APC
by Schneider Electric

User Guide

150/175kW Modular Power Distribution Unit

PDPM150L6F
PDPM150G6F
PDPM175G6H

Legal Information

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

Contents

Introduction

Product Features

The APC by Schneider Electric Modular Power Distribution Unit provides power distribution and management of electrical power to equipment racks. The Modular PDU provides full management capabilities over a network using Telnet, Secure SHell (SSH), HyperText Transfer Protocol (HTTP), HTTP over Secure Sockets Layer (HTTPS), File Transfer Protocol (FTP), Secure CoPy (SCP), Modbus, and Simple Network Management Protocol (SNMP) versions 1 and 3. The Modular PDU also provides the following features:

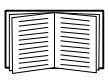
- Supports input contact and relay output monitoring for use with dry contact sensors.
- Provides the ability to export a user configuration (.ini) file from a configured Modular PDU to one or more unconfigured Modular PDUs without converting the file to a binary file.
- Supports using a Dynamic Host Configuration Protocol (DHCP) or server to provide the network (TCP/IP) values for the Modular PDU.
- Provides data and event logs.
- Enables you to configure notification through event logging (by the Modular PDU and Syslog), e-mail, and SNMP traps. You can configure notification for single events or groups of events, based on the severity level or category of events.
- Provides a selection of security protocols for authentication and encryption.

Initial setup

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

- IP address of the Modular PDU
- Subnet mask
- IP address of the default gateway

Caution: Do not use the loopback address as the default gateway. Doing so disables the Modular PDU. You must then log on using a serial connection and reset TCP/IP settings to their defaults.



To configure the TCP/IP settings, see the Modular PDU *Installation and Start-Up Manual*, available in printed form and on the APC Web site, **www.apc.com**.
For detailed information on how to use a DHCP server to configure the TCP/IP settings at the Modular PDU, see “TCP/IP and Communication Settings”.

Network management features

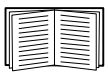
These applications and utilities work with a Modular PDU that connects to the network through its Network Management Card:

- APC InfraStruxure® Central—Provide enterprise-level power management and management of APC agents, Modular PDUs, information controllers, and environmental monitors
- APC PowerNet® Management Information Base (MIB) with a standard MIB browser—Perform SNMP SETs and GETs and to use SNMP traps
- APC Device IP Configuration Wizard—Configure the basic settings of one or more Modular PDUs over the network
- APC Security Wizard—Create the components needed for high security for the Modular PDU when you are using Secure Sockets Layer (SSL) and related protocols and encryption routines

Internal Management Features

Overview

Use the Web interface or the command line interface to manage the Modular PDU.



For more information about the internal user interfaces, see “Web Interface” and “Command Line Interface”.

Access priority for logging on

Only one user at a time can log on to the Modular PDU. The priority for access, beginning with the highest priority, is as follows:

- Local access to the command line interface from a computer with a direct serial connection to the Modular PDU.
- Telnet or Secure SHell (SSH) access to the command line interface from a remote computer.
- Web access, either directly or through InfraStruxure Central

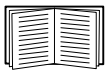
Types of user accounts

The Modular PDU has three levels of access (Administrator, Device User, and Read-Only User), which are protected by user name and password requirements. During authentication, the user's credentials are compared against the Local User Database and/or are validated against a RADIUS server (depending on configuration). If valid, access with appropriate permissions is granted to the command line interface.

- An Administrator can use all the menus in the Web interface and command line interface. The default user name and password are both **apc**.
- The default user name for the Device User is **device**, and the default password is **apc**. A Device User can access only the following:
  - In the Web interface, the menus on the **Home**, **Power Distribution**, **Contacts/Relays**, **Alarms**, and **Logs** tabs and the event and data logs.
  - In the command line interface, the equivalent features and options.

- A Read-Only User has the following restricted access:
  - Access through the Web interface only. You must use the Web interface to configure values for the Read-Only User.
  - Access to the same tabs and menus as a Device User, but without any capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled, and the event and data logs display no button to clear the log.

  The default user name is **readonly**, and the default password is **apc**.



To set User Name and Password values for the three account types, see “Setting user access”.

How to Recover from a Lost Password

You can use a local computer, a computer that connects to the Modular PDU or other device through the serial port or USB console port, to access the command line interface.

1. At the local computer, do one of the following:
   - Select a serial port and disable any service that uses it. Connect the provided serial cable between the selected serial port on the local computer and the serial port on the modular PDU, OR
   - Connect the provided standard USB cable between the modular PDU USB console port and the computer USB port. A virtual serial port will be discovered on the computer.
2. Open a terminal program/emulator (such as HyperTerminal®) and configure the (virtual) serial port for 9600 bps (USB serial works with any other baud rate automatically), 8 data bits, no parity, 1 stop bit, and no flow control.
3. 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 2.
   - The correct cable is being used as specified in step 1.
4. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
5. Press ENTER as many times as necessary to redisplay the **User Name** prompt, 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 redisplayed, you must repeat step 5 and log on again.)
6. From the **command line interface** menu, select **System**, then **User Manager**.
7. Select **Administrator**, and change the **User Name** and **Password** settings, both of which are now defined as **apc**.
8. Press CTRL+C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the Modular PDU uses internal, system-wide watchdog mechanisms. When it restarts to recover from an internal problem, a **System: Warmstart** event is recorded in the event log.

Network interface watchdog mechanism

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

Resetting the network timer

To ensure that the Modular PDU does not restart if the network is quiet for 9.5 minutes, the Modular PDU attempts to contact the default gateway every 4.5 minutes. If the gateway is present, it responds to the Modular PDU, and that 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 most of the time and is on the same subnet. The network traffic of that computer will restart the 9.5-minute timer frequently enough to prevent the Modular PDU from restarting.

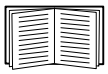
Command Line Interface

Overview

Overview

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection with a computer on the same network as the Modular PDU to access the command line interface.

Use case-sensitive user name and password entries to log on (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device User). A Read-Only User cannot access the command line interface.



If you cannot remember your user name or password, see “How to Recover from a Lost Password”.

Remote access to the command line interface

You can access the command line interface through Telnet or Secure SHel (SSH). Telnet is enabled by default. Enabling SSH disables Telnet.

To enable or disable these access methods:

- In the Web interface. On the **Administration** tab, select **Network** on the top menu bar, and then the **access** option under **Console** on the left navigation menu.
- In the command line interface, use the **Telnet/SSH** option of the **Network** menu.

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

To use Telnet to access the command line interface:

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

   If the Modular PDU uses a non-default port number (from 5000 to 32768), you must include a colon or a space, depending on your Telnet client, between the IP address (or DNS name) and the port number. (These are commands for general 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 an Administrator, or **device** and **apc** for a Device User).

SSH for high-security access. If you use the high security of SSL for the Web 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.

Local access to the command line interface

For local access, use a computer that connects to the Modular PDU through the serial port (available on all models) or USB console port (not available on older models) to access the command line interface:

1. At the local computer, do one of the following:
   a. Select a serial port and disable any service that uses it. Connect the provided serial cable (part 940-0299) between the selected serial port on the local computer and the serial port on the modular PDU, OR
   b. Connect the provided standard USB cable between the modular PDU USB console port and the computer USB port. A virtual serial port will be discovered on the computer.
2. Run a terminal program/emulator (e.g., HyperTerminal), and configure the (virtual) serial port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
3. Press ENTER. At the prompts, enter your user name and password.

Main Screen

Following is an example of the screen displayed when you log on to the command line interface of the Modular PDU.

```
User Name : <admin or device Name>
Password : <admin or device Password>

American Power Conversion              Network Management Card AOS  vx.x.x
(c)Copyright 2011 All Rights Reserved  Modular PDU                  vx.x.x
-------------------------------------------------------------------------
Name     : Test Lab                                  Date : 10/30/2011
Contact  : Don Adams                                 Time : 5:58:30
Location : Building 3                                User : Administrator
Up Time  : 7 Days, 21 Hours, 21 Minutes              Stat : P+ N+ A+

Type @ for command listing
Use tcpip command for IP address(-i), subnet(-s), and gateway(-g)

apc>
```

- Two fields identify the APC operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the device that connects to the network through this NMC. In the example above, the NMC uses the application firmware for a Modular PDU.

  ```
  NMC AOS                    vx.x.x
  Modular PDU APP            vx.x.x
  ```

- Three fields identify the system name, contact person, and location of the Modular PDU. (In the Web interface, select the **Administration** tab, **General** in the top menu bar, and **Identification** in the left navigation menu to set these values.)

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

- The **Up Time** field reports how long the Modular PDU has been running since it was last turned on or reset.

  ```
  Up Time: 7 Days 21 Hours 21 Minutes
  ```

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

  ```
  Date : 10/30/2011
  Time : 5:58:30
  ```

- The **User** field reports whether you logged in through the **Administrator** or **Device Manager** account. (The **Read Only User** account cannot access the command line interface.)
  When you log on as Device Manager (equivalent to Device User in the Web interface), you can access the event log, configure some settings, and view the number of active alarms.

  ```
  User : Administrator
  ```

- The **Stat** field reports the Modular PDU status.

  ```
  Stat:P+ N+ 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 Modular PDU failed to connect to the network.
N!	N6!	N4! N6!	Another device is using the Modular 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.

If P+ is not displayed, contact APC support.

Using the Command Line Interface

Logging in

On initial access to the MDU via a serial, Telnet, or SSHv1/v2 connection the user will be prompted to login. The user name prompt will be: `User Name:` Type in your user name and press ENTER. The password prompt is `Password :` If your user name and password are valid, then you will be logged into the command line interface.

The Modular PDU command line interface prompt is: `apc>`

Command errors

If the user enters a command that does not exist, then the following error message will be displayed: `E101: Command Not Found`.

The existence of commands can be probed by requesting help for the command (help <command>). If the command exists, then its help is displayed, else the message

"E102: Parameter Error" is displayed.

Options

The command line interface provides options to configure the network settings and manage the Modular PDU. At the command line interface, use commands to configure the Modular PDU. To use a command, type the command and press ENTER. Commands and arguments are completely case insensitive. 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 the command history.
- Type at least one letter of a command and press the TAB key to use the command completion function to complete the command to the first available matched command. Press the TAB key repeatedly to scroll through a list of valid commands that match the text you typed in the command line. Once all available commands have been scrolled through, then the original partial entered command is displayed. The backspace key will delete the last character of the command string entered and is the only editing function available during command entry.
- Use the command delimiter (a space) between commands and arguments. Extra white space between commands and arguments will be ignored. Command responses will have all fields delimited with commas for efficient parsing.
- Type `exit` or `quit` to close the connection to the command line interface.

Login timeout and lockout

- The Modular PDU will automatically logout of the command line interface due to inactivity. The default logout time due to inactivity is 3 minutes. The minimum inactivity timeout is 1 minute and the maximum is 10 minutes.
- Prompting for User Input during Command Execution: The execution of certain commands requires user input (ex. xferINI prompting for baudrate speed). There is a fixed timeout at such prompts of 1 minute. Should the user not enter any text within the timeout then the command will print: `"E100: Command Failed."` and the command prompt will be displayed.
- The Modular PDUModular PDU implements a fixed 2 minute lockout when more than three successive failed attempts have been made to login. During the lockout the Modular PDU will not respond to any input from the serial or remote interfaces.
- If the Modular PDU application layer does not start, then the Modular PDU specific commands will not be accessible.

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 pipe symbol (vertical line) between items enclosed in brackets or angle brackets indicates the word **OR**, meaning that the items are mutually exclusive. You must use one of the items.

Argument Quoting. Argument values may optionally be enclosed in double quote characters. String values beginning or ending with spaces, or containing commas or semicolons, must be enclosed in quotes for both input and output. Quote and backslash ("\") characters, appearing inside strings should NOT be encoded using traditional escape sequences (described Escape Sequences). All binary characters that appear inside strings will be treated as unreadable characters and rejected. Should a " or \ be part of the argument value then they must be escaped with a preceding backslash. When a quote or backslash symbol is supplied as a part of the input string - the input string must be provided in double quotes.

Escape sequences. Escape sequences, traditionally consisting of a backslash followed by a lower case letter or by a combination of digits, are ignored and not should be used to encode binary data or other special characters and character combinations. The result of each escape sequence is parsed as if it were a both the backslash and the traditionally escaped character. Again, any binary data will force an error and will cause the entire value and keyword pair to be ignored.

Syntax examples

```
<command> <arg1> [<agr2> <arg3a | arg3b> [<arg4a | arg4b | arg4c>]]
```

For the above example: arg1 must be used, but arg2-4 are optional. If arg2 is used, then arg3a or arg3b must also be used. arg4 is optional, but arg1-3 must be precede arg4.

With most commands if the last argument is omitted then the command provides information to the user, otherwise the last argument is used to change/set new information. For example:

```
apc> ftp -p (displays the port number when omitting the arg2)
E000: Success
Ftp Port:       5001

apc> ftp -p 21 (sets the port number to arg2)
E000: Success
```

A command that supports multiple options:

```
user [-an <admin name>] [-ap <admin password>]
```

In this example, the `user` command accepts the option `-an`, which defines the Administrator user name, and the option `-ap`, which defines the Administrator password. To change the Administrator user name and password to XYZ:

1. Type the `user` command, one option, and the argument XYZ:
   `user -ap XYZ`
2. After the first command succeeds, type the `user` command, the second option, and the argument XYZ:
   `user -an XYZ`

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 line interface reports all command operations with the following format:

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

Code	Message	Notes
E000	Success	
E001	Successfully Issued	
E100	Command failed	
E101	Command not found	
E102	Parameter Error	Reported when there is any problem with the arguments supplied to the command, too few, too many, wrong type, etc.
E103	Command Line Error	
E104	User Level Denial	
E105	Command Prefill	
E106	Data Not Available	
E200	Input error	Only reported when an error occurs durig the execution of a command.
E201	No Response	Reported when a sensor fails to respond.
E202	Invalid target	User failed to input a target or target was out of range.
E203		
E204		

All command operations that are successful will have an error code of 99 or less. Any error code 100 or greater indicates some kind of failure.

Example:

```
E000: Success
Followed by the output of the command, if any.
```

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

Prompting for user input during command execution. The execution of certain commands requires user input (ex. xferINI prompting for baudrate speed). There is a fixed timeout at such prompts of 1 minute. Should the user not enter any text within the timeout then the command will print "E100: Command Failed." and the command prompt will be displayed.

Configuration for data not supported directly by the command line interface . The command line interface allows an INI file push to the device via XMODEM. This mechanism allows full configurability of the Modular PDU via the command line interface. The user is not allowed to read the current INI file via XMODEM.

Interface Management Commands

? or **help**

Access: Administrator, Device

Description: View a list of all the commands available to your account type. To view help text for a specific command, type the command followed by a question mark (`?`) or the word `help`.

Example 1:

```
apc > ?

Network Management Card Commands:
------------------------------------------------------------------------
?            about         alarmcount    boot          cd            date
delete        dir           eventlog      exit          format        ftp
help          ping           portspeed     prompt         quit
radius
reboot        resetToDef    system        tcpip         user          web
xferINI       xferStatus
Device Commands:
------------------------------------------------------------------------
cableAlarm    cableHighThresh cableLowThresh cableMaxThresh
cableminThresh
cableTarget   moduleStatus    moduleTarget   subfeedAlarmGeneration
subfeedHighThresh  subfeedLowThresh subfeedMaxThresh  subfeedMinThresh
subfeedLocation  subfeedName  subfeedTarget
```

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>]
```

about

Access: Administrator, Device

Description: View hardware and firmware information (Model Number, Serial Number, Manufacture Dates). This information is useful in troubleshooting and enables you to determine if updated firmware is available at the APC Web site.

alarmcount

Access: Administrator, Device

Description: Display the count alarms that are present with-in the system. The 'all' option is the default when no parameters are entered.

