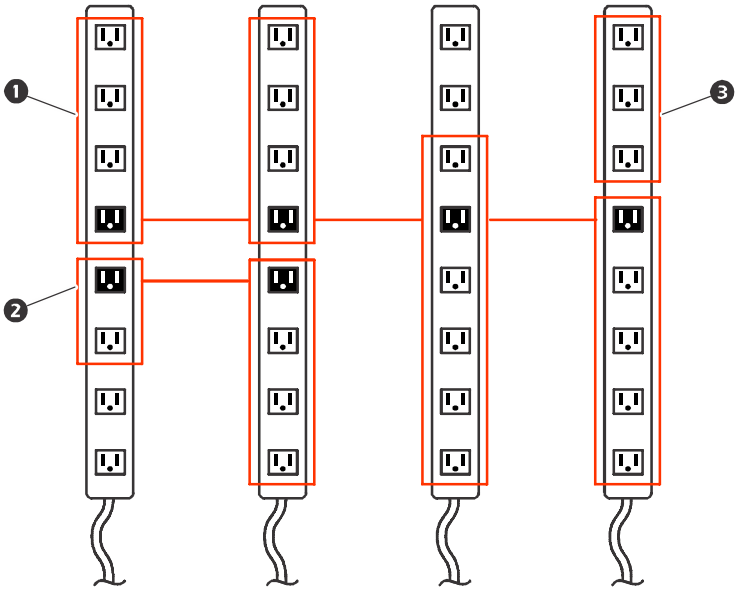
Typical outlet group configurations

The following configuration shows two devices, each with eight outlet groups. Each outlet group consists of a single global outlet. Each outlet group ❶ on the first device is linked to the outlet group ❷ in the same location on the second device. One power cord of a dual-corded server ❸ is connected to each outlet on the first device, and its other cord is connected to the corresponding outlet on the second device, ensuring that output power from both power sources to the server will turn On or Off in a synchronized manner in response to an outlet control action.



The following configuration shows three sets of synchronized outlets. Global outlets are shown in black. Outlet groups are enclosed in red rectangles.

❶	These four global outlet groups synchronize a total of 19 outlets.
❷	These two global outlet groups synchronize 6 outlets, 2 in one group and 4 in the other.
❸	This local outlet group synchronizes 3 outlets on the same device.



Verify your setup and configuration for global outlet groups

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

To ensure that your setup meets all system requirements for outlet groups and that you have configured the outlet groups correctly, view the groups and their connections:

- The **Configure Group** table displays the following:
  - All configured outlet groups on the current device.
  - The outlets in each group by outlet number.
  - Any outlet groups on other devices with which a global outlet group is synchronized. Each device is identified by its IP address if using network mode. Each global outlet is displayed in bold text.
- The **Global Outlet Overview** section displays the following:
  - The IP address of the current device.
  - The IP address of any devices that contain global outlets that are available to be synchronized with outlet groups on other devices.
  - All global outlets configured on the devices, regardless of whether they are synchronized with outlet groups on the current device.

Outlet Settings

Select From the options to control the outlets on your device.

Path: Configuration > RPDU > Switched Outlet (or Outlet Groups)

Configure outlet settings and the outlet name

The following settings are available:

Setting	Description
Name	Set the name for one or more outlets. The name is displayed next to the outlet number on status screens.
External Link	Define an HTTP or HTTPS link to a website or IP address. The external device web link can be set to the IP address of the external device plugged into the outlet (if applicable). Alternatively, it can be set to the device's manufacturer web page in order to more easily view user manuals, etc. Clicking the link on the Outlet Links page will open a new browser window to the link.
Power On Delay	Set the number of seconds that the device waits after a command is issued before applying power to an outlet. **NOTE:** To configure an outlet to remain off at all times, select the **Never** radio button next to **Power On Delay**.
Power Off Delay	Set the number of seconds that the device waits after a command is issued before removing power from an outlet. **NOTE:** To configure an outlet to remain on at all times, select the **Never** radio button next to **Power Off Delay**.
Reboot Duration	Set the number of seconds an outlet remains Off before restarting.

Path: Configuration > RPDU > Switched Outlet > Configuration

Click the **Configure Multiple Outlets** button in the **Outlet Configuration** section or click the outlet name.

- Configure outlet settings for multiple outlets:
  - Select the checkboxes next to the numbers of the outlets you want to modify, or select the **All Outlets** checkbox.
  - Enter values for **Name** and **Link**, and click the **Apply** button immediately below the list.
  - Enter values for **Power On Delay**, **Power Off Delay**, or **Reboot Duration**, and click the **Apply** button immediately below the list.
- Configure outlet settings for a single outlet:
  - Enter values for **Name** and **Link**, and click the **Apply** button immediately below the list.
  - Enter values for **Power On Delay**, **Power Off Delay**, or **Reboot Duration**, and click the **Apply** button immediately below the list.

Schedule Outlet Actions

Actions you can schedule

To configure values for **Power On Delay**, **Power Off Delay**, and **Reboot Duration** for each outlet, see “Configure outlet settings and the outlet name” on page 89. Although you must use the Web User Interface to schedule outlet actions, you can set these values in either the Web or Command Line Interfaces. For any outlets you select, you can schedule any of the actions listed in the following table to occur daily; at intervals of one, two, four, or eight weeks; or only once.

Option	Description
No Action	Do nothing.
On Immediate	Apply power to the selected outlets.
On Delayed	Apply power to each selected outlet according to its value for **Power On Delay**.†
Off Immediate	Remove power from the selected outlets.
Off Delayed	Remove power from each selected outlet according to its value for **Power Off Delay**.†
Reboot Immediate	Remove power from each selected outlet. Then apply power to each of these outlets according to its value for **Reboot Duration**.†
Reboot Delayed	Remove power from each selected outlet according to its value for **Power Off Delay**. Wait until all outlets are off (the highest value for **Reboot Duration**), and then apply power to each outlet according to its value for **Power On Delay**. †
† If a local outlet group is selected, only the configured delays and reboot duration of the lowest-numbered outlet of the group are used. If a global outlet group is selected, only the configured delays and reboot duration of the global outlet are used.	

Schedule an outlet event

Path: Configuration > RPDU > Switched Outlet > Scheduling

1. On the **Outlet Scheduling** page, select how often the event will occur (**One-Time**, **Daily**, or **Weekly**), and click the **Next** button.
   NOTE: If you select **Weekly**, you can choose to have the event occur once every week or once every two, four, or eight weeks.
2. On the **Schedule a Daily Action** page, in the **Name of event** text box, replace the default name, `Outlet Event`, with a name that will identify your new event.
3. Use the drop-down lists to select the type of event and when it will occur.
   The date format for one-time events is *mm/dd*, and the time format for all events is *hh/mm*, with the two-digit hour specified in 24-hour time.
   – An event that is scheduled daily or at one of the intervals available in the **Weekly** selection continues to occur at the scheduled interval until the event is deleted or disabled.
   – You can schedule a one-time event to occur only on a date within 12 months of the date on which you perform the scheduling. For example, on December 26, 2016, you could schedule a one-time event on any date from the current date until December 26, 2017.
4. Use the checkboxes to select which outlets will be affected by the action. You can select one or more individual outlets or **All Outlets**.
5. Click **Apply** to confirm the scheduling of the event, or **Cancel** to clear it.

When you confirm the event, the summary page is re-displayed, with the new event displayed in the list of scheduled events.

Edit, disable, enable, or delete a scheduled outlet event

Path: Configuration > RPDU > Switched Outlet > Scheduling

1. In the event list in the **Scheduled Outlet Action** section of the **Scheduling** page, click on the name of the event.
2. On the **Daily/Weekly scheduled action detail** page, you can do any of the following:
   - Change details of the event, such as the name of the event, when it is scheduled to occur, and which outlets are affected.
   - Under **Status of event** at the top of the page you can perform the following tasks:
     - Disable the event, leaving all its details configured so that it can be re-enabled later. A disabled event will not occur. An event is enabled by default when you create it.
     - Enable the event, if it was previously set to **Disable**.
     - Delete the event, removing the event completely from the system. A deleted event cannot be retrieved.