Option	Arguments	Description
-p	all	View the number of active alarms reported by the NMC. 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:

```
alarmcount -p warning
```

boot

Access: Administrator only

Description: Allows the user to get/set the network startup configuration of the device, such as setting boot mode (DHCP vs BOOTP vs MANUAL). Defines how the NMC will obtain its network settings, including the IP address, subnet mask, and default gateway. Then configure the BOOTP or DHCP server settings.

Option	Argument	Description
-b <boot mode>	dhcp | bootp | manual	Define how the TCP/IP settings will be configured when the NMC turns on, resets, or restarts. See “TCP/IP and Communication Settings” for information about each boot mode setting.
-a	remainDhcpBootp | gotoDhcpOrBootp	After IP Assignment
-o	stop | prevSettings	On Retry Fail
-c	enable | disable	`dhcp` boot modes only. Enable or disable the requirement that the DHCP server provide the APC cookie.
-s	retry then stop #	Note: 0 = never
-v	retry then fail #	Note: 0 = never
The default values for these three settings generally do not need to be changed: -v <vendor class>: APC -i <client id>: The MAC address of the NMC, which uniquely identifies it on the network -u <user class>: The name of the application firmware module		

Example:

```
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
```

cd

Access: Administrator, Device User

Description: Allow 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 command line interface.

Parameters: directory name

Example 1:

```
apc> cd logs
E000: Success

apc> cd /
E000: Success
```

console

Access: Administrator only

Description: Define whether users can access the command line interface using Telnet, which is enabled by default, or Secure SHell (SSH), which 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.

Option	Argument	Description
-S	disable | telnet | ssh	Configure access to the command line interface, or use the `disable` command to prevent access.. Enabling SSH enables SCP and disables Telnet.
-pt	<telnet port n>	Define the Telnet port used to communicate with the NMC (23 by default).
-ps	<SSH port n>	Define the SSH port used to communicate with the NMC (22 by default).
-b	2400 | 9600 | 19200 | 38400	Configure the speed of the serial port connection (2400 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:

```
console -pt 5000
```

date

Access: Administrator only

Definition: Set the date and time.

Option	Argument	Description
-d	“datestring”	Set the current date. Use the date format specified by the `date -f` command.
-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 synchonize with other people in different time zones.

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

Example 2: To define the date as October 30, 2011, using the format configured in the preceding example, type: `date -d “2011-10-30”`

Example 3: To define the time as 5:21:03 p.m., type: `date -t 17:21:03`

delete

Access: Administrator only

Description: Delete the event or data log, or delete a file in the file system.

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

Example: To delete the event log:

1. Navigate to the folder that contains the file to delete. For example, to navigate to the `logs` folder, type: `cd logs`
2. To view the files in the `logs` folder, type: `dir`

   The file `event.txt` is listed.
3. Type `delete event.txt`.

dir

Access: Administrator, Device

Description: Display the files and folders stored in the working directory.

Example:

```
apc> dir
E000: Success
--wx-wx-wx  1 apc      apc      3145728 Mar 3  2011 aos.bin
--wx-wx-wx  1 apc      apc      3145728 Mar 4  2011 app.bin
-rw-rw-rw-  1 apc      apc        45000 Mar 6  2011 config.ini
drwxrwxrwx  1 apc      apc            0 Mar 3  2011 db/
drwxrwxrwx  1 apc      apc            0 Mar 3  2011 ssl/
drwxrwxrwx  1 apc      apc            0 Mar 3  2011 ssh/
drwxrwxrwx  1 apc      apc            0 Mar 3  2011 logs/
drwxrwxrwx  1 apc      apc            0 Mar 3  2011 sec/
drwxrwxrwx  1 apc      apc            0 Mar 3  2011 dbg/
drwxrwxrwx  1 apc      apc            0 Mar 3  2011 Modular PDU/
```

dns

Access: Administrator

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

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.

eventlog

Access: Administrator, Device User

Description: View the date and time you retrieved the event log, the status of the Modular PDU, and the status of sensors. View the most recent device events, and the date and time they occurred. Use the following keys to navigate the event log:

Key	Description
ESC	Close the event log and return to the command line interface.

Key	Description
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: 03/06/2011 Time: 13:22:26
     ----------------------------------
     Modular PDU: Communication Established
     Date        Time      Event
     ------------------------------------------------------------
     03/06/2009  13:17:22  System: Set Time.
     03/06/2009  13:16:57  System: Configuration change. Date format
                           preference.
     03/06/2009  13:16:49  System: Set Date.
     03/06/2009  13:16:35  System: Configuration change. Date format
                           preference.
     03/06/2009  13:16:08  System: Set Date.
     03/05/2009  13:15:30  System: Set Time.
     03/05/2009  13:15:00  System: Set Time.
     03/05/2009  13:13:58  System: Set Date.
     03/05/2009  13:12:22  System: Set Date.
     03/05/2009  13:12:08  System: Set Date.
     03/05/2009  13:11:41  System: Set Date.
   <ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

exit or **quit**

Access: Administrator, Device User

Description: Exit/Quit/ Leave the command line interface session.

Example:

```
apc> exit
Bye
```

format

Access: Administrator only

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

Note: To reset to the default configuration, use the `resetToDef` command.

Parameters: None, but you must enter a "`YES`" to confim after the command has been issued.

Example:

```
apc> format
 Format FLASH file system
 Warning: This will delete all configuration data,
          event and data logs, certs and keys.
Enter 'YES' to continue or <ENTER> to cancel :
apc>
```

ftp

Access: Administrator only

Description: Enable or disable access to the FTP server. Optionally, change the port setting to the number of any unused port (21, the default, and 5000 to 32768) for added security.

Option	Argument	Definition
-p	port number	Define the TCP/IP port that the FTP server uses to communicate with the NMC (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.

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

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

To display the TCP/IP port number, type:

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

To change the TCP/IP port to 21, type:

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

ping

Access: Administrator, Device

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

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

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

portSpeed

Access: Administrator

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

Option	Arguments	Description
-s	auto | 10H | 10F | 100H | 100F	Define the communication speed of the Ethernet port. The `auto` command enables the Ethernet devices to negotiate to transmit at the highest possible speed. auto = Auto_negotiation H = Half Duplex F = Full Duplex 10 = 10 Meg Bits 100 = 100 Meg Bits

Examples:
To display portspeed, type:

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

To configure the TCP/IP port to communicate using 100 Mbps with half-duplex communication (communication in only one direction at a time), type:

```
apc> portspeed -s 100h
E000: Success
```

To configure the TCP/IP port to communicate using the auto command.

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

prompt

Access: Administrator, Device User

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

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>`

Examples:
To include the account type of the currently logged-in user in the command prompt, type:

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

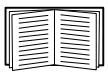
To change the command prompt to the default setting:

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

radius

Access: Administrator only

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".

Additional authentication parameters for RADIUS servers are available at the Web interface of the Modular PDU. See "RADIUS" for more information.

For detailed information about configuring your RADIUS server, see the *Security Handbook*, available on the *Utility* CD and at the APC Web site, **www.apc.com**.

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.

Option	Argument	Description
-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.
-s1 -s2	server secret	The shared secret between the primary or secondary RADIUS server and the Modular PDU.
-t1 -t2	server timeout	The time in seconds that the Modular PDU waits for a response from the primary or secondary RADIUS server.

Examples:
To view the existing RADIUS settings for the Modular PDU, type `radius` and press ENTER.

To enable RADIUS and local authentication, type:
```
radius -a radiusLocal
```

To configure a 10-second timeout for a secondary RADIUS server, type:
```
radius -t2 10
```

reboot

Access: Administrator only

Description: Restart the interface of the Modular PDU. Confirm the operation by entering a "`YES`" after the command has been entered.

Example:

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

resetToDef

Access: Administrator only

Description: Reset all configuration parameters to the factory default. Confirm the operation by entering a "`YES`" after the command has been entered. The system will reboot if any configuration is changed once the user logs out of the command line interface.

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

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

```
apc> resettodef -p keepip
Reset to Defaults Except TCP/IP
Enter 'YES' to continue or <ENTER> to cancel : : <user enters 'YES'>
all User Names, Passwords.
Please wait...

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

snmp, snmp3

Access: Administrator only

Description: Enable or disable SNMP 1 or SNMP 3.

Option	Arguments	Description
-S	enable | disable	Enable or display the respective version of SNMP, 1 or 3.

Example: To enable SNMP version 1, type:

```
apc> -S enable
E000: Success
SNMPv3
```

system

Access: Administrator only

Description: View and set the system name, contact, and location. If no parameters are entered, then the device displays all of the current system descriptions. If the second parameter is not entered, then the device displays the current system description. If the second parameter is entered, that parameter is stored at the appropriate retentive memory address.

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 InfraStruxure Central and the NMC's SNMP agent.
-c	<system contact>	
-l	<system location>	

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

```
system -l "Test Lab"
```

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

```
system -n "Don Adams"
```

tcpip

Access: Administrator only

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

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

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

```
apc> tcpip
E000: Success
IP Address:     192.168.1.49
MAC Address:    XX XX XX XX XX XX
Subnet Mask:    255.255.255.0
Gateway:        192.168.1.1
Domain Name:    example.com
Host Name:      HostName
```

Example 2: To manually configure an IP address of `192.168.1.49` for the Modular PDU, type:

```
tcpip -i 192.168.1.49
```

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

tcpip6

Access: Administrator only

Description: Enable IPv6 and view and manually configure these network settings for the Modular PDU:

Option	Argument	Description
-S	enable | disable	Enable or disable IPv6.
-man	enable | disable	Enable manual adressing for the IPv6 address of the NMC.
-auto	enable | disable	Enable the NMC to automatically configure the IPv6 address.
-i	<IPv6 address>	Set the IPv6 address of the Modular PDU.
-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 1: To view the network settings of the Modular PDU, type `tcpip6` and press ENTER.

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

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

user

Access: Administrator only

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

Option	Argument	Description
-an -dn -rn	<admin name> <device name> <read-only name>	Set the case-sensitive user name for each account type. The maximum length is 10 characters.
-ap -dp -rp	<admin password> <device password> <read-only password>	Set the case-sensitive password for each account type. The maximum length is 32 characters. Blank passwords (passwords with no characters) are not allowed.
-t	<minutes>	Configure the time (3 minutes by default) that the system waits before logging off an inactive user.

Example 1: To change the Administrator user name to XYZ, type: `user -an XYZ`

```
apc> user -an XYZ
E000: Success
```

Example 2: To change the log off time to 10 minutes, type: `user -t 10`

```
apc> user -t 10
E000: Success
```

web

Access: Administrator

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

For additional security, you can change the port setting for HTTP and HTTPS to any unused port from 5000 – 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:
`http://152.214.12.114:5000`

Option	Argument	Definition
-S	disable | http | https	Configure access to the Web interface. 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 Modular PDU (80 by default). Choose from 5000 to 32768.
-ps	<https port #>	Specify the TCP/IP port used by HTTPS to communicate with the Modular PDU (443 by default). Choose from 5000 to 32768.

Example: To prevent all access to the Web interface, type: `web -S disable`

xferINI

Access: Administrator only.

Description: Use XMODEM to upload an .ini file while you are accessing the command line interface through a serial connection. This command is only available through the serial interface. 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 the Modular PDU, you must reset the baud rate to the default to re-establish communication with the Modular PDU.

Example:

```
apc> xferINI
Enter 'YES' to continue or <ENTER> to cancel : <user enters 'YES'>
------- 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 (The capital Cs are the xmodem receiver waiting on input. There may be 1 or multiple Cs. They occur about every 2-3 seconds.)

```
<user starts sending INI>
150 bytes have successfully been transmitted.
apc>
```

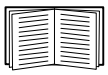
xferStatus

Access: Administrator only

Description: View the result of the last INI file transfer.

Example:

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



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

Device Management Commands

Many device management commands are settable and will accept data values in integer or floating-point format. Once a value has been entered it may be rounded based on the command. For example: If the user sets a command to a value of **1.33** and that command has a resolution of 0.1, then the value will be rounded to **1.3**. The value will be checked against the acceptable range of the command before being accepted. The commands are logically segmented to represent the physical device. The system segment supports status and alarm configuration for the power available to the device. The power distribution segment is comprised of subfeeds, modules and cables, supports status, configuration and alarm controls for those components. Additionally, the environment segment supports status, configuration and alarm controls for input contacts and output relays. Finally there is support to display the manufacturing configuration of the device and components.

System

The system voltage and current alarm thresholds are configuration commands that are overloaded to provide a status version of the command. The status version is issued with no parameters. Examples are contained in some of the command description sections that follow.
System voltage and current alarm threshold commands:

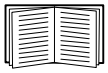
```
sysThrMxV
sysThrHiV
sysThrLoV
sysThrMnV
sysThrMxI
sysThrHiI
sysThrLoI
sysThrMnI
```

System frequency deviation and alarm command:

`sysFreqDev`

System measurement display command:

`sysOutput`



See system commands starting on page 28.

Subfeeds

Power distribution subfeed alarm thresholds and enable commands:

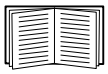
`subfdThrMx`
`subfdThrHi`
`subfdThrLo`
`subfdThrMn`
`subfdAlarm`

Subfeed configuration commands:

`subfdTarget`
`subfdName`
`subfdLocation`

Subfeed status request command:

`subfdStatus`



See subfeed commands starting on page 32.

Modules and Cables

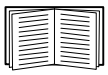
Each module and associated cable/cables can be queried for status, configured for alarm thresholds and identified with name and location.

The module commands are:

`modStatus`
`modTarget`

The commands dealing with the cables associated with the target module are:

`cblAlarm`
`cblThrMx`
`cblThrHi`
`cblThrLo`
`cblThrMn`
`cblTarget`
`cblName`
`cblLoc`

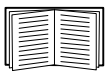


See module and cable commands starting on page 36

Manufacturing Info

The devices that comprise the 150kW Modular PDU are configured at manufacture time and at assembly time. This information is available through the following commands:

```
mfactElec
mfactMeter
mfactMod
```



See manufacturing commands starting on page 40

Input Contacts

Input contacts provide a means for an external stimulus to generate an alarm. The input contact commands are:

```
icStatus
icTarget
icName
icLoc
icNormal
icStatus
icAlarm
icSeverity
```

Output Relays

The output relays provide a means to generate an external signal based on predetermined conditions. The signal can be generated based on power distribution modules, subfeeds and/or system voltage and current thresholds and frequency deviation and input contacts. This functionality is more intuitive to configure on the web interface.
Output relay configuration and status commands:

```
orName
orNormal
orStatus
orTarget
```

Output relay excitation control commands:

```
orBrkrMxI
orBrkrHiI
orBrkrLoI
orBrkrMnI
orBrkrPos
orSub1MxI
orSub1HiI
orSub1LoI
```

```
orSub1MnI
orSub1Brkr
orSub2MxI
orSub2HiI
orSub2LoI
orSub2MnI
orSub2Brkr
orSysFreq
orSysMxI
orSysHiI
orSysLoI
orSysMnI
orSysMxV
orSysHiV
orSysLoV
orSysMnV
orIC1Alrm
orIC2Alrm
orIC3Alrm
orIC4Alrm
```

sysOutput

Access: Administrator, Device

Description: View each phase-to-phase voltage, each phase-to-neutral voltage, load supported by each phase and the frequency. Output measurements are made at the transformer.

Example:

```
apc> sysOutput
1. L1-L2,415, L2-L3,413V, L3-L1,415V
2. L1,244V, 0A, 0kW, L2,243V, 0A,0kW, L3,244V,0A,0kW
3. 60.0 Hz
```

sysAlrmCfg

Access: Administrator, Device

Description: View the configuration of the system alarm thresholds. Display order:

- Maximum output voltage threshold and enable
- High output voltage threshold and enable
- Low output voltage threshold and enable
- Minimum output voltage threshold and enable
- Maximum current threshold and enable
- High current threshold and enable
- Low current threshold and enable
- Minimum current threshold and enable
- Frequency Deviation enable

Example:

```
apc> sysAlrmCfg
1.MaxV,+20% ,Disable,HiV,+12%,Disable,LoV,-12%,Disable,MinV,-20%,Disable
2.MaxA,0%,Disable,HiA,0%,Disable,LoA,0%,Disable,MinA,0%,Disable,Freq,Disable
```

sysThrMxV

Access: Administrator, Device

Description: Configure the maximum voltage (L-N) alarm threshold and enable corresponding critical alarm. Parameters: [<fraction>] [<enable|disable>]
Fraction = percent above device nominal voltage.

Example:

```
apc> sysAlrmCfg
1.MaxV,+20% ,Disable,HiV,+12%,Disable,LoV,-12%,Disable,MinV,-20%,Disable
2.MaxA,0%,Disable,HiA,0%,Disable,LoA,0%,Disable,MinA,0%,Disable,Freq,Disable

apc> sysThrMxV 25 Enable
1.25%,Enable

apc> sysAlrmCfg
1.MaxV,25% ,Enable,HiV, +12%,Disable,LoV,-12%,Disable,MinV,-20%,Disable
2.MaxA,90%,Disable,HiA,80%,Disable,LoA,0%,Disable,MinA,0%,Disable,Freq,Disable
```

sysThrHiV

Access: Administrator, Device

Description: Configure the high voltage (L-N) alarm threshold and enable a corresponding warning alarm. Note the status version of the command. Parameters: [<fraction>] [<enable|disable>]
Fraction = percent above device nominal voltage.

Example:

```
apc> sysThrHiV
1.12%,Disable

apc> sysThrHiV 15 Enable
1.15%,Disable

apc> sysThrHiV
E000: Success
1. 15%,Enable
```

sysThrLoV

Access: Administrator, Device

Description: Configure the low voltage (L-N) alarm threshold and enable a corresponding warning alarm. The minus sign is implied, not expressed. Parameters: [<fraction>] [<enable|disable>]
Fraction = percent below device nominal voltage.

Example:

```
apc> sysThrLoV
1.-12%,Disable

apc> sysThrLoV 15 Enable
1.-15%,Disable

apc> sysThrLoV
1.-15%,Enable
```

sysThrMnV

Access: Administrator, Device

Description: Configure the minimum voltage (L-N) alarm threshold and enable a corresponding critical alarm. The minus sign is implied, not expressed. Parameters: [<fraction>] [<enable|disable>]
Fraction = percent below device nominal voltage.

Example:

```
apc> sysThrMnV
1.-20%,Disable

apc> sysThrMnV Enable
1.-20%,Enable

apc> sysThrMnV
1.-20%,Enable
```

sysThrMxI

Access: Administrator, Device

Description: Configure the maximum current alarm threshold and enable a corresponding critical alarm. Parameters: [<fraction>] [<enable|disable>]
Fraction = percent of rated current.

Example:

```
apc> sysThrMxI
1.0%,Disable

apc> sysThrMxI 90 Enable
1.90%,Enable

apc> sysThrMxI
1.90%,Enable
```

sysThrHiI

Access: Administrator, Device

Description: Configure the high current alarm threshold and enable a corresponding warning alarm.
Parameters: [<fraction>] [<enable|disable>]
Fraction = percent of rated current.

Example:

```
apc> sysThrHiI
1.0%,Disable

apc> sysThrHiI 80 Enable
1.80%,Enable

apc> sysThrHiI
1.80%,Enable
```

sysThrLoI

Access: Administrator, Device

Description: Configure the low current alarm threshold and enable a corresponding warning alarm.
Parameters: [<fraction>] [<enable|disable>]
Fraction = percent of rated current.

Example:

```
apc> sysThrLoI
1.0%,Disable

apc> sysThrLoI 30 Enable
1.30%,Enable

apc> sysThrLoI
1.30%,Enable
```

sysThrMnI

Access: Administrator, Device

Description: Configure the low current alarm threshold and enable a corresponding warning alarm.
Parameters: [<fraction>] [<enable|disable>]
Fraction = percent of rated current.

Example:

```
apc> sysAlrmCfg
1.0%,Disable

apc> sysThrMnI 10 Enable
1.10%,Enable

apc> sysAlrmCfg
1.10%,Enable
```

sysFreqDev

Access: Administrator, Device

Description: Configure the frequency deviation threshold and enable a corresponding warning alarm. Input is either a deviation value or disable.
Parameters: [<Deviation >]
Deviation = disable,0.2, 0.5, 1.0, 1.5, 20.,3.0, 4.0, 5.0, 9.0 Hz

Example:

```
apc> sysAlrmCfg
1.MaxV,+25% ,Enable,HiV, +15%,Enable,LoV,-15%,Enable,MinV,-25%,Enable
2.MaxA,90%,Enable,HiA,80%,Enable,LoA,30%,Enable,MinA,10%,Enable,Freq,Disable

apc> sysFreqDev 1.0
1.1.0

apc> sysAlrmCfg
1.MaxV,+25% ,Enable,HiV, +15%,Enable,LoV,-15%,Eable,MinV,-25%,Enable
2.MaxA,90%,Enable,HiA,80%,Enable,LoA30%,Enable,MinA,10%,Enable,Freq,1.0,Enable
```

subfdStatus

Access: Administrator, Device

Description: If no parameter is entered, the status of the subfeeds is displayed (name, alarm condition, power and location). If a parameter is entered, the alarm status, subfeed breaker position, breaker rating, energy usage and date last reset are displayed. Current, percent of capacity, power and current alarm per phase are also displayed.
Parameters: [<subfeed>]

Subfeed = 1 to number of subfeeds.
No parameter indicates all subfeeds and yields abbreviated status.

Example:

```
apc> subfdStatus
1.Subfeed 1,Normal,0.0kW,Sub Location 1
2.Subfeed 2,Normal,0.0kW,Sub Location 2
3.Subfeed 3,Normal,0.0kW,Sub Location 3
4.Subfeed 4,Normal,0.0kW,Sub Location 4

apc> subfdStatus 1
1.Normal,Open,160A,765kWh,10/27/2010
2.3A,0%,0.0kW,Low,0A,0%,0.0kW,Low,0A,0%,0.0kW,Low
```

subfdTarget

Access: Administrator, Device

Description: Selects a subfeed as the target for configuration and displays subfeed details: individual phase threshold values and threshold enables, as well as the subfeed breaker position, breaker alarm, breaker rating, energy usage and date last reset.
Parameters: [<subfeed>]
Subfeed = subfeed of interest. Default is 0, so parameter is required.

Example:

```
apc> subfdTarget 1
1.Enable,Enable,89%,Enable,72%,Enable,30%,Enable,20%,Disable
2.Open,Critical,160A,765kWh,10/27/2010
```

subfdName

Access: Administrator, Device

Description: Configure the name of the target subfeed.
Parameters: [<name>]
name = a string of up to 20 characters. Quotes are required if the string contains a space.

Example:

```
apc> subfdTarget 1
1.Enable,Enable,89%,Enable,72%,Enable,30%,Enable,20%,Disable
2.Open,Critical,160A,765kWh,10/27/2010

apc> subfdStatus
1.Subfeed 1,Normal,0.0kW,Sub Location 1
2.Subfeed 2,Normal,0.0kW,Sub Location 2
3.Subfeed 3,Normal,0.0kW,Sub Location 3
4.Subfeed 4,Normal,0.0kW,Sub Location 4

apc> subfdName "Newname 1"
Newname 1,Warning,0.0kW,Sub Location 1

apc> subfdStatus
1.Newname 1,Normal,0.0kW,Sub Location 1
2.Subfeed 2,Normal,0.0kW,Sub Location 2
3.Subfeed 3,Normal,0.0kW,Sub Location 3
4.Subfeed 4,Normal,0.0kW,Sub Location 4
```

subfdLoc

Access: Administrator, Device

Description: Configure the location of the targeted subfeed.
Parameters: [<location>]
location = a string of up to 20 characters

Example:

```
apc> subfdTarget 1
1.Enable,Enable,89%,Enable,72%,Enable,30%,Enable,20%,Disable
2.Open,Critical,160A,765kWh,10/27/2010

apc> subfdStatus
1.Newname 1,Normal,0.0kW,Sub Location 1
2.Subfeed 2,Normal,0.0kW,Sub Location 2
3.Subfeed 3,Normal,0.0kW,Sub Location 3
4.Subfeed 4,Normal,0.0kW,Sub Location 4

apc> subfdLoc "New  Location 1"
```

```
1.Newname 1,Normal,0.0kW,New  Location 1

apc> subfdStatus
1.Newname 1,Normal,0.0kW,New  Location 1
2.Subfeed 2,Normal,0.0kW,Sub Location 2
3.Subfeed 3,Normal,0.0kW,Sub Location 3
4.Subfeed 4,Normal,0.0kW,Sub Location 4
```

subfdAlarm

Access: Administrator, Device

Description: Enable or disable alarm generation by target subfeed.
Parameters: <enable|disable>

Example:

```
apc> subfdTarget 1
1.Enable,Enable,89%,Enable,72%,Enable,30%,Enable,20%,Disable
2.Open,Critical,160A,765kWh,10/27/2010

apc> subfdStatus 1
1.Normal,Open,160A,765kWh,10/27/2010
2.Enable,Enable,90%,Disable,70%,Disable,20%,Disable,10%,Disable

apc> subfdAlarm disable
1.Disable,Enable,90%,Disable,70%,Disable,20%,Disable,10%,Disable

apc> subfdStatus 1
1.Normal,Open,160A,765kWh,10/27/2010
2.Disable,Enable,90%,Disable,70%,Disable,20%,Disable,10%,Disable
```

subfdThrMx

Access: Administrator, Device

Description: Configure the maximum load alarm threshold and critical alarm for target subfeed.
Parameters: [[<thresh>] [<enable|disable>]]
Thresh = % rated load

Example:

```
apc> subfdStatus 1
1. Normal,Open,160A,765kWh,10/27/2010
2. Disable,Enable,90%,Disable,70%,Disable,20%,Disable,10%,Disable

apc> subfdThrMx 95 enable
1.Disable,Enable,95%,Enable,70%,Disable,20%,Disable,10%,Disable

apc> subfdStatus 1
1. Normal,Open,160A,765kWh,10/27/2010
2. Disable,Enable,95%,Enable,70%,Disable,20%,Disable,10%,Disable
```

subfdThrHi

Access: Administrator, Device

Description: Configure the high load alarm threshold and warning alarm for the target subfeed.
Parameters: [[<thresh>] [<enable|disable>]]
Thresh = % rated load

Example:

```
apc> subfdStatus 1
1. Normal,Open,160A,765kWh,10/27/2010
2. Disable,Enable,95%,Enable,70%,Disable,20%,Disable,10%,Disable

apc> subfdThrHi 75 enable
1.Disable,Enable,95%,Enable,75%,Enable,20%,Disable,10%,Disable

apc> subfdStatus 1
1. Normal,Open,160A,765kWh,10/27/2010
2. Disable,Enable,95%,Enable,75%,Enable,20%,Disable,10%,Disable
```

subfdThrLo

Access: Administrator, Device

Description: Configure the low load alarm threshold and warning alarm for the target subfeed.
Parameters: [[<thresh>] [<enable|disable>]]
Thresh = % rated load

Example:

```
apc> subfdStatus 1
1. Normal,Open,160A,765kWh,10/27/2010
2. Disable,Enable,95%,Enable,75%,Enable,20%,Disable,10%,Disable

apc> subfdThrLo 25 enable
1.Disable,Enable,95%,Enable,75%,Enable,25%,Enable,10%,Disable

apc> subfdStatus 1
1. Normal,Open,160A,765kWh,10/27/2010
2. Disable,Enable,95%,Enable,75%,Enable,25%,Enable,10%,Disable
```

subfdThrMn

Access: Administrator, Device

Description: Configure the minimum load alarm threshold and critical alarm for target subfeed.
Parameters: [[<thresh>] [<enable|disable>]]
Thresh = % rated load

Example:

```
apc> subfdStatus 1
1. Normal,Open,160A,765kWh,10/27/2010
2. Disable,Enable,95%,Enable,75%,Enable,25%,Enable,10%,Disable
```

```
apc> subfdThrMn 5 enable
1.Disable,Enable,95%,Enable,75%,Enable,25%,Enable,5%,Enable

apc> subfdStatus 1
1. Normal,Open,160A,765kWh,10/27/2010
2. Disable,Enable,95%,Enable,75%,Enable,25%,Enable,5%,Enable
```

subfdBrkr

Access: Administrator, Device

Description: Configure the breaker position critical alarm for the target subfeed.
Parameters: [<enable|disable>]

Example:

```
apc> subfdStatus 1
1. Normal,Open,160A,765kWh,10/27/2010
2. Disable,Enable,95%,Enable,75%,Enable,25%,Enable,5%,Enable

apc> subfdBrkr disable
1.Disable,Disable,95%,Enable,75%,Enable,25%,Enable,5%,Enable

apc> subfdStatus 1
1. Normal,Open,160A,765kWh,10/27/2010
2. Disable,Disable,95%,Enable,75%,Enable,25%,Enable,5%,Enable
```

subfdRstkWh

Access: Administrator, Device

Description: Reset the usage and usage date for the target subfeed.

Example:

```
apc> subfdStatus 1
1. Normal,Open,160A,765kWh,10/27/2010
2. Disable,Disable,95%,Enable,75%,Enable,25%,Enable,5%,Enable

apc> subfdRstkWh
1.Normal,Open,160A,0kWh,12/27/2010

apc> subfdStatus 1
1. Normal,Open,160A,0kWh,12/27/2010
2. Disable,Disable,95%,Enable,75%,Enable,25%,Enable,5%,Enable
```

modStatus

Access: Administrator, Device

Description: Displays module number, status, each breaker rating, load name, each breaker current and module power. If no module number is input, the status for modules that are populated will be displayed. Refer to the module definition table for breaker details.
Parameters: [<module>]
Module=module # of interest

Example:

```
apc> modStatus 1
1.1,Normal,20A,20A,20A,Closed,Closed,Closed,Circuit 1A,0.0A,0.0A,0.0A,0.00kW

apc> modStatus 3
1.3,Normal,50A,Closed,Circuit 3A, 0.0A, 0.0A, 0.0A,0.00kW   (single 3-pole)
```

modTarget

Access: Administrator, Device

Description: Select the module to be configured. By selecting a single target for configuration, there is no module number in each of the commands configuring one of the attached cables.
Parameters: [<module>]
Module=module # of interest

Example:

```
apc> modTarget 2
1.2,Normal,20A,20A,20A,Closed,Closed,Closed,Circuit 1A,0.0A,0.0A,0.0A,0.00kW
```

cblTarget

Access: Administrator, Device

Description: Select the cable on the target module to be configured. By selecting a single target for configuration, there is no need to insert the cable number in each of the commands configuring the desired cable.
When a cable is targeted, the name, location, alarm status, total power, energy usage, usage reset date, alarm enable and threshold configurations are displayed in the order of maximum current, high current, low current and minimum current.
Parameters: <cable>
cable=cable # of interest(normally 1|2|3)

Example:

```
apc> cblTarget 1
1.Circuit 2b,Ckt Location 2b,Normal,20A,Closed,2.6A,0.28kW,21.0kWh,05/05/2011

apc> cblTarget 3
1.Circuit 2b,Ckt Location 2b,Normal,20A,Closed,2.6A,0.28kW,21.0kWh,05/05/2011
```

cblStatus

Access: Administrator, Device

Description: Displays the cable parameters (name, location, alarm status, total power, energy usage, usage reset date, alarm generation enable and threshold configurations) on the selected cable with the cblTarget command on the module selected by the modTarget command. Threshold order is maximum current and enable, high current and enable, low current and enable and minimum current and enable. The module and cable must be selected with the appropriate target commands.