When you finish making changes on this page, click **Apply** to confirm the changes or **Cancel**.

Outlet User Manager

The Outlet User Management web page allows a user with administrative rights to view existing outlet user information and to add new users. Individual outlets can be assigned to each outlet user. When an outlet user logs into the device, he or she will only be able to view or control outlets that have been assigned to the outlet user.

To modify an existing outlet user's assigned outlets, click on the outlet listing under the desired device icon. To modify an existing outlet user's properties, click on the desired user name.

To create a new outlet user account, click the **Add User** button on the web page. This will take you to the new user configuration web page. Be sure to select **Outlet** in the **User Type** field. After filling out all of the fields, click **Next >>** to continue to the next page which allows you to select the desired outlets for the outlet user.

Configure an outlet user

Path: Configuration > RPDU > Outlet User

1. Click the **Add New User** button.
2. Type in the information for the following options and click **Apply** to confirm the changes.

Option	Description
User Name	Set the outlet user name. "New User" is reserved and is not allowed. **NOTE:** A user name in orange indicates the user account has been disabled.
Password	Set the outlet user password.
User Description	Set identification/description of outlet user.
Account Status	Enable, disable, or delete outlet user's account.
Device outlet access	Select the outlets the user can access.

Security

Session Management screen

Path: Configuration > Security > Session Management

Enabling **Allow Concurrent Logins** means that two or more users can log on at the same time. Each user has equal access and each interface (HTTP, FTP, telnet console, serial console (CLI), etc.) counts as a logged-in user.

Remote Authentication Override: The device supports Radius storage of passwords on a server. However, if you enable this override, the device will allow a local user to log on using the password for the device that is stored locally on the device. See also “Local Users” and “Remote Users authentication”.

Ping Response

Path: Configuration > Security > Ping Response

Select the Enable check box for **IPv4 Ping Response** to allow the device to respond to network pings. Clear the check box to disable an device response. This does not apply to IPv6.

Local Users

Use These menu options to view, and to set up access and individual preferences (like displayed date format), to the device user interfaces. This applies to users as defined by their logon name.

Path: Configuration > Security > Local Users > Management

Setting user access: With this option an Administrator or Super User can list and configure the users allowed access to the UI. The Super User user account always has access to the device.

Click on **Add User** to add a user. On the resulting **User Configuration** screen, you can add a user and withhold access by clearing the **Access** check box. User names and passwords are case-sensitive. The maximum length for both the name and password is 64 bytes, with less for multi-byte characters. You have to enter a password. Blank passwords, (passwords with no characters) are not allowed.

NOTE: Values greater than 64 bytes in Name and Password might get truncated. To change an Administrator/ Super User setting, you must enter all three password fields.

Use **Session Timeout** to configure the time (3 minutes by default) that the UI waits before logging off an inactive user. If you change this value, you must log off for the change to take effect.

NOTE: This timer continues to run if a user closes the browser window without first logging Off by clicking **Log Off** at the upper right.Because that user is still considered to be logged on, no user can log on until the time specified as **Minutes of Inactivity** expires. For example, with the default value for **Minutes of Inactivity**, if a user closes the browser window without logging off, no user can log on for 3 minutes.

Serial Remote Authentication Override: By selecting this option, you can bypass RADIUS by using the serial console (CLI) connection. This screen enables it for the selected user, but it must also be enabled globally to work, (through the “Session Management” screen).

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.

- Access: Put a check in the Enable box to allow access.
- User Type: Select the user type from the dropdown menu.
- User Description: Type the user Description in the box.
- Session Timeout: Select from 1 to 60 seconds.
- Bad Login Attempts. Set the number of failed login attempts the user can have. Select from 0 to 99 attempts. 0= unlimited.

User Preferences: This option is enabled by default.

- **Event Log Color Coding:** Mark the checkbox to enable color-coding of alarm text recorded in the event log. System event entries and configuration change entries do not change color.

Text Color	Alarm Severity
Red	**Critical**: A critical alarm exists, which requires immediate action.
Orange	**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	**Normal**: No alarms are present. The Rack PDU and all connected devices are operating normally.

- **Change the default temperature scale:** Select the temperature scale, **US Customary** (Fahrenheit) or **Metric** (Celsius), in which to display all temperature measurements in this user interface.
- **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.
- **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.
- **Language:** Select the user interface display languages from the drop-down box.

Password Requirements:

- **Strong Passwords:** Configure whether new passwords created for user accounts will require additional rules such as at least one lowercase character, one uppercase character, one number, and one symbol.
- **Password Policy:** Select the duration (in days) to which the user will be required to change their password. A value of 0 days disables this feature (by default).

Remote Users

Authentication : Specify how you want users to be authenticated at logon.

Path: Configuration > Security > Remote Users > Authentication

For information about local authentication (not using the centralized authentication of a RADIUS server), see the *Security Handbook,* available at **www.apc.com**.

The authentication and authorization functions of RADIUS (Remote Authentication Dial-In User Service) is supported.

- When a user accesses the Rack PDU or other network-enabled device that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the User permission level.
- RADIUS user names used with the Rack PDU are limited to 32 characters.

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 Command Line Interface 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**

RADIUS:

Path: Configuration > Security > Remote Users > RADIUS

Use this option to do the following:

- List the RADIUS servers (a maximum of two) available to the device and the time-out period for each.
- Click on a link, and configure the parameters for authentication by a new RADIUS server.
- Click a listed RADIUS server to display and modify its parameters.

RADIUS Setting	Definition
RADIUS Server	The server name or IP address (IPv4 or IPv6) of the RADIUS server. Click on a link to configure the server. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. The device supports ports 1812, 5000 to 32768.
Secret	The shared secret between the RADIUS server and the device.
Reply Timeout	The time in seconds that the device waits for a response from the RADIUS server.
Test Settings	Enter the 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)

Configure the RADIUS Server

Summary of the configuration procedure:

You must configure your RADIUS server to work with the device.

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 *Security Handbook*.

1. Add the IP address of the device 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 User Interface only).

   See your RADIUS server documentation for information about the RADIUS users file, and see the *Security Handbook* for an example.

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 the names for the ATTRIBUTE and VALUE keywords, but not for the 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`.

  ```
  DEFAULT      Auth-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`:

  ```
  bconners     Auth-Type = System
               APC-Service-Type = Admin
  thawk        Auth-Type = System
               APC-Service-Type = Device
  ```

Supported RADIUS servers

FreeRADIUS v 1.x and v 2.x, Microsoft Server 2008 and 2012 Network Policy Server (NPS) are supported. Other commonly available RADIUS applications may work but have not been fully tested.

Firewall Menus

Path: Configuration > Security > Firewall

Configuration: Enable or disable the firewall functionality. The configured policy is listed by default. Select the **Enable** checkbox to enable the firewall. The check box is un-checked 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: 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. (See Configuration above.)

Click **Cancel** to restore the original active policy and stay on the Active Policy page.

Active Rules: When a firewall is enabled, this read-only page lists the individual rules that are being enforced by a current active policy. See the **Create/Edit Policy** section for descriptions of the fields (Priority, Destination, Source, Protocol, Action, and Log).

Create/Edit Policy: Create a new policy; delete or edit an existing policy:

NOTE: While deleting an active enabled firewall policy cannot be done, editing a running policy can be done but 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 2 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 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" on page 124.

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

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

802.1X Security Configuration

Path: Configuration > Security > 802.1X Security

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.

The Web UI offers the following options for EAPoL configuration:

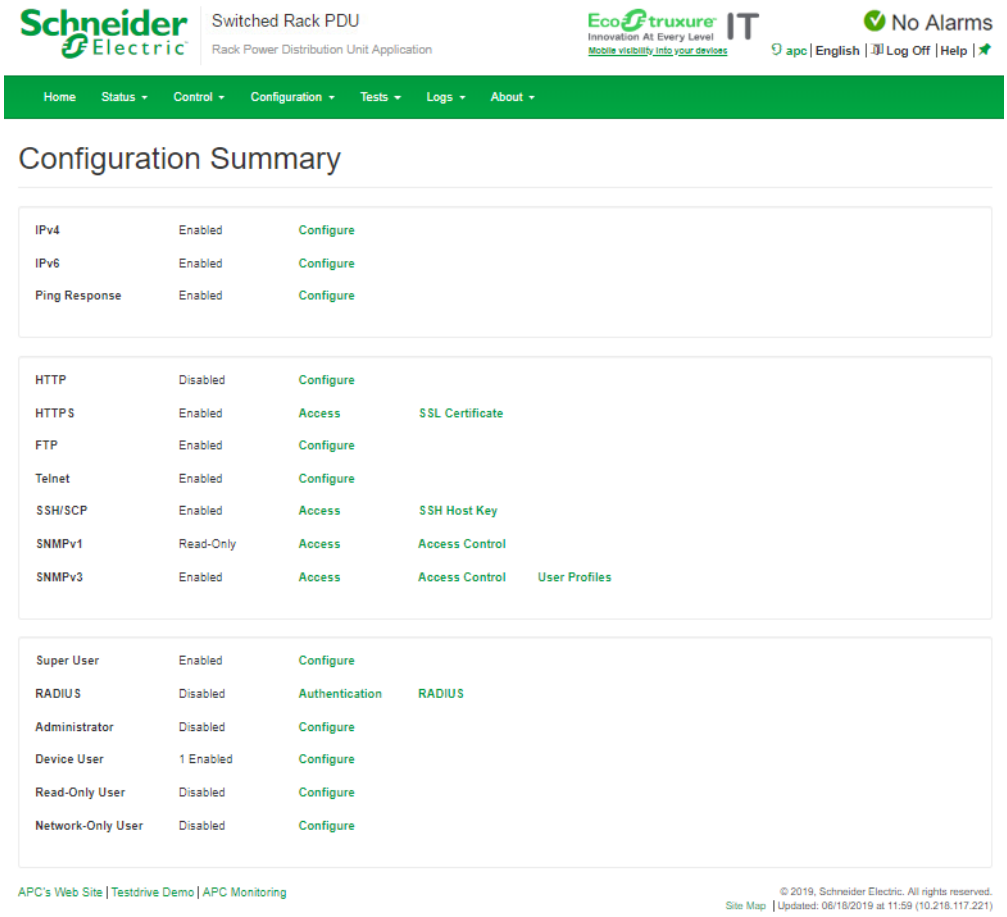
Setting	Description
EAPoL Access	Used to enable or disable 802.1X Security Access. **NOTE:** The 802.1X security access is disabled by default. The user can enable only when valid certificates and a valid passphrase for the private key are provided by the user.
Supplicant Identifier	Allows the users to set their own supplicant identifier (up to 32 characters including whitespace). **NOTE:** By default, the supplicant identifier is set to “NMC-Supplicant-xx:xx:xx:xx:xx:xx” where six octets of ‘xx’ are the MAC ID of the NMC.
CA Certificate	Upload/replace or remove 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.
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.

Network Features

Protocol Configuration Summary

Path: Configuration > Network > Summary

You can use this page to view all protocols enabled or disabled on your Rack PDU. Select a link for any protocol to go to the appropriate configuration page.



TCP/IP and Communication Settings

TCP/IP:

Path: Configuration > Network > TCP/IP

The **TCP/IP** option on the left navigation menu, selected by default when you choose **Network** on the top menu bar, displays the current IPv4 address, subnet mask, default gateway, MAC address, and boot mode of the device. For information on DHCP and DHCP options, see **RFC2131** and **RFC2132**.

Setting	Description
Enable	Enable or disable IPv4 with this check box.
Manual	Configure IPv4 manually by entering the IP address, subnet mask, and default gateway.
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the device requests network assignment from any BOOTP server: • If the device receives a valid response, it starts the network services. • If the device finds a BOOTP server, but a request to that server fails or times out, the device stops requesting network settings until it is restarted. • By default, if previously configured network settings exist, and the device receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible. Click **Next>>** to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail :[1] • **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	The default setting. At 32-second intervals, the device requests network assignment from any DHCP server. • If the device 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 device finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted.[1] • **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 device.

[1.] The default values for these three settings on the configuration pages generally do not need to be changed:
- **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 device needs to operate on a network, and other information that affects the operation of the device.

Vendor Specific Information (option 43): The device 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.

- **APC Cookie. Tag 1, Len 4, Data "1APC"**

Option 43 communicates to the device 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 device 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 device.
- **Subnet Mask** (option 1): The Subnet Mask value that the device needs to operate on the network.
- **Router,** i.e., Default Gateway (option 3): The default gateway address that the device needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the device.
- **Renewal Time, T1** (option 58): The time that the device 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 device 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): Up to two NTP servers (primary and secondary) that the device can use.
- **Time Offset** (option 2): The offset of the device's subnet, in seconds, from Coordinated Universal Time (UTC).
- **Domain Name Server** (option 6): Up to two Domain Name System (DNS) servers (primary and secondary) that the device can use.
- **Host Name** (option 12): The host name that the device will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the device 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 device will download the .ini file. After the download, the .ini file is used as a boot file to reconfigure the settings.

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

Setting	Description
Enable	Enable or disable IPv6 with this check box.
Manual	Configure IPv6 manually by entering the IP address and the default gateway.
Auto Configuration	When the Auto Configuration 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	**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 device checks whether the M or the O flag is set. The device interprets the state of the M (Managed Address Configuration Flag) and O (Other Stateful Configuration Flag) "bits" for the following cases: • *Neither is set*: Indicates the local network has no DHCPv6 infrastructure. The device uses router advertisements and manual configuration to get addresses that are not link-local and other settings. • *M, or M and O are set*: In this situation, full DHCPv6 address configuration occurs. DHCPv6 is used to obtain addresses AND other configuration settings. This is known as `DHCPv6 stateful`. 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. If an O flag is received first, then an M flag is received subsequently, the device performs full address configuration upon receipt of the M flag • *Only O is set*: 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 `DHCPv6 stateless`. **Address and Other Information:** With this radio box selected, DHCPv6 is used to obtain addresses AND other configuration settings. This is known as `DHCPv6 stateful`. **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 `DHCPv6 stateless`. **Never**: Select this to disable DHCPv6.

Port Speed

Path: Configuration > Network > Port Speed

The **Port Speed** setting defines the communication speed of the TCP/IP port.

- For **Auto-negotiation** (the default), 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.
- Alternatively, you can choose 10 Mbps or 100 Mbps, each with the option of half-duplex (communication in only one direction at a time) or full-duplex (communication in both directions on the same channel simultaneously).

DNS

Path: Configuration > Network > DNS > Configuration

Use the options under **Configuration** to configure and test the Domain Name System (DNS):

- **Override Manual DNS Settings:** Selection of Override Manual DNS Settings will result in configuration data from other sources (typically DHCP) taking precedence over the manual configurations set here.
- Select **Primary DNS Server** or **Secondary DNS Server** to specify the IPv4 or IPv6 addresses of the primary and optional secondary DNS server. For the device to send e-mail, you must at least define the IP address of the primary DNS server.
  - The device waits up to 15 seconds for a response from the primary DNS server or secondary DNS server (if specified). If the device does not receive a response within that time, e-mail cannot be sent. Use DNS servers on the same segment as the device 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:** Allow the system name to be synchronized with the host name so both fields automatically contain the same value.
  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).
- **Host Name**: Configure a host name here and a domain name in the **Domain Name** field then users can enter a host name in any field in the device interface (except e-mail addresses) that accepts a domain name.
- **Domain Name (IPv4/IPv6)**: Configure the domain name here only. In all other fields in the device interface (except e-mail addresses) that accept domain names, the device adds this domain name when only a host name is entered.
  - 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, `somedomain.com`, or to `0.0.0.0`.