Example:

```
apc> cblStatus
1.Circuit 1a,Ckt Location 1a,Normal,0.00kW,21.1kWh,10/27/2010,
2.Enable,Enable,90%,Enable, 80%,Enable,20%,Disable,10%,Disable
```

cblName

Access: Administrator, Device

Description: Configure the name of the cable selected by the cblTarget and modTarget commands.
Parameters: [<name>]
name = a string of up to 20 characters. Quotes are required if the string contains a space.

Example:

```
apc> cblStatus
1.Circuit 1b,Ckt Location 1b,Normal,20A,Closed,2.7A,0.29kW,9.6kWh,05/05/2011
2.Enable,Enable,90%,Disable,80%,Enable,20%,Disable,10%,Disable

apc> cblName "New 1b"
1.New 1b,Ckt Location 1b, Normal,20A,Closed,2.7A,0.29kW,9.6kWh
```

cblLoc

Access: Administrator, Device

Description: Configure the location of the selected cable.
Parameters: [<location>]
location = a string of up to 20 characters. Quotes are required if the string contains a space.

Example:

```
apc> cblStatus
1.New 1b,Ckt Location 1b,Normal,20A,Closed,2.7A,0.29kW,9.6kWh,05/05/2011
2.Enable,Enable,90%,Disable,80%,Enable,20%,Disable,10%,Disable

apc> cblLoc "New Loc 1b"
1.New 1b, New Loc 1b, Normal,20A,Closed,2.7A,0.29kW,9.6kWh
```

cblAlrm

Access: Administrator, Device

Description: Enables alarm generation on the selected cable.
Parameters: <switch>
switch=enable|disable

Example:

```
apc> cblAlrm enable
2.Enable,Enable,90%,Enable, 80%,Enable,20%,Disable,10%,Disable
```

cblThrMx

Access: Administrator, Device

Description: Configure the max load alarm threshold and critical alarm on the cable selected by the cblTarget and modTarget commands. Valid threshold values are 0-100% where ThrMx > ThrHi > ThrLo > ThrMn.
Parameters: [<thresh>] [<enable|disable>]
Thresh = % rated load

Example:

```
apc> cblStatus
1.Circuit 1a,Ckt Location 1a,Normal,0.00kW,21.1kWh,10/27/2010,
2.Enable,Enable,90%,Enable, 80%,Enable,20%,Disable,10%,Disable

apc> cblThrMx 85 enable
1.Circuit 1a,Ckt Location 1a,Normal,0.00kW,21.1kWh,10/27/2010,

apc> cblStatus
1.Circuit 1a,Ckt Location 1a,Normal,0.00kW,21.1kWh,10/27/2010,
2.Enable,Enable,90%,Enable, 80%,Enable,20%,Disable,10%,Disable
```

cblThrHi

Access: Administrator, Device

Description: Configure the high load alarm threshold and warning alarm on the cable selected by the cblTarget and modTarget commands. Valid threshold values are 0-100% where ThrMx > ThrHi > ThrLo > ThrMn.
Parameters: [<thresh>] [<enable|disable>]
Thresh = % rated load

Example:

```
apc> cblStatus
1.Circuit 1a,Ckt Location 1a,Normal,0.00kW,21.1kWh,10/27/2010,
2.Enable,Enable,90%,Enable, 80%,Enable,20%,Disable,10%,Disable

apc> cblThrHi 75 enable
1.Enable,Enable,90%,Enable, 75%,Enable,20%,Disable,10%,Disable

apc> cblStatus
1.Circuit 1a,Ckt Location 1a,Normal,0.00kW,21.1kWh,10/27/2010,
2.Enable,Enable,90%,Enable, 75%,Enable,20%,Disable,10%,Disable
```

cblThrLo

Access: Administrator, Device

Description: Configure the low load alarm threshold and warning alarm on the cable selected by the cblTarget and modTarget commands. Valid threshold values are 0-100% where ThrMx > ThrHi > ThrLo > ThrMn.
Parameters: [<thresh>] [<enable|disable>]
Thresh = % rated load

Example:

```
apc> cblStatus
1.Circuit 1a,Ckt Location 1a,Normal,0.00kW,21.1kWh,10/27/2010,
2.Enable,Enable,90%,Enable, 75%,Enable,20%,Disable,10%,Disable

apc> cblThrLo 45 enable
1.Enable,Enable,90%,Enable, 75%,Enable,45%,Enable,10%,Disable

apc> cblStatus
1.Circuit 1a,Ckt Location 1a,Normal,0.00kW,21.1kWh,10/27/2010
2.Enable,Enable,90%,Enable, 75%,Enable,45%,Enable,10%,Disable
```

cblThrMn

Access: Administrator, Device

Description: Configure the minimum load alarm threshold and critical alarm on the cable selected by the cblTarget and modTarget commands.
Parameters: [<thresh>] [<enable|disable>]
Thresh = % rated load

Example:

```
apc> cblStatus
1.Circuit 1a,Ckt Location 1a,Normal,0.00kW,21.1kWh,10/27/2010
2.Enable,Enable,90%,Enable, 75%,Enable,45%,Enable,10%,Disable

apc> cblThrMn 25 enable
1.Enable,Enable,90%,Enable, 75%,Enable,45%,Enable,25%,Enable

apc> cblStatus
1.Circuit 1a,Ckt Location 1a,Normal,0.00kW,21.1kWh,10/27/2010
2.Enable,Enable,90%,Enable, 75%,Enable,45%,Enable,25%,Enable
```

cblBrkrPos

Access: Administrator, Device

Description: Enables alarm generation on the cable selected by the cblTarget and modTarget commands.
Parameters: <switch>
switch=enable|disable

Example:

```
apc> cblBrkrPos enable
1.Enable,Enable,90%,Enable, 80%,Enable,20%,Disable,10%,Disable
```

cblRstkWh

Access: Administrator, Device

Description: Reset the usage and usage date on the cable selected by the cblTarget and modTarget commands.

Example:

```
apc> cblRstkWh
1.New 1b,Ckt Location 1b,Normal,20A,Closed,2.7A,0.3kW,0.0kWh,05/10/2011
```

mfactElec

Access: Administrator, Device

Description: Displays nominal line-to-neutral voltage, nominal frequency and maximum panel current for the 150kW Modular PDU.

Example:

```
apc> mfactElec
1.230v /4-Wire,60Hz,400A
```

mfactMeter

Access: Administrator, Device

Description: Displays model number, serial number, date of manufacture and firmware revision for each metering device in the Modular PDU.

Example:

```
apc> mfactMeter
1.0P2495,0524950601929504,12242009,00.98
2.0P2495,0524950602259176,04052010,00.98
3.0P2495,0524950602259175,04052010,00.98
4.0P2495,0524950902275872,04052010,00.98
```

mfactMod

Access: Administrator, Device

Description: If no parameter is entered, the model number, serial number, date of manufacture and number of attached cables for each module in the Modular PDU is displayed.
If a parameter is entered, the above information plus cable information, breaker rating, length, connector style and available voltage, for any cables attached to the module is displayed.
Parameters: [<module>]
Module = module number of interest.

Example:

```
apc> mfactMod
1.PDM3450IEC309-200,5F0938P00031,09172009,1
2.PDM3563IEC309-200,5F1003P00094 ,01192010,1
3.PDM2332IEC-3P30RCD-1, ED0123456789, 061708, 3
4.PDM332IEC-30R-1040 ,ED012345987, 061708,1
5.PDM3232IEC-0320 ,AB1243459990,05012007,1

apc> mfactMod 1
1.PDM3440IEC309-200,5F0938P00031,09172009,1
2.L1: 40A,L2:40A,L3:40A ,2.0m (6.6ft) ,IEC309-5w,230:400V
```

icStatus

Access: Administrator, Device

Description: Display input contact, alarm status, alarm severity, alarm enable, contact state and location of each input contact in the Modular PDU.

Example:

```
apc> icStatus
1.User Contact 1,Normal,Critical,Enable,Open,Location 1
2.User Contact 2,Normal,Warning,Enable,Open,Location 2
3.User Contact 3,Normal,Warning,Enable,Open,Location 3
4.User Contact 4,Normal,Warning,Enable,Open,Location 4
```

icTarget

Access: Administrator, Device

Description: Selects input contact for configuration.
Parameters: <contact>
Contact = input contact of interest.

Example:

```
apc> Target 1
1.User Contact 1,Normal,Critical,Enable,Open,Location 1
```

icName

Access: Administrator, Device

Description: Configure the name of the targeted input contact.
Parameters: <name>
name = character string of up to 20 characters.

Example:

```
apc> icStatus
1.New Contact 1,Normal,Critica,Enable,Open,Location 1
2.User Contact 2,Normal,Warning,Enable,Open,Location 2
3.User Contact 3,Normal,Warning,Enable,Open,Location 3
4.User Contact 4,Normal,Critical,Enable,Open,Location 4

apc> icName "New Contact 1"
1.New Contact 1,Normal,Critical,Enable,Open,Location 1

apc> icStatus
1.New Contact 1,Normal,Critical,Enable,Open,Location 1
2.User Contact 2,Normal,Warning,Enable,Open,Location 2
3.User Contact 3,Normal,Warning,Enable,Open,Location 3
4.User Contact 4,Normal,Critical,Enable,Open,Location 4
```

icLoc

Access: Administrator, Device

Description: Configure the location of the targeted input contact.
Parameters: <location>
location = character string of up to 20 characters.

Example:

```
apc> icStatus
1.New Contact 1,Normal,Critical,Enable,Open,Location 1
2.User Contact 2,Normal,Warning,Enable,Open,Location 2
3.User Contact 3,Normal,Warning,Enable,Open,Location 3
4.User Contact 4,Normal,Critical,Enable,Open,Location 4
```

```
apc> icLoc "Door Switch"
1.New Contact 1,Normal,Critical,Enable,Open,Door Switch

apc> icStatus
1.New Contact 1,Normal,Critical,Enable,Open,Door Switch
2.User Contact 2,Normal,Warning,Enable,Open,Location 2
3.User Contact 3,Normal,Warning,Enable,Open,Location 3
4.User Contact 4,Normal,Critical,Enable,Open,Location 4
```

icNormal

Access: Administrator, Device

Description: Configure the normal state of the targeted input contact. When the normal state and the physical state of the alarm are opposite, the contact will generate an alarm.
Parameters: <normal state>
Normal state = open|closed.

Example:

```
apc> icStatus
1.New Contact 1,Normal,Critical,Enable,Open,Door Switch
2.User Contact 2,Normal,Warning,Enable,Open,Location 2
3.User Contact 3,Normal,Warning,Enable,Open,Location 3
4.User Contact 4,Normal,Critical,Enable,Open,Location 4

apc> icNormal closed  //reversing the normal generates an alarm
1.New Contact 1,Critical,Critical,Enable,Open,Door Switch

apc> icStatus
1.New Contact 1,Critical,Critical,Enable,Open,Door Switch
2.User Contact 2,Normal,Warning,Enable,Open,Location 2
3.User Contact 3,Normal,Warning,Enable,Open,Location 3
4.User Contact 4,Normal,Critical,Enable,Open,Location 4
```

icAlarm

Access: Administrator, Device

Description: Enable/disable alarm of the targeted input contact.
Parameters: <alarm>
alarm = enable|disable

Example:

```
apc> icStatus
1.New Contact 1,Critical,Critical,Open,Door Switch
2.User Contact 2,Normal,Warning,Open,Location 2
3.User Contact 3,Normal,Warning,Open,Location 3
4.User Contact 4,Normal,Critical,Open,Location 4

apc> icAlarm disable //disabling clears the alarm
1.New Contact 1,Normal,Critical,Closed,Door Switch
```

```
apc> icStatus
1.New Contact 1,Normal,Critical,Closed,Door Switch
2.User Contact 2,Normal,Warning,Open,Location 2
3.User Contact 3,Normal,Warning,Open,Location 3
4.User Contact 4,Normal,Critical,Open,Location 4
```

icSeverity

Access: Administrator, Device

Description: Enable/disable alarm of the targeted input contact.
Parameters: <severity>
alarm = critical|warning

Example:

```
apc> icStatus
1.New Contact 1,Critical,Critical,Open,Door Switch
2.User Contact 2,Normal,Warning,Open,Location 2
3.User Contact 3,Normal,Warning,Open,Location 3
4.User Contact 4,Normal,Critical,Open,Location 4

apc> icSeverity warning
1.New Contact 1,Normal,Warning,Closed,Door Switch

apc> icStatus
1.New Contact 1,Normal,Warning,Closed,Door Switch
2.User Contact 2,Normal,Warning,Open,Location 2
3.User Contact 3,Normal,Warning,Open,Location 3
4.User Contact 4,Normal,Critical,Open,Location 4
```

orStatus

Access: Administrator, Device

Description: Display the output relay name and the state of each output relay in the Modular PDU.

Example:

```
apc> orStatus
1.Output Relay 1,Closed
2.Output Relay 2,Closed
3.Output Relay 3,Closed
4.Output Relay 4,Closed
```

orTarget

Access: Administrator, Device

Description: Select the output relay to configure.
Parameters: [relay]
relay = output relay of interest(normally 1|2|3|4).

Example:

```
apc> orTarget 1
1.Output Relay 1,Closed
```

orName

Access: Administrator, Device

Description: Configure the name of the targeted output relay.
Parameters: [name]
name = character string of up to 20 characters.

Example:

```
apc> orStatus
1.Output Relay 1,Closed
2.Output Relay 2,Closed
3.Output Relay 3,Closed
4.Output Relay 4,Closed

apc> orName "New Relay  1"
1.New Relay 1,Closed

apc> orStatus
1.New Relay 1,Closed
2.Output Relay 2,Closed
3.Output Relay 3,Closed
4.Output Relay 4,Closed
```

orNormal

Access: Administrator, Device

Description: Configure the normal state of the targeted output relay. The output relay will remain in the normal state until a condition occurs that causes the output relay to change to the state opposite the normal state.
Parameters: <normal state>
normal state = open|closed.

Example:

```
apc> orTarget 1
1.Output Relay 1,Closed

cli>orStatus
1.Output Relay 1,Closed
2.Output Relay 2,Closed
3.Output Relay 3,Closed
4.Output Relay 4,Closed

apc> orNormal open
1.Output Relay 1,Open

apc> orStatus
1.Output Relay 1,Open
2.Output Relay 2,Closed
3.Output Relay 3,Closed
4.Output Relay 4,Closed
```

Output Relay to Module Alarm Association

orBrkrxxx

Access: Administrator, Device

Description: This category of alarm mapping commands associates any module threshold alarm with the output relay/relays designated in the parameters.
With no parameter, display the currently associated output relays.