  - To override the expansion of a specific host name entry, include a trailing period. The device recognizes a host name with a trailing period (such as *`mySnmpServer.`*) as if it were a fully-qualified domain name and does not append the domain name.
- **Domain Name (IPv6)**: Specify the IPv6 domain name here.

Test:

Path: Configuration > Network > DNS > Test

Use this option to send a DNS query that tests the setup of your DNS servers by looking up the IP address. View the result of a test in the **Last Query Response** field.

- Select **test** to send a DNS query that tests the setup of your DNS servers:
  - As **Query Question**, identify the value to be used for the selected query type:

Query Type Selected	Query Question to Use
by Host	The URL
by FQDN	The fully qualified domain name, *`my_server.my_domain`*
by IP	The IP address
by MX	The Mail Exchange address

Web

Path: Configuration > Network > Web

Option	Description

access	To activate changes to any of these selections, log off from the device:
	• **Disable**: Disables access to the Web User Interface. (To re-enable access, log in to the Command Line Interface, then type the command `http -S enable`. For HTTPS access, type `https -S enable`.)
	• **Enable HTTP** (the default): Enables 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.
	• **Enable HTTPS**: Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer/Transport Layer Security (SSL/TLS). SSL/TLS encrypts user names, passwords, and data during transmission, and authenticates the device by digital certificate. When HTTPS is enabled, your browser displays a small lock icon. HTTPS is enabled by default.
	See "Creating and Installing Digital Certificates" in the *Security Handbook*, available at **www.apc.com**.
	HTTP Port: The TCP/IP port (80 by default) used to communicate by HTTP with the device.
	HTTPS Port: The TCP/IP port (443 by default) used to communicate by HTTPS with the device.
	For either of these ports, you can change the port setting to any unused port from 5000 to 32768 for additional security. 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:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`
	Minimum Protocol: Choose from the drop down menu - SSL 3.0, TLS 1.0, TLS 1.1, or TLS 1.2
	Require Authentication Cookie: Click to put a check the **Enable** box.
	Limited Status Access: Click to put a check in the box before **Enable** or **Use as a default page**.

Option	Description
ssl certificate	Add, replace, or remove a security certificate. **Status**: • **Not installed**: A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Using **Add or Replace Certificate File** installs the certificate to the correct location, **/ssl** on the device. • **Generating**: The device is generating a certificate because no valid certificate was found. • **Loading**: A certificate is being activated on the device. • **Valid certificate**: A valid certificate was installed or was generated by the device. Click on this link to view the contents of the certificate. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL/TLS, the device generates a default certificate, a process which delays access to the interface for up to one minute.** You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on. **Add or Replace Certificate File**: Enter or browse to the certificate file created with the Security Wizard. See “Creating and Installing Digital Certificates” in the *Security Handbook,* available at **www.apc.com**, to choose a method for using digital certificates created by the Security Wizard or generated by the device. **Remove**: Delete the current certificate.

Console

Path: Configuration > Network > Console > *options*

Option	Description

access	• **Disable**: Disables all access to the Command Line Interface.
	• **Enable Telnet** (the default): Telnet transmits user names, passwords, and data without encryption. Telnet is disabled by default.
	• **Enable SSH**: SSH transmits user names, passwords, and data in encrypted form, providing protection from attempts to intercept, forge, or alter data during transmission. SSH is enabled by default
	Configure the ports to be used by these protocols:
	• **Telnet Port**: The Telnet port used to communicate with the device (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 device (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.

ssh host key	**Status** indicates the status of the host key (private key): • **SSH Disabled: No host key in use:** When disabled, SSH cannot use a host key. • **Generating**: The device is creating a host key because no valid host key was found. • **Loading**: A host key is being activated on the device. • **Valid**: One of the following valid host keys is in the **/ssh** directory (the required location on the device): • A 1024-bit or 2048-bit host key created by the Security Wizard • A 2048-bit RSA host key generated by the device **Add or Replace**: Browse to and upload a host key file created by the Security Wizard. To use the Security Wizard, see the *Security Handbook, available* at www.apc.com. **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 device takes up to one minute to create a host key, and the SSH server is not accessible during that time.** **Remove**: Remove the current host key.

NOTE: To use SSH, you must have an SSH client installed. Most Linux and other UNIX platforms include an SSH client, but Microsoft Windows operating systems do not. Clients are available from various vendors.

SNMP

All user names, 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 StruxureWare to manage a device on the public network, you must have SNMP enabled in the device interface. Read access will allow the StruxureWare to receive traps from the device, but Write access is required while you use the interface of the device to set the StruxureWare as a trap receiver.

For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available at **www.apc.com.**

SNMPv1

Path: Configuration > Network > SNMPv1 > *options*

NOTE: SNMPv1 is disabled by default. SNMPv2c is supported under SNMPv1 in this configuration.

Option	Description
access	**Enable SNMPv1 Access:** Enables SNMP version 1 as a method of communication with this device. **NOTE**: This configuration also supports SNMPv2c.
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, click its community name. • 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. • 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. **Community Name:** The name that an NMS must use to access the community. The maximum length is 15 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: • 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 setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. **Access Type**: The actions an NMS can perform through the community. • **Read**: GETS only, at any time • **Write**: GETS at any time, and SETS when no user is logged onto the Web User Interface or Command Line Interface. • **Write+**: GETS and SETS at any time. • **Disable**: No GETS or SETS at any time.

SNMPv3

Path: Configuration > Network > SNMPv3 > *options*

For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users. An SNMPv3 user must have a user profile assigned in the MIB software program to perform GETs and SETs, browse the MIB, and receive traps.

NOTE: SNMPv3 is disabled by default. To use SNMPv3, you must have a MIB program that supports SNMPv3. The device supports SHA or MD5 authentication and AES or DES encryption.

Option	Description
access	**SNMPv3 Access:** Enables SNMPv3 as a method of communication with this device.
user profiles	By default, 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. **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 Schneider Electric implementation of SNMPv3 supports SHA and MD5 authentication. Authentication will not occur unless an authentication protocol is selected. **Privacy Protocol:** 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. **NOTE:** You cannot select the privacy protocol if no authentication protocol is selected.

Option	Description
access control	You can configure up to four access control entries to specify which 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. • If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device. • 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, click its user name. **Access:** Mark the **Enable** checkbox to activate the access control specified by the parameters in this access control entry. **User Name:** From the drop-down list, select the user profile to which this access control entry will apply. The choices available are the four user names that you configure through the **user profiles** option on the left navigation menu. **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: • 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 setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

FTP Server

Path: Configuration > Network > FTP Server

The **FTP Server** settings enable (by default) or disable access to the FTP server. FTP is disabled by default.

By default, the FTP server communicates with the 8 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, disable the FTP server, and transfer files with SCP. Selecting and configuring Secure SHell (SSH) 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 StruxureWare, FTP Server must be enabled in the Rack PDU interface.

For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available at **www.apc.com**.

Notifications

Event Actions

Path: Configuration > Notification

Types of notification:

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

    You can also log system performance data to use for device monitoring. See “Logs in the Configuration Menu” on page 117 for information on how to configure and use this data logging option.
  - Queries (SNMP GETs)

    For more information, see “SNMP” on page 107. 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.

Configure event actions

Path: Configuration > Notification > Event Actions > By Event

By default, logging an event is selected for all events. To define event actions for an individual event:

1. To find an event, click on a column heading to see the lists under the **Device Events** or **System Events** categories.
   Or you can click on a sub-category under these headings, like **Security** or **Temperature**.
2. Click on the event name to view or change the current configuration, such as recipients to be notified by e-mail, or Network Management Systems (NMSs) to be notified by SNMP traps.
   If no Syslog server is configured, items related to Syslog configuration are not displayed.

NOTE: When viewing details of an event configuration, you can enable or disable event logging or Syslog, or disable notification for specific e-mail recipients or trap receivers, but you cannot add or remove recipients or receivers. To add or remove recipients or receivers, see the following:

- “Identifying Syslog servers” on page 117
- “Configuration > Notification > E-mail > Recipients” on page 112
- “SNMP trap receiver screen” on page 114

Path: Configuration > Notification > Event Actions > By Group

To configure a group of events simultaneously:

1. Select how to group events for configuration:
   - Select **Events by Severity**, and then select one or more severity levels. You cannot change the severity of an event.
   - Select **Events by Category**, and then select all events in one or more pre-defined categories.
2. Click **Next** to move to the next screen to do the following:
   - Select event actions for the group of events.
     - To select any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
     - If you selected **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** on the next screen. See “Logs in the Configuration Menu” on page 117
3. Click **Next** to move to the next screen to do the following:
   - If you selected **Logging** on the previous screen, select **Enable Notifications** or **Disable Notification**.
   - 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 move to the next screen to do the following:
   - If you are configuring **Logging** settings, view the pending actions and click **Apply** to accept the changes or click **Cancel** to revert to the previous settings.
   - If you are configuring **Email Recipients** or **Trap Receivers,** select **Enable Notifications** or **Disable Notification** and set the notification timing settings (see “Notification parameters:” on page 111 for more information on these settings).
5. Click **Next** to move to the next screen to do the following:
   - View the pending actions and click **Apply** to accept the changes or click **Cancel** to revert to the previous settings.

Notification parameters: These configuration fields define e-mail parameters for sending notifications of events.

They are usually accessed by clicking 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 2 minutes until the condition clears).
Up to *n* times	During an active event, the notification repeats for this number of times.
or	
Until condition clears	The notification is sent repeatedly until the condition clears or is resolved.

NOTE: For events that have an associated clearing event, you can also set these parameters.

E-mail notification screens

Use Simple Mail Transfer Protocol (SMTP) to send e-mail to up to four recipients when an event occurs. To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and, optionally, the secondary Domain Name System (DNS) servers.
- The IP address or DNS name for the SMTP Server and From Address.
- The e-mail addresses for a maximum of four recipients.
- You can use the To Address setting of the recipients option to send e-mail to a text-based screen.

Path: Configuration > Notification > E-mail > Server

This screen lists your primary and secondary DNS servers and displays the following fields:

From Address: The contents of the From field in e-mail messages sent by the device:

- In the format user@ [IP_address] (if an IP address is specified as Local SMTP Server)
- In the format user@domain (if DNS is configured and the DNS name is specified as Local SMTP Server) in the e-mail messages.
  NOTE: The local SMTP server may require that you use a valid user account on the server for this setting. See the server documentation.

SMTP Server: The IPv4/ IPv6 address or DNS name of the local SMTP server.
NOTE: This definition is required only when the SMTP server is set to **Local**.

Authentication: Enable this if the SMTP server requires authentication.

Port: The SMTP port number, with a default of 25. The range is 25, 465, 587, 2525, 5000 to 32768.

User Name, Password, and Confirm Password: If your mail server requires authentication, enter your user name and password here. This performs a simple authentication, not SSL/TLS.

Use SSL/TLS: Select when encryption is used.

- **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: This should only 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 root CA certificate must be loaded onto the device for encrypted e-mails to be sent.

File Name: This field is dependent on the root CA certificates installed on the device and whether or not a root CA certificate is required.

Path: Configuration > Notification > E-mail > Recipients

Specify up to four e-mail recipients. Click on a name to configure the settings.

Generation: Enables (default) or disables sending e-mail to the recipient.

To Address: The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page.

To bypass the DNS lookup of the IP address of the mail server, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.

Language: The language which the e-mail notification will be sent in. This is dependent on the installed language pack (if applicable).

Port: The SMTP port number, with a default of 25. The range is 25, 465, 587, 2525, 5000 to 32768.

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: Select one of the following methods for routing e-mail:

- **Local:** This is through the site-local SMTP server. This recommended setting ensures that the e-mail is sent using the site-local SMTP server. Choosing this setting limits delays and network outages and retries sending e-mail 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 e-mail account to receive the forwarded e-mail. Check with your SMTP server administrator before making these changes.
- **Recipient:** This is the SMTP server of the recipient. The Rack PDU performs an MX record look-up on the recipients e-mail address and uses that as its SMTP server. The e-mail is only sent once so it could easily be lost.
- **Custom:** This setting enables each e-mail recipient to have its own server settings. These settings are independent of the settings given under “SMTP Server” above.

Path: Configuration > Notification > E-mail > SSL Certificates

Load a mail SSL/TLS certificate on the device 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 here. An invalid certificate will display “n/a” for all fields except **File Name**.

Certificates can be deleted using this screen. Any e-mail recipients using the certificate should be manually modified to remove reference to this certificate.

Path: Configuration > Notification > E-mail > Test

Send a test message to a configured recipient.

SNMP trap receiver screen

Path: Configuration > Notification > SNMP Traps > Trap Receivers

With Simple Network Management Protocol (SNMP) traps, you can automatically get notifications for significant device events. They are a useful tool for monitoring devices on your network.

The trap receivers are displayed by **NMS IP/Host Name**, where 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) one, click its IP address/host name.

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.

Language: Select a language from the drop-down list. This can differ from the UI and from other trap receivers.

Select either the **SNMPv1** or **SNMPv3** radio button 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: Settings for SNMPv1.

- **Community Name:** The name used as an identifier when SNMPv1 traps are sent to this trap receiver.
- **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).

SNMPv3: Settings for SNMPv3.

- **User Name:** Select 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.

SNMP traps test screen

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 a 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 is displayed.

General Menu

This menu contains miscellaneous configuration items including device identification, date and time, exporting and importing your device configuration options, the three links at the bottom left of the screen, and consolidating data for troubleshooting purposes.

Identification screen

Path: Configuration > General > Identification

Define the **Name**, the **Location** (the physical location), and the **Contact** (the person responsible for the device) used by:

- the SNMP agent of the device and
- StruxureWare