Output relay power distribution breaker alarm association commands:

```
orBrkrMxI
orBrkrHiI
orBrkrLoI
orBrkrMnI
orBrkrPos
```

Parameters: [<relay> <enable|disable>]
relay = output relay to be triggered(normally 1|2|3|4).

Example:

```
apc> orpdBrkrPos
1.Breaker Modules,Breaker Position,1,disable,2,disable,3,disable,4,disable

apc> orpdBrkrPos 2 enable
1.BreakerModules,Breaker Position,1,disable,2,enable,3,disable,4,disable

apc> orpdBrkrPos
1.Breaker Module,Breaker Position,1,disable,2,enable,3,disable,4,disable
```

Output Relay to Subfeed Alarm Association

orSubxxxx

Access: Administrator, Device

Description: This category of alarm mapping commands associates a subfeed threshold alarm with the output relay/relays designated in the parameters. With no parameter, display the current associated relays.

Subfeed alarm association commands:

```
orSub1MxI
orSub1HiI
orSub1LoI
orSub1MnI
orSub1Brk
orSub2MxI
orSub2HiI
orSub2LoI
orSub2MnI
orSub2Brkr
```

Parameters: [<relay> <enable|disable>]
relay = output relay to be triggered(normally 1|2|3|4).

Example:

```
apc> orSub1Brkr
1.Subfeed 1Breaker Position,1,disable,2,disable,3,disable,4,disable

apc> orSub1Brkr 3 enable
1.Subfeed 1 Breaker Position,1,disable,2,disable,3,enable,4,disable

apc> orpdBrkrPosition
1.Subfeed 1 Breaker Position,1,disable,2,disable,3,enable,4,disable
```

Output Relay to System Alarm Association

orSysxxxxx

Access: Administrator, Device

Description: This category of alarm mapping commands associates a system output threshold alarm with the output relay/relays designated in the parameters. With no parameter, display the current associated relays.

System output alarm association commands:

```
orSysFreq
orSysMxI
orSysHiI
orSysLoI
orSysMnI
orSysMxV
orSysHiV
orSysLoV
orSysMnV
```

Parameters: [<relay> <enable|disable>]
relay = output relay to be triggered(normally 1|2|3|4).

Example:

```
apc> orSysFreq
1.System Frequency,1,disable,2,disable,3,disable,4,disable

apc> orSysFreq 4 enable
1.Subfeed 1 Breaker Position,1,disable,2,disable,3,disable,4,enable
```

Output Relay to Input Contact Alarm Association

orICxxxxx

Access: Administrator, Device

Description: This category of alarm mapping commands associates an input contact alarm with the output relay/relays designated in the parameters. With no parameter, display the current associated relays.

Subfeed alarm association commands:

```
orIC1Alrm
orIC2Alrm
orIC3Alrm
orIC4Alrm
```

Parameters: [<relay> <enable|disable>]
relay = output relay to be triggered(normally 1|2|3|4).

Example:

```
apc> orIC2Alrm
1.Input Contact 2,1,disable,2,disable,3,disable,4,disable

apc> orIC2Alrm 4 enable
1.Input Contact 2,1,disable,2,disable,3,disable,4,enable
```

Web Interface

Introduction

Supported Web browsers

You can use Microsoft® Internet Explorer (IE) 7.x and higher (on Windows operating systems only) or Mozilla Firefox 3.0.6 or higher (on all operating systems) to access the Modular PDU through its Web interface. Other commonly available browsers may work but have not been fully tested by APC.

The Modular PDU cannot work with a proxy server. Therefore, before you can use a Web browser to access its Web interface, you must do one of the following:

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

Log On

Overview

You can use the DNS name or System IP address of the Modular PDU for the URL address of the Web interface. Use your case-sensitive user name and password to log on. The default user name differs by account type:

- **apc** for an Administrator
- **device** for a Device user
- **readonly** for a Read-Only user

The default password is **apc** for all three account types.

Note: If you are using HTTPS (SSL/TSL) as your access protocol, your logon credentials are compared with information in a server certificate. If the certificate was created with the APC 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 Modular PDU. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

URL address formats

Type the DNS name or IP address of the Modular PDU in the URL address field of the Web browser 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
“You are not authorized to view this page” or “Someone is currently logged in...”	Internet Explorer, Firefox	Someone else is logged on.
“This page cannot be displayed.”	Internet Explorer	Web access is disabled, or the URL was not correct
“Unable to connect.”	Firefox	

URL format examples.

- For a DNS name of Web1:
  - `http://Web1` if HTTP is your access mode
  - `https://Web1` if HTTPS (HTTP with SSL) 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) 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) is your access mode.

Home Page

Overview

On the **Home** tab, displayed when you log on to the Web interface, you can view active alarm conditions and the most recent events recorded in the event log.

Quick status icons. At the upper right corner of every page, one or more icons indicate the current operating status of the Modular PDU and the number of active alarms of that severity:

Icon	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 Present:** The Modular PDU is operating normally.

Active alarms. The **Power Distribution** section of the **Home** page summarizes the status of the Modular PDU:

- The **No Alarms Present** icon displays if no alarms exist.
- One or both of the other icons (**Critical** and **Warning**) display if any alarms exist, and after each icon, the number of active alarms of that severity.
- The input and output voltages, the supported load, and the active power provided for each phase.
- The bypass voltages, if your Modular PDU model includes a Bypass Input Switch

Note: Click a quick status icon on any page of the interface to return to the **Home**.

Recent System Events. The **Recent System Events** section displays, in reverse chronological order, the events that occurred most recently and the dates and times they occurred. Click **More Events** to view the entire event log.

How to Use the Tabs, Menus, and Links

Tabs

In addition to the tab for the **Home** page, the following tabs are displayed. Click a tab to display a set of menu options:

- **Power Distribution**: View the power output of the Modular PDU and its breakers, and configure alarm thresholds.
- **Contacts/Relays**: Configure the name and normal state of the Modular PDU's input contacts and output relays.
- **Alarms**: View active alarms and recent events, and configure how the relays will respond to Modular PDU alarms.
- **Logs**: View and configure event and data logs.
- **Administration**: Configure security, network connection, notification, and general settings.

Menus

Left navigation menu. Each tab (except the tab for the home page) has a left navigation menu, consisting of headings and options:

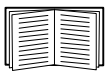
- If a heading has indented option names below it, the heading itself is not a navigational link. Click an option to display or configure parameters.
- If a heading has no indented option names, the heading itself is the navigational link. Click the heading to display or configure parameters.

Top menu bar. The **Administration** and **Power Distribution** tabs have a selection of menu options on the top menu bar. Select one of the menu options to display its left navigation menu.

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 Web site
- **Link 2**: Demonstrations of APC Web-enabled products.
- **Link 3**: Information on APC Remote Monitoring Services.



To reconfigure the links, see "Configuring Links".

Monitor and Configure the Modular PDU

The **Power Distribution** tab has two top menu bar options, **Main Modular PDU** and **Branch Circuits**, which provide system performance information and configuration options.

View Modular PDU Information

Access detailed Modular PDU status information

View output measurements.

Path: Power Distribution > Main Modular PDU > Modular PDU Monitoring > panel output

The first time you select the **Power Distribution** tab, then **Main Modular PDU** from the top menu bar, the **Modular PDU Monitoring > panel output** page displays. If an alarm caused by an output power condition exists, a status icon and accompanying text display at the top of the page.

The **Output Measurements** section lists detailed information about power leaving the Modular PDU:

- Voltage: The phase-to-phase output voltage (e.g., L1-2 for phase L1 to phase L2) for a 3-wire connection, or the phase-to-neutral output voltage (e.g., L1 for phase 1 to neutral) for a 4-wire connection.
- Current: The load supported by each phase, in RMS current (Irms).
- Power: The active power, in kW, provided for each phase and for the total of the three phases.
- Apparent Power: The apparent power, in kVA, provided for each phase and for the total of the three phases.
- Power Factor: The ratio between active power and apparent power (kW/kVA). This ratio affects the power available to the load.
- Frequency: The frequency, in Hz, of the output.

View input measurements.

Path: Power Distribution > Main Modular PDU > Modular PDU Monitoring > main input

If an alarm caused by an input power condition exists, a status icon and accompanying text display at the top of the **Modular PDU Monitoring > main input** page.

The **Input Measurements** section lists detailed information about the power entering the Modular PDU:

- Main Input Breaker: The status of the main input breaker at the Modular PDU, open or closed. When the Modular PDU is operating normally, this breaker is closed.
- Main Voltage: The phase-to-phase input voltage (e.g., L1-2 for phase L1 to phase L2) for a 3-wire connection, or the phase-to-neutral input voltage (e.g., L1 for phase 1 to neutral) for a 4-wire connection.
- Bypass Voltage (Modular PDU models with a Bypass Input Switch only): The phase-to-phase and phase-to-neutral voltages

View breaker status

Breaker status icons. Color-coded breaker icons show the status of the system breakers:

- Red: The breaker position is causing one or more critical alarms.
- Yellow: The breaker position is causing one or more warning alarms.
- Gray: The breaker position is not influencing the status of the Modular PDU.
- Green: The Modular PDU is operating normally.

View the status of the input breakers.

Path: Power Distribution > Main Modular PDU > Modular PDU Breakers > input breakers

If an alarm caused by the breaker position exists, a status icon and accompanying text display at the top of the **Modular PDU Breakers** > **input breakers** page.

- Main Input Breaker: When the Modular PDU is operating normally, this breaker is closed.
- Cross Tie Breaker: When the Modular PDU is operating normally, this breaker is closed.

View hardware information and electrical ratings

Path: Power Distribution > Main Modular PDU > Modular PDU Info

The **Electrical Configuration** section of the page lists the electrical hardware in your Modular PDU.

- Input Voltage: The nominal input voltage that the Modular PDU Main Input Switch receives, and the type of electrical connection used by the Modular PDU Main Input Switch. (3-wire connections are measured phase-to-phase; 4-wire connections are measured phase-to-neutral.)
- Input Transformer: Indicates whether the Modular PDU has an input transformer.
- Main Breaker Rating: The rating, in amps, of the breaker supplying power to the Modular PDU.
- Output Voltage: The configured nominal output voltage that is supporting the load.
- Panel Breaker Rating: The rating, in amps, of the breaker supplying power to the distribution circuit breaker panels.
- Maximum System Power: The maximum amount of power, in kW, that the Modular PDU can supply to the load.

The **Installed Options** section defines whether the following components are installed in the Modular PDU. The availability of these components varies by Modular PDU model.

- Cooling Fans: Fans that cool the transformer.
- Load Test Port: A port that enables you to test whether the Modular PDU can support the load.

The **Power Metering** section specifies the version number of the metering firmware module.

Configure Modular PDU Settings

Configure alarm thresholds

Path: Power Distribution > Main Modular PDU > Modular PDU Monitoring > alarm setup

The **Modular PDU Monitoring** > **alarm setup** page displays the configurable low and high alarm thresholds for these measurements:

- Input Voltage L-L: The acceptable range for the voltage entering the Modular PDU.
- Bypass Voltage L-N: The acceptable range for bypass voltage.
- Output Voltage L-N: The acceptable range for the voltage that the Modular PDU provides to the load.
- Output Current: The acceptable range for the output current. The Modular PDU monitors the output current on each phase, and a threshold violation on any phase generates an alarm.
- High Neutral Current: The acceptable range for the current on the output neutral line.
- Frequency: The acceptable frequency variation for the output current, in Hertz.

For each measurement, a value below the **Low** threshold or above the **High** threshold generates an alarm.

Click **Input Thresholds** to define the acceptable range for input voltage: The default values are:

- Low threshold: –30% of the expected input voltage
- High threshold: +30% of the expected input voltage

Click **Output Thresholds** to define the acceptable output ranges. The default values are:

- Output voltage threshold: +/–12%
- High output current threshold: 80%
- Low output current threshold: Disabled
- High neutral current: 80%
- Acceptable frequency range: +/–5 Hertz

Add a branch breaker or sub-feed breaker

Path: Power Distribution > Branch Circuits > Configuration > add breakers *or* add sub-feed

In the **Breaker Details** section of the **Configuration** > **add breakers** page, or the **Sub-Feed Breaker Details** section of the **Configuration** > **sub-feed** page, define these settings:

- Panel Position:
  - To add a branch breaker, enter the position number. The value is listed on the circuit breaker panel.
  - To add a sub-feed breaker, select the three numbers that match its sub-feed position. These values are listed on the breaker panel.
- Number of Poles: Select the number of poles in the breaker.
  - For a branch breaker, valid values are 1-pole, 2-pole, or 3-pole. Select the value that matches the type of load (1-phase, 2-phase, or 3-phase) that is receiving power.
  - For sub-feed breakers, 3-pole is the only valid value.
- Breaker Rating: Set the rating of this breaker, in Amps.

In the **Breaker Identification** section, type a descriptive name and location (up to 19 characters each) for the breaker.

In the **Branch Current Thresholds** section, mark the **Enable** check box to generate an alarm when the electric current violates a threshold, or clear the check box to disable alarms. Define each threshold as a percentage of the rated current.

When the configuration is complete, click **Add Branch Breaker** (or **Add Sub-Feed**, if you are configuring a sub-feed breaker) to apply your changes.

View and edit branch circuit breaker settings

Path: Power Distribution > Branch Circuits > Panel Status

Select a group of circuit breakers (**01..41 [odd]**, **02..42 [even]**, **43..83 [odd]**, or **44..84 [even])** to view the following data:

- Pos: The position of the breaker on the circuit breaker panel.
- Rating: The rating of the breaker occupying this panel position, in amps.
- Status: The state of the breaker.
  - Normal: The breaker is operating normally.
  - Warning: The low or high rating threshold has been violated.
  - Critical: The minimum or maximum rating threshold has been violated.
- Name: A descriptive name for the breaker.
- Current: The measured root mean square (RMS) current of the panel position.
- Location: A user-configured description of the location of the branch breaker (for example, the phsyical location of the Modular PDU in which it is installed)

To edit the name, location, or rating of a branch circuit breaker, select the text to modify. In the configuration page that opens, type your changes in the text field and click **Apply**.

To edit threshold settings for a branch circuit breaker, select its name, then select **Percent Rating**. Mark or clear the check box for each threshold to define whether that threshold will generate breaker alarms. Define each threshold as a percentage of the rated current, then click **Apply**.

To delete a breaker or group, click **Delete Group**.

Apply configuration changes to all branch circuit breaker settings

Apply threshold setting changes to all branch breakers.

Path: Power Distribution > Branch Circuits > Configuration > global thresholds

1. Mark the **Apply** check box that is associated with a threshold to apply this configuration to all of the branch breakers, or clear the **Apply** check box to prevent this setting from overwriting an existing threshold configuration.
2. Define the maximum, high, low, and minimum thresholds as a percentage of the rated current.
3. Click **Apply to All Checked** to save your changes.

Delete all branch breaker settings.

Path: Power Distribution > Branch Circuits > Configuration > global delete

1. To delete the branch breaker panel settings for a range of breakers, mark its **Delete** check box. To retain the settings for a range of breakers, clear its check box.
2. Click **Delete All Checked** to apply your changes.

Configure Contacts and Relays

View and configure input contact settings

Path: Contacts/Relays > Input Contacts

The first time you select the **Contacts/Relays** tab, the **Input Contacts** page displays. View the name of each input contact, its alarm status, and its current state. Up to four inputs can be connected to the Modular PDU.

Click the name of the input to configure a descriptive name (up to 14 characters) and to define its normal state. An alarm will be generated when the input switches to the abnormal state. Click **Apply** to save your changes.