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® *SNMP Management Information Base (MIB) Reference Guide*, available at **www.apc.com**.

Host Name Synchronization allows the host name to be synchronized with the system name so both fields automatically contain the same value.
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).

System Message: When defined, a custom message will appear on the log on screen for all users.

Date/Time screen

Path: Configuration > General > Date/Time > Mode

Set the time and date used by the device. You can change the current settings manually or through a Network Time Protocol (NTP) Server:

With both, you select the **Time Zone**. This is your local time difference with Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT).

Manual Mode: Do one of the following:

- Enter the date and time for the device
- Select the check box **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 device. By default, any device on the private side of a StruxureWare obtains its time settings by using StruxureWare as an NTP server.

- **Override Manual NTP Settings:** If you select this, data from other sources (typically DHCP) take precedence over the NTP configurations you set here.
- **Primary NTP Server:** Enter the IP address or domain name of the primary NTP server.
- **Secondary NTP Server:** Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.
- **Update Interval:** Define, in hours, how often the device 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.

Daylight Saving:

Path: Configuration > General > Date /Time > Daylight Saving

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.

Creating and importing settings with the config file

Path: Configuration > General > User Config File

Use the settings from one device to configure another. Retrieve the config.ini file from the configured device, customize that file (e.g., change the IP address), and upload the customized file to the new device. The file name can be up to 64 characters, and must have the.ini suffix.

Status	Reports the progress of the upload. The upload succeeds even if the file contains errors, but a system event reports the errors in the event log.
Upload	Browse to the customized file and upload it so that the current device can use it to set its own configuration.
Download	Allows the download of the Configuration File (config.ini) file directly through the Web browser to the user's computer.

To retrieve and customize the file of a configured device, see “How to Export Configuration Settings” on page 128.

Instead of uploading the file to one device, you can export the file to multiple devices by using an FTP or SCP script.

Configure Links

Path: Configuration > General > Quick Links

Select **Configuration** > **General** > **Quick Links** to view and change the URL links displayed at the bottom left of each page of the interface.

By default, these links access the following Web pages:

- **Link 1**: The home page of the APC by Schneider Electric website
- **Link 2**: Demonstrations of APC by Schneider Electric web-enabled products
- **Link 3:** Information on EcoStruxure IT

Logs in the Configuration Menu

Identifying Syslog servers

Path: Configuration > Logs > Syslog > Servers

Click **Add Server** to configure a new 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 device.

Port: The port that the device will use to send Syslog messages. The default UDP port assigned to Syslog is 514.

Language: Select the language for any Syslog messages.

Protocol: Select either UDP or TCP.

Syslog 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 device (User, by default).

NOTE: **User** best defines the Syslog messages sent by the device. 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 device 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
- **Informational**: Informational messages
- **Debug**: Debug-level messages

The following are the default settings for the **Local Priority** settings:

- **Critical** is mapped to **Critical**
- **Warning** is mapped to **Warning**
- **Informational** is mapped to **Info**

Syslog test and format example

Path: Configuration > Logs > Syslog > Test

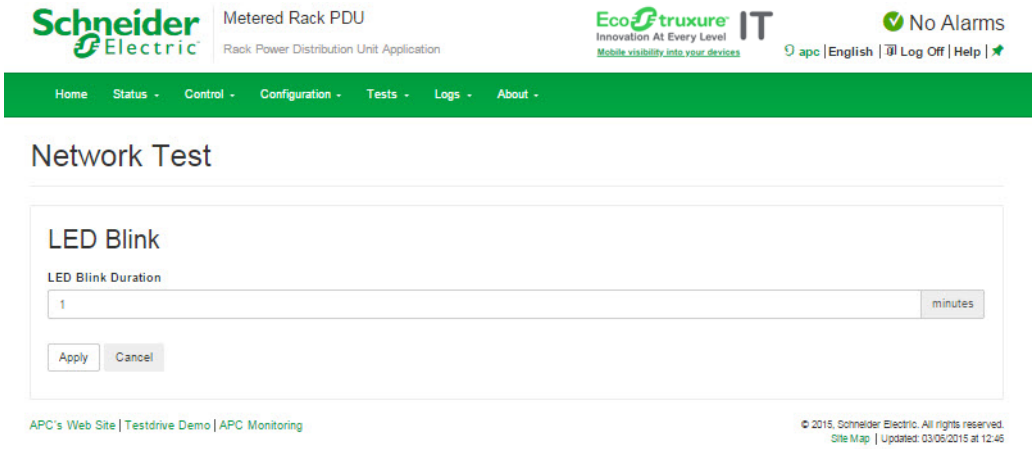
Send a test message to the Syslog servers (configured through the “Identifying Syslog servers” option above). The result will be sent to all configured Syslog servers.

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 device.
- The Header: a time stamp and the IP address of the device.
- 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.`

Tests Tab



Setting the Network Status LED to Blink

Path: Tests > Network > LED Blink

If you are having trouble finding your device, enter a number of minutes in the **LED Blink Duration** field, click **Apply**, and the Status LED on the display will blink.

Logs Tab

Event, Data and Firewall Logs

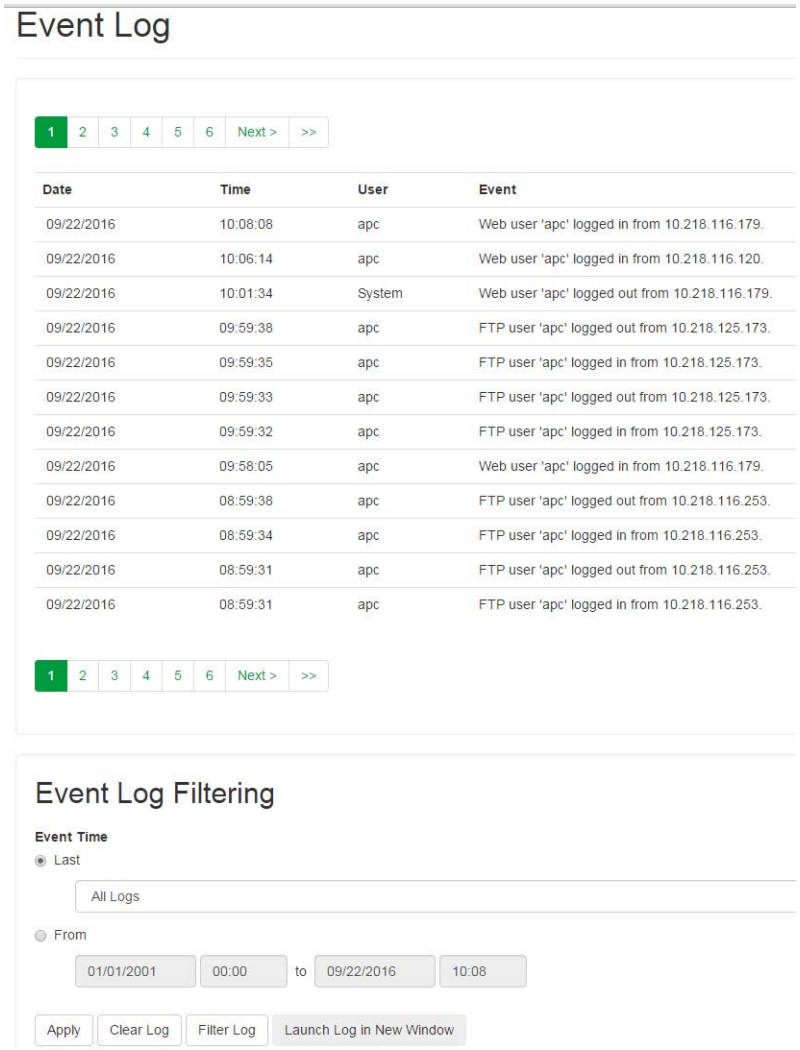
Event log

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.



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” on page 124.

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 device restarts.)
- Filtering the log by event severity or category:
  - Click **Filter Log**.
  - Clear a check box to remove it from view.
  - 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 device restarts.
- Removing an active filter:
  - Click **Filter Log.**
  - Click **Clear Filter (Show All)**.
  - As Administrator, click **Save As Default** to save this filter as the new default log view for all users.

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” on page 110

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.

Path: Logs > Events > Size

Use **Event Log Size** to specify the maximum number of log entries.

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.

Data log

Use the data log to display measurements about the device and the power input to the device.

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.

- Filtering the log by date or time: Use the **Last** or **From** radio buttons. (The filter configuration is saved until the device restarts.)
- Filtering the log by event severity or category:
  - Click **Filter Log**.
  - Clear a check box to remove it from view.
  - 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 device restarts.
- Removing an active filter:
  - Click **Filter Log.**
  - Click **Clear Filter (Show All)**.
  - 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.

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.

Path: Logs > Data > 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.

Path: Logs > Data > 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 *mmddyyyy_<filename>.txt*, 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.

Path: Logs > Data > 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, discarded). When logged here, these events are not logged in the main Event Log (see “Event log” on page 120).

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-delineated 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 device
  - The unique **Event Code** for each recorded event (*event.txt* file only)

NOTE: The device 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 for setting up the type of security you need.

To 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`

NOTEs:

- 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.

To use FTP to retrieve the `event.txt` or `data.txt` files.

1. At a command prompt, type `ftp` and the IP address of the device, 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`

   To set a non-default port value to enhance security for the FTP Server, see “FTP Server” on page 109. 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.

About Tab

About the Rack PDU

Path: About > RPDU/Network

The hardware information is useful to Schneider Electric Customer Support for troubleshooting problems with the device. The serial number and MAC address are also available on the device itself.

Firmware information for the Application Module, APC OS (AOS), and APC Boot Monitor indicates the name, the firmware version, and 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.apc.com.

Management Uptime is the length of time the network management interface has been running continuously.

Support Screen

Path: About > Support

With this option, you can consolidate various data in this interface into a single zipped file for troubleshooting purposes and customer support. The data includes the event and data logs, the configuration file and complex debugging information.

Click **Generate Logs** to create the file and then **Download**. You will be asked whether you want to view or save the zipped file.

Device IP Configuration Wizard

Capabilities, Requirements, and Installation

How to use the Wizard to configure TCP/IP settings

The Device IP Configuration Wizard can discover devices that do not have an IP address assigned. Once discovered, you can configure the IP address settings for the cards.

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 devices that already have a DHCP-assigned IP address.

NOTE: For detailed information on the Utility, see the Knowledge Base on the support page of the www.apc.com website and search for FA156064 (the ID of the relevant article).

NOTE: To use the DHCP Option 12 (AOS 5.1.5 or higher), see Knowledge Base ID FA156110.

System requirements