Configure output relays

Path: Contacts/Relays > Output Relays

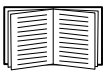
The **Output Relays** page displays the name and state of each relay. The Modular PDU has four relays.

Click the name of the relay to configure a descriptive name (up to 14 characters) and to define its normal state.

Monitor and Map Alarms

View active alarms

By default, the first time you click the **Alarms** tab, the **Active Alarms** page displays a list of active critical and warning alarms that affect the performance of the Modular PDU.



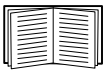
To view a complete event log, see “Logs”.

Configure the alarm relay map

Select the **Alarms** tab and then **Alarm Relay Map** to view a list of actions that can cause the relay to change its state.

To configure a relay to react to an alarm condition, mark the check box that corresponds to the alarm condition and the relay:

- Any Load: Change the state of the relay when an over-current or under-current alarm is detected for a circuit breaker panel or branch circuit.
- Overload: An over-current alarm is detected for a circuit breaker panel, branch circuit, or system ground.
- Input Voltage: An input voltage alarm is active.
- Output Voltage: An output voltage alarm is active.
- Contact 1–4 Alarms: The input is not in its normal state.



To configure the normal state of a relay, see “Configure output relays”.

Logs

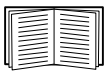
Use the Event and Data Logs

Event log

Path: Logs > Events > *options*

You can view, filter, or delete the event log. By default, the log displays all events recorded during the last two days, in reverse chronological order.

For lists of all configurable events and their current configuration, select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.

 For information about configuring event actions, see “Configuring by event”.

To display the event log (Logs > Events > log):

- By default, view the event log as a page of the Web interface.
- To see the listed events on one page, click **Launch Log in New Window** from the event log page to display a full-screen view of the log.

Note: In your browser's options, JavaScript® must be enabled for you to use the **Launch Log in New Window** button.
You can also use FTP or SCP to view the event log. See “Using FTP or SCP to retrieve log files”.

To filter the log (Logs > Events > log):

- **Filter the log by date or time:** To display the entire event log, or to change the number of days or weeks for which the log displays the most recent events, select **Last**. Select a time range from the drop-down menu, then click **Apply**. The filter configuration is saved until the Modular PDU restarts.
  To display events logged during a specific time range, select **From**. Specify the beginning and ending times (using the 24-hour clock format) and dates for which to display events, then click **Apply**. The filter configuration is saved until the Modular PDU restarts.
- **Filter the log by event**: To specify the events that display in the log, click **Filter Log**. Clear the check box of an event category or alarm severity level to remove it from view. Text at the upper right corner of the event log page indicates that a filter is active.
  As Administrator, click **Save As Default** to save this filter as the default log view for all users. If you do not click **Save As Default**, the filter is active until you clear it or until the Modular PDU restarts.
- To remove an active filter, click **Filter Log**, then **Clear Filter (Show All)**.

Note: Events are processed through the filter using **OR** logic.

- Events that are not selected from the **Filter By Severity** list never display in the filtered event log, even if the event occurs in a selected category from the **Filter by Category** list.
- Events that are not selected from the **Filter by Category** list never display in the filtered event log, even if devices in the category enter an alarm state selected from the **Filter by Severity** list.

To disable the logging of events based on their assigned severity level or their event category, see “Configuring by group”.

To delete the log (Logs > Events > log):

- When the log is full, the older entries are deleted.
- To delete all events recorded in the log, click **Clear Log** on the Web page that displays the log. Deleted events cannot be retrieved.

To configure reverse lookup (Logs > Events > reverse lookup):

Reverse lookup is disabled by default. Enable this feature unless you have no DNS server configured or have poor network performance because of heavy network traffic.

With reverse lookup enabled, when a network-related event occurs, both the IP address and the domain name for the networked device associated 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.

Data log

Path: Logs > Data > *options*

View a log of measurements about the Modular PDU. Each entry is listed by the date and time the data was recorded. The **Input Voltage** filter is enabled by default.To view the electrical current data for a panel, click its name and click **Apply**.

To display the data log (Logs > Data > log):

- By default, view the data log as a page of the Web interface.
- To see the listed data on one page, click **Launch Log in New Window** from the data log page to display a full-screen view of the log.

Note: In your browser's options, JavaScript® must be enabled for you to use the **Launch Log in New Window** button.
You can also use FTP or SCP to view the event log. See “Using FTP or SCP to retrieve log files”.

To filter the log by date or time (Logs > Data > log):

To display the entire **Input Voltage** or **Panel Current** data log, or to change the number of days or weeks for which the log displays the most recent events, select **Last**. Select a time range from the drop-down menu, then click **Apply**. The filter configuration is saved until the device restarts.

To display data logged during a specific time range, select **From**. Specify the beginning and ending times (using the 24-hour clock format) and dates for which to display data, then click **Apply**. The filter configuration is saved until the device restarts.

To view the entire data log, export the log and then view it using a spreadsheet application. To export the log, see “Using FTP or SCP to retrieve log files”.

To delete the data log:

To delete all data recorded in the log, click **Clear Data Log** on the Web page that displays the log. Deleted data cannot be retrieved.

To set the data collection interval (Logs > Data > interval):

Define, in the **Log Interval** setting, how frequently data is sampled and stored in the data log, and view the calculation of how many days of data the log can store, based on the interval you selected.

When the log is full, the older entries are deleted. To avoid automatic deletion of older data, enable and configure data log rotation, described in the next section.

To configure data log rotation (Logs > Data > rotation):

Set up a password-protected data log repository on a specified FTP server. Enabling rotation causes the contents of the data log to be appended to the file you specify by name and location. Updates to this file occur at the upload interval you specify.

Parameter	Description
Data Log Rotation	Enable or disable (the default) data log rotation.
FTP Server Address	The location of the FTP server where the data repository file is stored.
User Name	The user name 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.
Password	The password required to send data to the repository file.
File Path	The path to the repository file.
Filename	The name of the repository file (an ASCII text file).
Unique File Name	Add a date stamp prefix to the filename, using the format *MMDDYYY_filename.txt*. If updates occur more than once on the same day, the data is appended to the file created that day.
Delay *X* hours between uploads.	The number of hours between uploads of data to the file.
Upload every *X* minutes	The number of minutes between attempts to upload data to the file after an upload failure.
Up to *X* times	The maximum number of times the upload will be attempted after an initial failure.
Until Upload Succeeds	Attempt to upload the file until the transfer is completed.

To upload the file one time and then disable future uploads:

1. In the **Data Log Rotation** field, mark the **Enable** check box.
2. Click the **Upload Now!** button.
3. Clear the **Enable** check box.

Using FTP or SCP to retrieve log files

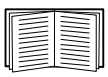
An Administrator or Device User can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) or data log file (*data.txt*) and import it into a spreadsheet.

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

Note: The Modular PDU uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits.

If you are using the encryption-based security protocols for your system, use Secure CoPy (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.



See the *Security Handbook*, available on the *Utility* CD provided with your InRow RD or on the APC Web site (**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 use SCP to retrieve the *event.txt* file, use the following command:

```
scp username@hostname_or_ip_address:event.txt ./event.txt
```

To use SCP to retrieve the *data.txt* file, use the following command:

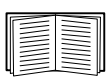
```
scp username@hostname_or_ip_address:data.txt ./data.txt
```

To use FTP to retrieve the files. To use FTP to retrieve the *event.txt* or *data.txt* file:

1. At a command prompt, type `ftp` and the IP address of the Modular PDU, and press ENTER.

   If the **Port** setting for the **FTP Server** option (set through the **Network** menu of the **Administration** tab) has been changed from its default (**21**), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

   ```
   ftp>open ip_address port_number
   ```

   To set a non-default port value to enhance security for the FTP Server, see “FTP Server”. You can specify any port from 5001 to 32768.

2. Use the case-sensitive **User Name** and **Password** for Administrator or Device User to log on. For Administrator, **apc** is the default for **User Name** and **Password**. For the Device User, the defaults are **device** for **User Name** and **apc** for **Password**.

3. Use the **get** command to transmit the text of a log to your local drive.

   ```
   ftp>get event.txt
   ```

   or

   ```
   ftp>get data.txt
   ```

4. You can use the **del** command to clear the contents of either log.

   ```
   ftp>del event.txt
   ```

   or

   ```
   ftp>del data.txt
   ```

   You will not be asked to confirm the deletion.

   - If you clear the data log, the event log records a deleted-log event.
   - If you clear the event log, a new *event.txt* file records the event.

5. Type `quit` at the `ftp>` prompt to exit from FTP.

Administration: Security

Local Users

Setting user access

Path: Administration > Security > Local Users > *options*

You set the case-sensitive user name and password for each account type in the same manner. Maximum length is 10 characters for a user name and 32 characters for a password. Blank passwords (passwords with no characters) are not allowed.

Note: For information on the permissions granted to each account type (Administrator, Device User, and Read-Only User, see “Types of user accounts”.

Account Type	Default User Name	Default Password	Permitted Access
Administrator	apc	apc	Web interface and command line interface
Device User	device	apc	
Read-Only User	readonly	apc	Web Interface only

Remote Users

Authentication

Path: Administration > Security > Remote Users > Authentication Method

Use this option to select how to administer remote access to the Modular PDU.

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

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

- When a user accesses the Modular PDU that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user’s permission level.
- RADIUS user names used with the Modular 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, improperly identified, or improperly configured, you must use a serial connection to the command line interface and change the **Access** setting to **Local Authentication Only** or **RADIUS, then Local Authentication** to regain access.

RADIUS

Path: Administration > Security > Remote Users > RADIUS

Use this option to do the following:

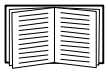
- List the RADIUS servers (a maximum of two) available to the Modular PDU and the time-out period for each.
- Click **Add Server**, and configure the parameters for authentication by a new RADIUS server:
- Click a listed RADIUS server to display and modify its parameters.

RADIUS Setting	Definition
RADIUS Server	The server name or IP address of the 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.
Secret	The shared secret between the RADIUS server and the Modular PDU.
Reply Timeout	The time in seconds that the Modular PDU 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.
Switch Server Priority	Change which RADIUS server will authenticate users if two configured servers are listed and **RADIUS, then Local Authentication** or **RADIUS Only** is the enabled authentication method.

Configure the RADIUS Server

Summary of the configuration procedure

You must configure your RADIUS server to work with the Modular PDU.



For examples of the RADIUS users file with Vendor Specific Attributes (VSAs) and an example of an entry in the dictionary file on the RADIUS server, see the APC *Security Handbook*.

1. Add the IP address of the Modular PDU to the RADIUS server client list (file).
2. Users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined. If no Service-Type attributes are configured, users will have read-only access (on the Web interface only).

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

3. Vendor Specific Attributes (VSAs) can be used instead of the Service-Type attributes provided by the RADIUS server. VSAs requires 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.

Configure 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 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

APC supports FreeRADIUS and Microsoft IAS 2003. Other commonly available RADIUS applications may work but have not been fully tested by APC.

Inactivity Timeout

Path: Administration > Security > Auto Log Off

Use this option to configure the time (3 minutes by default) that the system 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 of that account type can log on until the time specified as **Minutes of Inactivity** expires. For example, with the default value for **Minutes of Inactivity**, if a Device User closes the browser window without logging off, no Device User can log on for 3 minutes.

Administration: Network Features

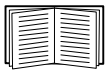
TCP/IP and Communication Settings

TCP/IP settings

Path: Administration > Network > TCP/IP

The **TCP/IP** option on the side menu bar, selected by default when you choose **Network** on the top menu bar, displays the current IP address, subnet mask, default gateway, and MAC address of the Modular PDU.

On the same page, **TCP/IP Configuration** provides the following options for how the TCP/IP settings will be configured when the Modular PDU is powered on, resets, or restarts: **Manual**, **BOOTP**, **DHCP**, and **DHCP & BOOTP**.



For information on DHCP and DHCP options, see **RFC2131** and **RFC2132**.

Setting	Description
Manual	The IP address, subnet mask, and default gateway must be configured manually. Click **Next>>**, and enter the new values.
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Modular PDU requests network assignment from any BOOTP server: • If it receives a valid response, it starts the network services. • If it finds a BOOTP server, but a request to that server fails or times out, the Modular PDU stops requesting network settings until it is restarted. • By default, if previously configured network settings exist, and it 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	At 32-second intervals, the Modular PDU requests network assignment from any DHCP server. By default, the number of retries is unlimited. • If it receives a valid response, by default it requires the APC cookie from the DHCP server in order to accept the lease and start the network services. • If it finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted. To change these values, click **Next>>** for the **DHCP Configuration** page[1]: • **Require vendor specific cookie to accept DHCP Address**: Disable or enable the requirement that the DHCP server provide the APC cookie. • **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.

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 Modular PDU, which uniquely identifies it on the local area network (LAN)
   •**User Class**: The name of the application firmware module

Setting	Description
DHCP & BOOTP	The default setting. The Modular PDU tries to obtain its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server. If it obtains its TCP/IP settings from either server, it switches this setting to **BOOTP** or **DHCP**, depending on the type of server that supplied the TCP/IP settings to the Modular PDU. Click **Next>>** to configure the same settings that are on the **BOOTP Configuration** and **DHCP Configuration** pages[1] and to specify that the **DHCP and BOOTP** setting be retained after either type of server provides the TCP/IP values.

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 Modular PDU, which uniquely identifies it on the local area network (LAN)
   - **User Class**: The name of the application firmware module

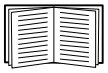
DHCP response options

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

Vendor Specific Information (option 43). The Modular PDU uses this option in a DHCP response to determine whether the DHCP response is valid. This option contains up to two APC-specific options in a TAG/LEN/DATA format: the APC Cookie and the Boot Mode Transition.

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

  Option 43 communicates to the Modular PDU that a DHCP server is configured to service APC devices. By default, this DHCP response option must contain the APC cookie for the Modular PDU to accept the lease.

  To disable the requirement of an APC cookie, see "DHCP".