The Device IP Configuration Wizard is a Windows application designed specifically to remotely configure the basic TCP/IP settings of Network Management Cards. The Wizard runs on Microsoft® Windows® 2000, Windows Server® 2003, Windows Vista, Windows XP, Windows 7, Windows Server® 2008, Windows 8, and Windows 10, and Window 2012. This utility supports cards that have firmware version 3.x.x or higher and is for IPv4 only.

Installation

To install the Device IP Configuration Wizard from a downloaded executable file

1. Go to www.apc.com
2. Download the Device IP Configuration Wizard.
3. Run the downloaded executable file.

When installed, the Device IP Configuration Wizard is available through the Windows Start menu options.

How to Export Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

A Super User/Administrator can retrieve the .ini file of a device and export it to another device or to multiple devices. The steps are below; see details in the sections following.

1. Configure a device with the desired settings and export them.
2. Retrieve the .ini file from that device.
3. Customize the file to change the TCP/IP settings at least.
4. Use a file transfer protocol supported by the device to transfer a copy to one or more other devices. For a transfer to multiple devices, use an FTP or SCP script or the .ini file utility.
   NOTE: FTP is disabled by default. See “FTP Server” on page 109 to enable FTP.

Each receiving device uses the file to reconfigure its own settings and then deletes it.

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 article ID FA176542 in the Knowledge Base at **www.apc.com**.

Contents of the .ini file

The config.ini file you retrieve from a device 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 device settings. Each keyword is followed by an equals sign and a value (either the default or a configured value).
- The `Override` keyword: With its default value, this keyword prevents 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 device) blocks the exporting of values for the `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.

Detailed procedures

Retrieving: To set up and retrieve an .ini file to export:

1. If possible, use the interface of a device to configure it with the settings to export. (Directly editing the .ini file risks introducing errors).
2. Use FTP or SCP to retrieve the *config.ini* from the configured Rack PDU:
   - To use FTP:
     a. Open a connection to the Rack PDU using its IP address:
     ```
     ftp> open ip_address
     ```
     b. Log on using the Super User/Administrator user name and password.
     c. 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 the FTP.

     To retrieve configuration settings from multiple Rack PDUs and export them to other Rack PDUs, see *Release Notes: ini File Utility, version 2.0,* available at **www.apc.com**.
   - To use SCP, use the following command:
     `scp -c` *<cipher>* *username@hostname_or_ip_address*`:config.ini ./config.ini`

     Then enter the correct password.

     NOTEs:
     - 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.

Customizing: You must customize the file before you export it.

1. Use a text editor to customize the file.
   - 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 devices 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.**

Transferring the file to a single device: : To transfer the .ini file to another device, do either of the following:

- From the Web UI of the receiving device, 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 devices, i.e., FTP, FTP Client, SCP, or TFTP. The following example uses FTP:
  - From the folder containing the copy of the customized .ini file, use FTP to log in to the device to which you are exporting the .ini file:

    ```
    ftp> open ip_address
    ```

  - Export the copy of the customized .ini file to the root directory of the receiving device:

    ```
    ftp> put filename.ini
    ```

Exporting the file to multiple devices: To export the .ini file to multiple devices:

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single device.
- Use a batch processing file and the .ini file utility.
- To create the batch file and use the utility, see *Release Notes: ini File Utility, version 2.0*, available at **www.apc.com**.

The Upload Event and Error Messages

The event and its error messages

The following event occurs when the receiving device 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 device 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 device from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the device 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 device 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” on page 128 for information about which values are overridden.

Because the overridden values are device-specific and not appropriate to export to other devices, 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 device and configure other settings through its user interface. See “Device IP Configuration Wizard” on page 127.

File Transfers

Upgrading Firmware

Benefits of upgrading firmware

When you upgrade the firmware on the device:

- You obtain the latest bug fixes and performance improvements.
- New features become available for immediate use.

Keeping the firmware versions consistent across your network ensures that all devices support the same features in the same manner.

Upgrading here means simply placing the module files on the device; there is no installation required. Check regularly on **www.apc.com** for any new upgrades.

Firmware module files (device)

A firmware release has three modules, and they *must* be upgraded (that is, placed on the device) in the same order as shown in the table below.

NOTE: It is possible to skip upgrading the bootmon file if it is already the same version as the file located on the card.

Order	Module	Description
1	Boot Monitor (bootmon)	Roughly equivalent to the BIOS of a PC
2	American Power Conversion Operating System (AOS)	Can be considered the operating system of the device
3	Application	Specific to the device type

(Each module contains one or more Cyclical Redundancy Checks (CRCs) to protect its data from corruption).

The boot monitor module, the AOS, and the application file names share the same basic format:

`apc_hardware-version_type_firmware-version.bin`

- `apc`: Indicates the context.
- `hardware-version: hw0n` where n identifies the hardware version on which you can use this file.
- `type`: Identifies which module.
- `version`: The version number of the file.
- `bin`: Indicates that this is a binary file.

Firmware File Transfer Methods

NOTE: Upgrade the bootmon module first, then the AOS module, and finally, the application module by placing them on the device in that order.

Obtain the free, latest firmware version from the APC by Schneider Electric website. To upgrade the firmware of one or more devices, use 1 of these 5 methods:

- On a Windows operating system, use the **Firmware Upgrade Utility** downloaded from the website **www.apc.com**.
- On any supported operating system, use **FTP or SCP** to transfer the individual AOS and application firmware modules.
- For a device that is NOT on your network, use **XMODEM** through a serial connection to transfer the individual firmware modules from your computer to the device.
- For upgrades to **multiple devices**, see “Upgrading the firmware on multiple devices” and “Using the Firmware Upgrade Utility for multiple upgrades on Windows”.

Using the Firmware Upgrade Utility

This Firmware Upgrade Utility is part of the firmware upgrade package available on the **www.apc.com** website. (*Never* use an Upgrade Utility designated for one product to upgrade the firmware of another product).

Using the Utility for upgrades on Windows-based systems: On any supported Windows operating system, the Firmware Upgrade Utility automates the transferring of the firmware modules, *in the correct module order*.

Unzip the downloaded firmware upgrade file and double-click the .exe file. Then enter the IP address, the user name, and the password in the dialog fields and click **Upgrade Now**. You can use the **Ping** button to test your entered details. See “How to upgrade multiple devices” on page 135.

Using the Utility for manual upgrades, primarily on Linux: On non-Windows operating systems, the Firmware Upgrade Utility extracts the individual firmware modules, but does not upgrade the device. See “Firmware File Transfer Methods” on page 133 for the different upgrade methods after extraction.

To extract the firmware files:

1. After extracting files from the downloaded firmware upgrade file, run the **Firmware Upgrade Utility** (the .exe file).
2. At the prompts, click **Next>**, and then specify the directory location to which the files will be extracted.
3. When the **Extraction Complete** message displays, close the dialog box.

Use FTP or SCP to upgrade one Rack PDU

FTP: To use FTP to upgrade a device over the network:

- The device must be on the network, with its system IP, subnet mask, and default gateway configured.
- The FTP server must be enabled at the device, see “FTP Server” on page 109.

To transfer the files (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two, though):

1. The firmware module files must be extracted, see “To extract the firmware files:”.
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 device, 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 Administrator (**apc** is the default user name and password).
6. Upgrade the AOS. (Always upgrade the AOS before the application module).
   `ftp> bin`
   `ftp> put apc_hw05_aos_`*nnn*`.bin` (where *nnn* is the firmware version number)
7. When FTP confirms the transfer, type `quit` to close the session.
8. After 20 seconds, repeat step 3 through step 7, using the application module file name at step 6,

SCP: To use Secure CoPy (SCP) to upgrade 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.

This procedure assumes bootmon does not need upgrading. It is always necessary to upgrade the other two files:

1. Locate the firmware modules, see “Using the Utility for manual upgrades, primarily on Linux:” on page 133.
2. Use an SCP command line to transfer the AOS firmware module to the Rack PDU. The following example uses *nnn* to represent the version number of the AOS module:

   `scp -c <`*cipher*`> apc_hw05_aos_`*nnn*`.bin apc@158.205.6.185:apc_hw05_aos_`*nnn*`.bin`
   where <*cipher*> is either aes256-cbc or 3des-cbc.

   NOTE: This SCP command is for OpenSSH. The command may differ depending on the SSH tool used.
3. Use a similar SCP command line, with the name of the application module, to transfer the application firmware module to the Rack PDU. (Always upgrade the AOS before the application module).

Use XMODEM to upgrade one device

To use XMODEM to upgrade one device that is not on the network, you must extract the firmware files from the Firmware Upgrade Utility (see “To extract the firmware files:”).

To transfer the files (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two though):

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect the provided serial configuration cable (part number 940-0144A) to the selected port and to the RJ-12 style serial port at the device.
3. Run a terminal program such as Tera Term or HyperTerminal, and configure the selected port for 57600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press the **Reset** button on the device, then immediately press the **Enter** key 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 binary AOS firmware file to transfer using XMODEM. After the XMODEM transfer is complete, the Boot Monitor prompt returns.

   (Always upgrade the AOS before the application module).
7. To install the application module, repeat step 5 and step 6. In step 6, use the application module file name.
8. Type `reset` or press the **Reset** button to restart the device’s management interface.

How to upgrade multiple devices

Use one of these three methods:

- **Firmware Upgrade Utility:** Use this for multiple firmware updates in IPv4 if you have Windows. The utility records all upgrade steps in a log as a good reference to validate the upgrade.
- **Export configuration settings:** You can create batch files and use a utility to retrieve configuration settings from multiple devices and export them to other devices. See *Release Notes: ini File Utility, version 2.0,* available in the Knowledge Base at **www.apc.com**
- **Use FTP or SCP to upgrade multiple devices:** To upgrade multiple devices using an FTP client or using SCP, write a script which automatically performs the procedure.

NOTE: Utility is available from the Knowledge Base: **www.apc.com/support**

Using 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 device firmware:

1. Type in an IP address, a user name, and a password, and choose the **Ping** button if you need to verify an IP address.
2. Choose the **Device List** button to open the `iplist.txt` file. This should list any device IP, user name, and password.

   For example,
   ```
   SystemIP=192.168.0.1
   SystemUserName=apc
   SystemPassword=apc
   ```

   You can use an existing *iplist.txt* file if it already exists.
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.

Verifying Upgrades and Updates

Verify the success or failure of the transfer

To verify whether a firmware upgrade succeeded, use the `xferStatus` command in the Command Line Interface 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.

Code	Description
`Successful`	The file transfer was successful.
`Result not available`	There are no recorded file transfers.
`Failure unknown`	The last file transfer failed for an unknown reason.
`Server inaccessible`	The TFTP or FTP server could not be found on the network.
`Server access denied`	The TFTP or FTP server denied access.
`File not found`	The TFTP or FTP server could not locate the requested file.
`File type unknown`	The file was downloaded but the contents were not recognized.
`File corrupt`	The file was downloaded but at least one Cyclical Redundancy Check (CRC) failed.

Verify the version numbers of installed firmware.

Path: About > Network

Use the Web UI to verify the versions of the upgraded firmware modules. You could also use an SNMP GET to the MIB II sysDescr OID. In the Command Line Interface, use the **about** command.

Troubleshooting

Access Problems

For problems that persist or are not described here, contact APC by Schneider Electric Customer Care at www.apc.com.

Problem	Solution
Unable to ping the Rack PDU	If the device's Network Status LED is green, try to ping another node on the same network segment as the device. If that fails, it is not a problem with the device. If the Network Status LED is not green, or if the ping test succeeds, perform the following checks: • Verify all network connections. • Verify the IP addresses of the device and the NMS. • If the NMS is on a different physical network (or subnetwork) from the device, verify the IP address of the default gateway (or router). • Verify the number of subnet bits for the device's subnet mask.
Cannot allocate the communications port through a terminal program	Before you can use a terminal program to configure the device, you must shut down any application, service, or program using the communications port.
Cannot access the Command Line Interface through a serial connection	Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.
Cannot access the Command Line Interface remotely	• Make sure you are using the correct access method, Telnet or Secure SHell (SSH). The Super User or an Administrator can enable these access methods. By default, Telnet is disabled, and SSH is enabled. • For SSH, the device may be creating a host key. The device can take up to one minute to create the host key, and SSH is inaccessible for that time.
Cannot access the Web User Interface	• 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 device. SSL/TLS requires https, not http, at the beginning of the URL. • Verify that you can ping the device. • Verify that you are using a Web browser supported for the device. See "Supported Web Browsers" on page 72. • If the device has just restarted and SSL/TLS security is being set up, the device may be generating a server certificate. The Rack PDU can take up to one minute to create this certificate, and the SSL/TLS server is not available during that time. • Check that the Minimum Protocol setting configured on the Rack PDU for SSL/TLS does not match what is enabled or configured in your Web browser. **NOTE:** Check the specific error message reported by the browser. It may indicate the specific problem.
The Rack PDU reports "Component communications lost with Phase Meter" and/or "Communication lost" alarms	Refer to Knowledge Base FA168022 at www.apc.com.

SNMP Issues

Problem	Solution
Unable to perform a GET	• Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3). • Use the Command Line Interface or UI to ensure that the NMS has access. See “SNMP” on page 107
Unable to perform a SET	• Verify that SNMP is enabled. SNMPv1 and SNMPv3 are disabled by default. • Verify the read/write (SET) community name (SNMPv1) or the user profile configuration (SNMPv3). • Use the Command Line Interface or UI to ensure that the NMS has write (SET) access (SNMPv1) or is granted access to the target IP address through the access control list (SNMPv3). See “SNMP” on page 107.
Unable to receive traps at the NMS	• Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the NMS as a trap receiver. • For SNMP v1, query the **mconfigTrapReceiverTable** MIB OID to verify that the NMS IP address is listed correctly and that the community name defined for the NMS matches the community name in the table. If either is not correct, use SETs to the **mconfigTrapReceiverTable** OIDs, or use the Command Line Interface or UI to correct the trap receiver definition. • For SNMPv3, check the user profile configuration for the NMS, and run a trap test.. See “SNMP” on page 107, “SNMP trap receiver screen” on page 114, and “SNMP traps test screen” on page 114.
Traps received at an NMS are not identified	See your NMS documentation to verify that the traps are properly integrated in the alarm/trap database.

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. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the University of California, Berkeley and its contributors.
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.

Radio Frequency Interference

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

USA—FCC

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference. The user will bear sole responsibility for correcting such interference.

Canada—ICES

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Japan—VCCI

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると、電波妨害を引き起こすことがあります。この場合には、使用者が適切な対策を講ずるように要求されることがあります。

Taiwan—BSMI

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Worldwide Customer Support

Customer support is available at **www.apc.com**.

© 2019 APC by Schneider Electric. APC, PowerNet, StruxureWare, and EcoStruxure are trademarks owned by Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owners.