  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
  ```

- **Boot Mode Transition. Tag 2, Len 1, Data 1/2**

  This option 43 setting enables or disables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**, which, by default, is disabled.

  - A data value of 1 enables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. Whenever the Modular PDU reboots, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.
  - A data value of 2 disables the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** option. The **TCP/IP Configuration** setting option switches to **DHCP** when the Modular PDU accepts the DHCP response. Whenever the Modular PDU reboots, it will request its network assignment from a DHCP server only.

  Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie and the **disable** setting for **Boot Mode Transition**:

  ```
  Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43 0x02 0x01 0x01
  ```

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

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

Other options. The Modular 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 Modular PDU can use.
- **Time Offset** (option 2): The offset of the Modular PDU'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 Modular PDU can use.
- **Host Name** (option 12): The host name that the Modular PDU will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the Modular PDU will use (64-character maximum length).
- **Boot File Name** (from the **file** field of the DHCP response, described in **RFC2131**): The fully qualified directory-path to an user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the Modular PDU will download the .ini file. After the download, the Modular PDU uses the .ini file as a boot file to reconfigure its settings.

Port Speed

Path: Administration > 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: Administration > Network > DNS > *options*

Use the options under **DNS** on the left navigation menu to configure and test the Domain Name System (DNS):

- Select **servers** to specify the IP addresses of the primary and optional secondary DNS server. For the Modular PDU to send e-mail, at least the IP address of the primary DNS server must be defined.
  - The Modular PDU waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the Modular PDU does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the Modular PDU or on a nearby segment (but not across a wide-area network [WAN]).
  - After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for that computer.
- Select **naming** to define the host name and domain name of the Modular PDU:
  - **Host Name**: After you configure a host name here and a domain name in the **Domain Name** field, users can enter a host name in any field in the Modular PDU interface (except e-mail addresses) that accepts a domain name.
  - **Domain Name**: You need to configure the domain name here only. In all other fields in the Modular PDU interface (except e-mail addresses) that accept domain names, the Modular PDU 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 (or example, when defining a trap receiver) include a trailing period. The Modular PDU 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.
- Select **Test** to send a DNS query that tests the setup of your DNS servers:
  - As **Query Type**, select the method to use for the DNS query:
    - **by Host**: the URL name of the server
    - **by FQDN**: the fully qualified domain name
    - **by IP**: the IP address of the server
    - **by MX**: the Mail Exchange used by the server

– 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

– View the result of the test DNS request in the **Last Query Response** field.

Web

Path: Administration > Network > Web > *options*

Option	Description

access	To activate changes to any of these selections, log off from the Modular PDU:
	• **Disable**: Disables access to the Web interface. (You must use the command line interface to re-enable access. Select **Network** and **Web/SSL/TLS**. Then for HTTP, select **Access** and **Enabled**. For HTTPS access, also select **Web/SSL** and **Enabled**.)
	• **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.
	• **Enable HTTPS**: Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL). SSL encrypts user names, passwords, and data during transmission, and authenticates the Modular PDU by digital certificate. When HTTPS is enabled, your browser displays a small lock icon.
	
	See “Creating and Installing Digital Certificates” in the *Security Handbook* on the APC Web site, **www.apc.com**, to choose among the several methods for using digital certificates.
	
	HTTP Port: The TCP/IP port (80 by default) used to communicate by HTTP with the Modular PDU.
	
	HTTPS Port: The TCP/IP port (443 by default) used to communicate by HTTPS with the Modular PDU.
	
	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`

ssl cipher suites	Enable or disable any of the SSL encryption ciphers and hash algorithms: • **DES**: A block cipher that provides authentication by Secure Hash Algorithm. • **RC4_MD5** (enabled by default): A stream cipher that provides authentication by MD5 hash algorithm. • **RC4_SHA** (enabled by default): A stream cipher that provides authentication by Secure Hash Algorithm. • **3DES**: A block cipher that provides authentication by Secure Hash Algorithm.

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, **/sec** on the Modular PDU. • **Generating**: The Modular PDU is generating a certificate because no valid certificate was found. • **Loading**: A certificate is being activated on the Modular PDU. • **Valid certificate**: A valid certificate was installed or was generated by the Modular PDU. Click on this link to view the certificate's contents. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the Modular PDU generates a default certificate, a process which delays access to the interface for up to five minutes.** 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* on the APC Web site, **www.apc.com**, to choose a method for using digital certificates created by the Security Wizard or generated by the Modular PDU. **Remove**: Delete the current certificate.

Console

Path: Administration > Network > Console > *options*

Option	Description

access	Choose one of the following for access by Telnet or Secure SHell (SSH):
	• **Disable**: Disables all access to the command line interface.
	• **Enable Telnet** (the default): Telnet transmits user names, passwords, and data without encryption.
	• **Enable SSH v1 and v2**: Do not enable both versions 1 and 2 of SSH unless you require both. They use extensive processing power.)
	• **Enable SSH v1 only**: SSH version 1 encrypts user names, passwords, and data for transmission. There is little or no delay as you log on.
	• **Enable SSH v2 only**: SSH version 2 transmits user names, passwords, and data in encrypted form with more protection than version 1 from attempts to intercept, forge, or alter data during transmission. There is a noticeable delay as you log on.
	
	Configure the ports to be used by these protocols:
	• **Telnet Port**: The Telnet port used to communicate with the Modular PDU (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 Modular PDU (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 encryption	Enable or disable encryption algorithms (block ciphers) compatible with SSH version 1 or version 2 clients: If your SSH v1 client cannot use **Blowfish**, you must also enable **DES**. Your SSH v2 client selects the enabled algorithm that provides the highest security. If the client cannot use the default algorithms (**3DES** or **Blowfish**), enable an AES algorithm that it can use (**AES 128** or **AES 256**)

Option	Description
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 Modular PDU is creating a host key because no valid host key was found. • **Loading**: A host key is being activated on the Modular PDU. • **Valid**: One of the following valid host keys is in the **/sec** directory (the required location on the Modular PDU): •A 1024-bit host key created by the APC Security Wizard •A 768-bit RSA host key generated by the Modular PDU **Add or Replace**: Browse to and upload a host key file created by the Security Wizard: If you use FTP or Secure CoPy (SCP) instead to transfer the host key file, you must specify the **/sec** directory as the target location in the command. To use the APC Security Wizard, see the *Security Handbook* on the APC Web site, **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 Modular PDU takes up to 5 minutes 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

SNMPv1

Path: Administration > Network > SNMPv1 > *options*

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 InfraStruXure Central to manage the Modular PDU on the public network of an InfraStruXure system, you must have SNMP enabled in the Modular PDU interface. Read access will allow InfraStruxure Central to receive traps from the Modular PDU, but Write access is required while you use the interface of the Modular PDU to set InfraStrusure Central as a trap receiver.

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

Option	Description
access	**Enable SNMPv1 Access:** Enables SNMP version 1 as a method of communication with this device.
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 available SNMPv1 communities, but you can edit these settings to apply more than one entry to any community to grant access by several specific IP 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 a Network Management System (NMS) must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are `public`, `private`, `public2`, and `private2`. **NMS IP/Host Name:** The IP 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 interface or command line interface. • **Write+**: GETS and SETS at any time. • **Disabled**: No GETS or SETS at any time.

SNMPv3

Path: Administration > 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: To use SNMPv3, you must have a MIB program that supports SNMPv3.

The Modular PDU supports only MD5 authentication and DES encryption.

Option	Description
access	**SNMPv3 Access:** Enables SNMPv3 as a method of communication with this device.

Option	Description
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 (`apc auth passphrase`, by default) 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 (`apc crypt passphrase`, by default) that ensures the privacy of the data (by means of encryption) that an NMS is sending to this device or receiving from this device through SNMPv3. **Authentication Protocol:** The APC implementation of SNMPv3 supports MD5 authentication. Authentication will not occur unless MD5 is selected as the authentication protocol. **Privacy Protocol:** The APC implementation of SNMPv3 supports DES as the protocol for encrypting and decrypting data. Privacy of transmitted data requires that DES is selected as the privacy protocol. **NOTE:** You cannot select the privacy protocol if no authentication protocol is selected.
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:** Select from the drop-down list 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 contain 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

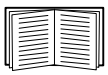
Path: Administration > Network > FTP Server

The **FTP server** settings enable (by default) or disable access to the FTP server and specify the TCP/IP port (21 by default) that the FTP server uses to communicate with the Modular PDU. 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 Secure CoPy (SCP). Selecting and configuring Secure SHell (SSH) enables SCP automatically.

At any time that you want a Modular PDU to be accessible for management by InfraStruxure Central, FTP Server must be enabled in the Modular PDU interface.



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

Administration: Notification and Logging

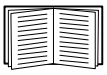
Event Actions

Path: Administration > Notification > Event Actions > *options*

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 in the event log. If no direct notification is configured, users must check the log to determine which events have occurred.



For another method of indirect notification, see “SNMP”. SNMP enables an NMS to perform informational queries. For SNMPv1, configuring the most restrictive SNMP access type, READ, enables informational queries without the risk of allowing remote configuration changes.

You can also log system performance data to use for device monitoring. See “Data log” for information on how to configure and use this data logging option.

Configure event actions

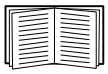
Notification Parameters. For events that have an associated clearing event, you can also set the following parameters as you configure events individually or by group, as described in the next two sections. To access the parameters, click the receiver or recipient name.

Parameter	Description
Delay x time before sending	If the event persists for the specified time, notification is sent. If the condition clears before the time expires, no notification is sent.
Repeat at an interval of *x* time	The notification is sent at the specified interval (e.g., every 2 minutes).
Up to *x* times	During an active event, the notification repeats for this number of times.
Until condition clears	The notification is sent repeatedly until the condition clears or is resolved.

Configure by event. To define event actions for an individual event:

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.
2. In the list of events, review the marked columns to see whether the action you want is already configured. (By default, logging is configured for all events.)
3. 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, click on the event name.

Note: If no Syslog server is configured, items related to Syslog configuration are not displayed.



When viewing details of an event's configuration, you can change the configuration, 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"
- "E-mail recipients"
- "Trap Receivers"

Configure by group. To configure a group of events simultaneously:

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by group** under **Event Actions** on the left navigation menu.
2. Choose how to group events for configuration:
   – Choose **Grouped by severity**, and then select all events of one or more severity levels. You cannot change the severity of an event.
   – Choose **Grouped by category**, and then select all events in one or more pre-defined categories.
3. Click **Next>>** to move from page to page to do the following:
   a. Select event actions for the group of events.
      - To choose any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
      - If you choose **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** (or both) on the next page.
   b. Select whether to leave the newly configured event action enabled for this group of events or to disable the action.

Active, Automatic, Direct Notification

E-mail notification

Overview of setup. Use the 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. (See “DNS”.)
- The IP address or DNS name for **SMTP Server** and **From Address**. (See “SMTP”.)
- The e-mail addresses for a maximum of four recipients. (See “E-mail recipients”.)

Note: You can use the **To Address** setting of the **recipients** option to send e-mail to a text-based pager.

SMTP.

Path: Administration > Notification > E-mail > server

Setting	Description
Local SMTP Server	The IP address or DNS name of the local SMTP server. **NOTE:** This definition is required only when **SMTP Server** is set to **Local**. See “E-mail recipients”.
From Address	The contents of the **From** field in e-mail messages sent by the Modular PDU: • 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’s documentation.

E-mail recipients.

Path: Administration > Notification > E-mail > recipients

Identify up to four e-mail recipients.

Setting	Description
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 mail server's IP address, 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. **NOTE:** The recipient's pager must be able to use text-based messaging.
SMTP Server	Select one of the following methods for routing e-mail: • **Local**: Through the Modular PDU's SMTP server. This setting (recommended) ensures that the e-mail is sent before the Modular PDU's 20-second time-out, and, if necessary, is retried several times. Also do one of the following: • Enable forwarding at the Modular PDU's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Check with the administrator of your SMTP server before changing its configuration to allow forwarding. • Set up a special e-mail account for the Modular PDU to forward e-mail to an external mail account. • **Recipient**: Directly to the recipient's SMTP server. With this setting, the Modular PDU tries to send the e-mail only once. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent. When the recipient uses the Modular PDU's SMTP server, this setting has no effect.
E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.
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.

Email test (Administration > Notification > E-mail > test). Send a test message to a configured recipient.

SNMP traps

Trap Receivers.

Path: Administration > Notification > SNMP Traps > trap receivers

View trap receivers by NMS IP/Host Name. You can configure up to six trap receivers.

- To open the page for configuring a new trap receiver, click **Add Trap Receiver**.
- To modify or delete a trap receiver, first click its IP address or host name to access its settings. (If you delete a trap receiver, all notification settings configured under Event Actions for the deleted trap receiver are set to their default values.)
- To specify the trap type for a trap receiver, select either the SNMPv1 or SNMPv3 radio button. For an NMS to receive both types of traps, you must configure two trap receivers for that NMS, one for each trap type.

Item	Definition
Trap Generation	Enable (the default) or disable trap generation for this trap receiver.
NMS IP/Host Name	The IP address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.

SNMPv1 option.

Community Name	The name (`public` by default) 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). To disable that ability, unmark the checkbox.

SNMPv3 option. Select the identifier of the user profile for this trap receiver. (To view the settings of the user profiles identified by the user names selectable here, choose **Network** on the top menu bar and **user profiles** under **SNMPv3** on the left navigation menu.)

See “SNMPv3” for information on creating user profiles and selecting authentication and encryption methods.

SNMP Trap Test

Path: Administration > 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:

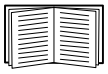
- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver is enabled.
- If a host name is selected for the **To** address, that host name can be mapped to a valid IP address.

To. Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver was ever configured, a link to the **Trap Receiver** configuration page is displayed.

Syslog

Path: Logs > Syslog > *options*

The Modular PDU can send messages to up to four Syslog servers when an event occurs. The Syslog servers record events that occur at network devices in a log that provides a centralized record of events.



This user's guide does not describe Syslog or its configuration values in detail. See **RFC3164** for more information about Syslog.

Identifying Syslog Servers.

Path: Logs > Syslog > servers

Setting	Definition
Syslog Server	Uses IP addresses or host names to identify from one to four servers to receive Syslog messages sent by the Modular PDU.
Port	The user datagram protocol (UDP) port that the Modular PDU will use to send Syslog messages. The default is **514**, the UDP port assigned to Syslog.

Syslog Settings.

Path: Logs > Syslog > settings

Setting	Definition
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the Modular PDU's Syslog messages (**User**, by default). **NOTE: User** best defines the Syslog messages sent by the Modular PDU. **Do not** change this selection unless advised to do so by the Syslog network or system administrator.
Severity Mapping	Maps each severity level of Modular PDU or Environment events to available Syslog priorities. You should not need to change the mappings. The following definitions are from RFC3164: • **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 Following are the default settings for the four **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** **NOTE:** To disable Syslog messages, see "Configuring event actions".

Syslog Test and Format example.

Path: Logs > Syslog > test

Send a test message to the Syslog servers configured through the **servers** option.

1. Select a severity to assign to the test message.
2. Define the test message, according to the required message fields
   – The priority (PRI): the Syslog priority assigned to the message's event, and the facility code of messages sent by the Modular PDU.
   – The Header: a time stamp and the IP address of the Modular PDU.
   – The message (MSG) part:
      • The TAG field, followed by a colon and space, identifies the event type.
      • The CONTENT field is the event text, followed (optionally) by a space and the event code.

   For example, `APC: Test Syslog` is valid.

Queries (SNMP GETs)

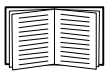
See "SNMP" for a description of SNMPv1 and SNMPv3 settings that enable an NMS to perform informational queries. With SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without allowing remote configuration changes.

Administration: General Options

Identification

Path: Administration > General > Identification

Define values for **Name** (the device name), **Location** (the physical location), and **Contact** (the person responsible for the device) used by the Modular PDU's SNMP agent. These settings are the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifiers (OIDs).



For more information about MIB-II OIDs, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide*, available on the APC Web site, **www.apc.com**.

Set the Date and Time

Method

Path: Administration > General > Date & Time > mode

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

- **Manual Mode**: Do one of the following:
  - Enter the date and time for the Modular PDU.
  - Mark the check box **Apply Local Computer Time** to match the date and time settings of the computer you are using.
- **Synchronize with NTP Server**: Have an NTP Server define the date and time for the Modular PDU.

Setting	Definition
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.
Time Zone	Select a time zone. The number of hours preceding each time zone in the list is the offset from Coordinated Universal Time (UTC), formerly Greenwich Mean Time).
Update Interval	Define how often, in hours, the Modular PDU accesses the NTP Server for an update. *Minimum*: 1; *Maximum*: 8760 (1 year).
Update Using NTP Now	Initiate an immediate update of date and time by the NTP Server.

Daylight saving

Path: Administration > General > Date & Time > daylight saving

Enable traditional United States Daylight Saving Time (DST), or enable and configure a customized daylight saving time to match how Daylight Saving Time is implemented in your local area. DST is disabled by default.

When customizing Daylight Saving Time (DST):

- If the 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 in a subsequent year, the time setting still changes on the fourth Sunday.
- If the 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**.

Format

Path: Administration > General > Date & Time > date format

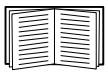
Select the numerical format in which to display all dates in this user interface. In the selections, each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.

Use an .ini File

Path: Administration > General > User Config File

Use the settings from one Modular PDU to configure another. Retrieve the config.ini file from the configured Modular PDU, customize that file (e.g., to change the IP address), and upload the customized file to the new Modular PDU. 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 r reports the errors in the event log.
Upload	Browse to the customized file and upload it so that the current Modular PDU can use it to set its own configuration**.**



To retrieve and customize the file of a configured Modular PDU, see “How to Export Configuration Settings”.

Instead of uploading the file to one Modular PDU, you can export the file to multiple Modular PDUs by using an FTP or SCP script or a batch file and the APC .ini file utility, available from **www.apc.com/tools/download**.

Temperature Units

Path: Administration > General > Unit Preference

Select the temperature scale (Fahrenheit or Celsius) in which to display all temperature measurements in this user interface.

Reset the Interface

Path: Administration > General > Reset/Reboot

Action	Definition
Reboot Management Interface	Restarts the interface of the Modular PDU.
Reset All[1]	Select **Exclude TCP/IP** to reset all values except TCP/IP; clear **Exclude TCP/IP** to reset all configuration values.
Reset Only[1]	**TCP/IP settings**: Set TCP/IP Configuration to **DHCP & BOOTP**, its default setting, requiring that the Modular PDU receive its TCP/IP settings from a DHCP or BOOTP server. See “TCP/IP and Communication Settings”.
	Event configuration: Reset all changes to event configuration, by event and by group, to their default settings.
1. Resetting may take up to a minute.	

Configuring Links

Path: Administration > General > Quick Links

Select the **Administration** tab, **General** on the top menu bar, and **Quick Links** on the left navigation menu 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 Web site.
- **Link 2**: A page where you can use samples of APC Web-enabled products.
- **Link 3**: The home page of the APC Remote Monitoring Service.

To reconfigure any of the following, click the link name in the **Display** column:

- **Display**: The short link name displayed on each interface page
- **Name**: A name that fully identifies the target or purpose of the link
- **Address**: Any URL—for example, the URL of another device or server

About the Modular PDU

Path: Administration > General > About

The hardware information is especially useful to APC Customer Support to troubleshoot problems with the Modular PDU. The serial number and MAC address are also available on the Modular PDU itself.

Firmware information for the Application Module and APC OS (AOS) 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 APC Web site.

Management Uptime is the length to time the interface has been running continuously.

APC Device IP Configuration Wizard

Capabilities, Requirements, and Installation

How to use the Wizard to configure TCP/IP settings

The APC Device IP Configuration Wizard configures the IP address, subnet mask, and default gateway of one or more Modular PDUs. You can use the Wizard in either of the following ways:

- Remotely over your TCP/IP network to discover and configure unconfigured Modular PDUs on the same network segment as the computer running the Wizard.
- Through a direct connection from a serial port of your computer to the Modular PDU to configure or reconfigure it.

System requirements

The Wizard runs on Microsoft Windows 2000, Windows 2003, and Windows XP operating systems.

Installation

To install the Wizard from the *Utility* CD, if one is provided with your Modular PDU:

1. If autorun is enabled, the user interface of the CD starts when you insert the CD. Otherwise, open the file **contents.htm** on the CD.
2. Click **Device IP Configuration Wizard** and follow the instructions.

To install the Wizard from a downloaded executable file:

1. Go to **www.apc.com/tools/download**.
2. Download the Device IP Configuration Wizard.
3. Run the executable file in the folder to which you downloaded it.

Use the Wizard

Note: Most software firewalls must be temporarily disabled for the Wizard to discover unconfigured Modular PDUs.

Launch the Wizard

The installation creates a shortcut link in the **Start** menu to launch the Wizard.

Configure the basic TCP/IP settings remotely

Prepare to configure the settings. Before you run the Wizard:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. If you are configuring multiple unconfigured Modular PDUs, obtain the MAC address of each one to identify it when the Wizard discovers it. (The Wizard displays the MAC address on the screen on which you then enter the TCP/IP settings.)
   - The MAC address is on a label on the Modular PDU.
   - You can also obtain the MAC address from the Quality Assurance slip that came with the Modular PDU.

Run the Wizard to perform the configuration. To discover and configure unconfigured Modular PDUs over the network:

1. From the **Start** menu, launch the Wizard. The Wizard detects the first Modular PDU that is not configured.
2. Select **Remotely (over the network)**, and click **Next >**.
3. Enter the system IP, subnet mask, and default gateway for the Modular PDU identified by the MAC address. Click **Next >**.

   On the **Transmit Current Settings Remotely** screen, if you select the **Start a Web browser when finished** check box, the default Web browser connects to the Modular PDU after the Wizard transmits the settings.
4. Click **Finish** to transmit the settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
5. If the Wizard finds another unconfigured Modular PDU, it displays the screen to enter TCP/IP settings. Repeat this procedure beginning at step 3, or to skip the Modular PDU whose MAC address is currently displayed, click **Cancel**.

Configure or reconfigure the TCP/IP settings locally

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the serial configuration cable (which came with the Modular PDU) from an available communications port on your computer to the serial port of the card or device. Make sure no other application is using the computer port.
3. From the **Start** menu, launch the Wizard application.
4. If the Modular PDU is not configured, wait for the Wizard to detect it. Otherwise, click **Next>**.
5. Select **Locally (through the serial port)**, and click **Next >**.
6. Enter the system IP, subnet mask, and default gateway for the Modular PDU, and click **Next >**.
7. On the **Transmit Current Settings Remotely** screen, if you select the **Start a Web browser when finished** check box, the default Web browser connects to the Modular PDU after the Wizard transmits the settings.
8. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
9. If you selected **Start a Web browser when finished** in step 7, you can now configure other parameters through the Web interface of the device.

Export Configuration Settings

Retrieve and Export the .ini File

Summary of the procedure

An Administrator can retrieve the .ini file of a Modular PDU and export it to another Modular PDU or to multiple Modular PDUs.

1. Configure one Modular PDU to have the settings you want to export.
2. Retrieve the .ini file from that Modular PDU.
3. Customize the file to change at least the TCP/IP settings.
4. Use a file transfer protocol supported by the Modular PDU to transfer a copy to one or more other Modular PDUs. For a transfer to multiple Modular PDUs, use an FTP or SCP script or the APC .ini file utility.

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

Contents of the .ini file

The config.ini file you retrieve from the Modular PDU contains the following:

- *section headings* and *keywords* (only those supported for the device from which you retrieve the file)*:* Section headings are category names enclosed in brackets ([ ]). Keywords, under each section heading, are labels describing specific Modular PDU 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, e.g., in the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the Modular PDU) 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:

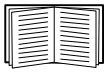
1. If possible, use the interface of a Modular PDU to configure it with the settings to export. Directly editing the .ini file risks introducing errors.
2. To use FTP to retrieve config.ini from the configured Modular PDU:
   a. Open a connection to the Modular PDU, using its IP address:

      `ftp>` **`open`** ***`ip_address`***

   b. Log on using the Administrator user name and password.
   c. Retrieve the config.ini file containing the Modular PDU's settings:

      `ftp>` **`get config.ini`**

   The file is written to the folder from which you launched FTP.



To retrieve configuration settings from multiple Modular PDUs and export them to other Modular PDUs, see *Release Notes: ini File Utility, version 1.0*, available on the APC Web site, **www.apc.com**.

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 Modular PDUs can access a Network Time Protocol server, configure `enabled` for `NTPEnable`:

     ```
     NTPEnable=enabled
     ```

     Alternatively, reduce transmission time by exporting the `[SystemDate/Time]` section as a separate .ini file.
   - To add comments, start each comment line with a semicolon (`;`).
2. Copy the customized file to another file name in the same folder:
   - The file name can have up to 64 characters and must have the .ini suffix.
   - Retain the original customized file for future use. **The file that you retain is the only record of your comments.**

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

- From the Web interface of the receiving Modular PDU, select the **Administration** tab, **General** on the top menu bar, and **User Config File** on the left navigation menu. Enter the full path of the file, or use **Browse**.
- Use any file transfer protocol supported by Modular PDUs, i.e., FTP, FTP Client, SCP, or TFTP). The following example uses FTP:
  a. From the folder containing the copy of the customized .ini file, use FTP to log in to the Modular PDU to which you are exporting the .ini file:

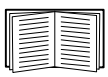
     ```
     ftp> open ip_address
     ```

  b. Export the copy of the customized .ini file to the root directory of the receiving Modular PDU:

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

Exporting the file to multiple Modular PDUs. To export the .ini file to multiple Modular PDUs:

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single Modular PDU.
- Use a batch processing file and the APC .ini file utility.



To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* on the APC Web site, **www.apc.com**.

The Upload Event and Error Messages

The event and its error messages

The following event occurs when the receiving Modular PDU completes using the .ini file to update its settings.

`Configuration file upload complete, with` *`number`* `valid values`

If a keyword, section name, or value is invalid, the upload by the receiving Modular PDU succeeds, and additional event text states the error.

Event text	Description
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number*.	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number*.	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, an incomplete upload occurs. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in config.ini

A device associated with the Modular PDU 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, for another reason, is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values.

If you did not intend to export the configuration of the device 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” for information about which values are overridden.

Because the overridden values are device-specific and not appropriate to export to other Modular PDUs, ignore these error messages. To prevent these error messages, you can 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 APC Device IP Configuration Wizard to update the basic TCP/IP settings of Modular PDUs and configure other settings through their user interface.

See “APC Device IP Configuration Wizard”.

File Transfers

Upgrading Firmware

Benefits of upgrading firmware

When you upgrade the firmware on the Modular PDU:

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

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

Firmware files (Modular PDU)

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module. Each module contains one or more Cyclical Redundancy Checks (CRCs) to protect its data from corruption during transfer.

The APC Operating System (AOS) and application module files used with the Modular PDU share the same basic format:

apc_*hardware-version*_*type*_*firmware-version*.bin

- `apc`: Indicates that this is an APC file.
- ***hardware-version*:** `hw0x` identifies the version of the hardware on which you can use this binary file.
- ***type*:** Identifies whether the file is for the APC Operating System (AOS) or the application module for the Modular PDU.
- ***version*:** The version number of the file.
- `bin`: Indicates that this is a binary file.

Obtain the latest firmware version

Automated upgrade tool for Microsoft Windows systems. An upgrade tool automates the transferring of the firmware modules on any supported Windows operating system. Obtain the latest version of the tool at no cost from **www.apc.com/tools/download**. At this Web page, find the latest firmware release for your APC product and download the automated tool. **Never** use the tool for one APC product to upgrade firmware of another.

Manual upgrades, primarily for Linux systems. If no computer on your network is running a Microsoft Windows operating system, you must upgrade the firmware of your Modular PDUs by using the separate AOS and application firmware modules.

Obtain the individual firmware modules by downloading the automated tool from **www.apcc.com/tools/download**, then extracting the firmware files from the tool.

To extract the firmware files:

1. Run the tool.
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.

Firmware File Transfer Methods

To upgrade the firmware of a Modular PDU, use one of these methods:

- From a networked computer running a Microsoft Windows operating system, use the firmware upgrade tool downloaded from the APC Web site.
- From a networked computer on any supported operating system, use FTP or SCP to transfer the individual AOS and application firmware modules.
- For a Modular PDU that is not on your network, use XMODEM through a serial connection to transfer the individual firmware modules from your computer to the Modular PDU.

Caution: When you transfer individual firmware modules, **you must** transfer the APC Operating System (AOS) module to the Modular PDU before you transfer the application module.

Use FTP or SCP to upgrade one Modular PDU

FTP. For you to use FTP to upgrade one Modular PDU over the network:

- The Modular PDU must be connected to the network, and its system IP, subnet mask, and default gateway must be configured
- The FTP server must be enabled at the Modular PDU
- The firmware files must be extracted from the firmware upgrade tool (see “To extract the firmware files:”)

To transfer the files:

1. Open a command prompt window of a computer on the network. Go to the directory that contains the firmware files, and list the files:

   ```
   C:\>cd\apc
   C:\apc>dir
   ```

   For the listed files, *xxx* represents the firmware version number:

   - `apc_hw03_aos_`***xxx***`.bin`
   - `apc_hw03_`**application_*xxx***`.bin`

2. Open an FTP client session:

   ```
   C:\apc>ftp
   ```

3. Type `open` and the Modular PDU’s IP address, 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:

   ```
   ftp> open 150.250.6.10 21000
   ```

   – Some FTP clients require a colon instead before the port number.

4. Log on as Administrator; **apc** is the default user name and password.
5. Upgrade the AOS. In the example, *xxx* is the firmware version number:

   ```
   ftp> bin
   ftp> put apc_hw03_aos_xxx.bin
   ```

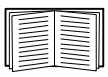
6. When FTP confirms the transfer, type **quit** to close the session.
7. After 20 seconds, repeat step 2 through step 6. In step 5, use the application module file name.

SCP. To use Secure CoPy (SCP) to upgrade firmware for a Modular PDU:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the Modular PDU. The following example uses *xxx* to represent the version number of the AOS module:
   `scp apc_hw03_aos_xxx.bin apc@158.205.6.185:apc_hw03_aos_xxx.bin`
3. Use a similar SCP command line, with the name of the application module, to transfer the second firmware module to the Modular PDU.

How to upgrade multiple Modular PDUs

Export configuration settings. You can create batch files and use an APC utility to retrieve configuration settings from multiple Modular PDUs and export them to other Modular PDUs.



See *Release Notes: ini File Utility, version 1.0,* available on the APC Web site, **www.apc.com**.

Use FTP or SCP to upgrade multiple Modular PDUs. To upgrade multiple Modular PDUs using an FTP client or using SCP, write a script which automatically performs the procedure.

Use XMODEM to upgrade one Modular PDU

To upgrade the firmware for one Modular PDU that is not on the network, you must extract the firmware files from the firmware upgrade tool (see “To extract the firmware files:”).

To transfer the files:

1. Obtain the individual firmware modules (the AOS module and the application module) from **www.apc.com/tools/download**.
2. Select a serial port at the local computer and disable any service that uses the port.
3. Connect the provided configuration cable to the selected port and to the serial port at the Modular PDU.
4. Run a terminal program such as HyperTerminal, and configure the selected port for 2400 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
5. Press ENTER to display the **User Name** prompt.
6. Enter the Administrator user name and password (**apc** by default for both).
7. From the **command line interface** menu, select **System**, then **Tools**, then **File Transfer**, then **XMODEM**; and type `Yes` at the prompt to continue.
8. Select a baud rate, change the terminal program’s baud rate to match your selection, and press ENTER. A higher baud rate causes faster upgrades.
9. From the terminal program’s menu, select the binary AOS file to transfer using XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 2400. The Modular PDU automatically restarts.
10. Repeat step 4 through step 9 to install the application module. In step 9, use the application module file name, not the AOS module file name.
11. For information about the format used for firmware modules, see “Firmware files (Modular PDU)”.

Verifying Upgrades and Updates

Verify the success or failure of the transfer

To verify whether a firmware upgrade succeeded, use the **Network** menu in the command line interface and select the **FTP Server** option to view **Last Transfer Result**, or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last Transfer Result codes

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.

Use the Web interface to verify the versions of the upgraded firmware modules by selecting the **Administration** tab, **General** on the top menu bar, and **About** on the left navigation menu, or use an SNMP GET to the MIB II **sysDescr** OID.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France
+ 33 (0) 1 41 29 70 00
www.se.com

990-4623A **2/2024**