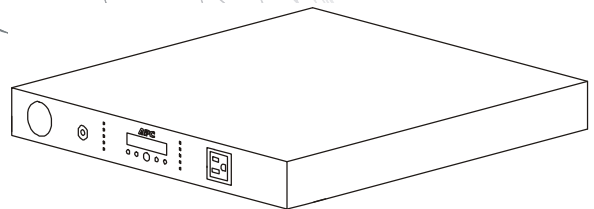


Operation

Network Management Card for G-Type Rack Power Filter

120 Vac
15 A
20 A



Contents

Using the Network Management Card 1

Product Features.....	1
Access Priorities for Logging on.....	2
Types of User Accounts.....	2
Watchdog Features.....	3
Getting Started	4
Establishing Network Settings	4
Recovering from a Lost Password	8

Command Line Interface 10

About the Command Line Interface	10
Logging on to the Command Line Interface.....	11
About the Main Screen.....	12
Using the Command Line Interface.....	14
Command Syntax	15
Command Response Codes	16
Network Management Card Command Descriptions	17
Device Command Descriptions	30

Web Interface..... 37

Supported Web Browsers	37
Logging On to the Web Interface.....	37
Web Interface Features.....	39
About the Device Summary Tab	41

About the Status Tab	42
About the Configuration and Control Tab.....	42
Logs	48
Using the Event and Data Logs	48
Administration: Security	55
Local Users	55
Remote Users	56
Configuring the RADIUS Server.....	58
Inactivity Timeout	59
Administration: Network Features	60
TCP/IP and Communication Settings	60
Ping Response.....	63
Port Speed	63
DNS.....	64
Web.....	65
Console	67
SNMP	68
FTP Server	71
Administration: Notification	72
Event Actions.....	72
Active, Automatic, Direct Notification	74
Administration: General Options	80
Identification	80
Set the Date and Time.....	80

Use an .ini File	81
Event Log and Temperature Units	82
Reset the Rack Power Filter	83
Configure Links	83
About the Rack Power Filter	84
Device IP Configuration Wizard	85
Capabilities, Requirements, and Installation	85
Use the Wizard	86
How to Export Configuration Settings.....	88
Retrieving and Exporting the .ini File	88
The Upload Event and Error Messages	91
Related Topics	92
File Transfers	93
How to Upgrade Firmware	93
Firmware File Transfer Methods	95
Verifying Upgrades and Updates	99
Troubleshooting	101
Rack Power Filter Access Problems	101
The unit will not turn on	102
The Overload indicator is illuminated	102
The Wiring OK indicator is not illuminated	102
Appendix A: List of Supported Commands	104

Using the Network Management Card

Product Features

The American Power Conversion (APC[®]) Audio/Visual G-Type Rack Power Filter is a stand-alone power distribution device that is network-manageable.

The Rack Power Filter provides real-time remote monitoring of connected loads. User-defined alarms warn of potential circuit overloads. The Rack Power Filter provides full control over outlets through remote commands and user interface settings.

You can manage a Rack Power Filter through its Web interface, its command line interface (CLI), InfraStruxure[®] Central, or Simple Network Management Protocol (SNMP).

(To use the PowerNet MIB with an SNMP browser, see the *PowerNet SNMP Management Information Base (MIB) Reference Guide*, available at www.apc.com.)

Rack Power Filters have these additional features:

- Peak load, and power and energy monitoring for all connected loads.
- Voltage, current, and power monitoring for phases.
- Current monitoring for outlet banks.
- Configurable alarm thresholds that provide network and visual alarms to help avoid overloaded circuits.
- Three levels of user access accounts: Administrator, Device User, and Read-Only User.
- Independent outlet control.
- Configurable power delays.
- Event and data logging. The event log is accessible by Telnet, Secure CoPy (SCP), File Transfer Protocol (FTP), serial connection, or Web browser (using HTTPS access with SSL, or using HTTP access). The data log is accessible by Web browser, SCP, or FTP.
- E-mail notifications for Rack Power Filter and system events.
- Security protocols for authentication and encryption.

Access Priorities for Logging on

Only one user at a time can log on to the Rack Power Filter. 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 Rack Power Filter
- Telnet or Secure SHell (SSH) access to the command line interface from a remote computer
- Web access, either directly or through InfraStruxure Central



Note: See “SNMP” on page 68 for information about how SNMP access to the Rack Power Filter is controlled.

Types of User Accounts

The Rack Power Filter has three levels of access (Administrator, Device User, and Read-Only User), which are protected by user name and password requirements.

- An Administrator can use all of the menus in the Web interface and all of the commands in the command line interface. The default user name and password are both **apc**.
- A Device User can access only the following:
 - In the Web interface, the menus on the **Device Manager** tab, the **Environment** tab, and the event and data logs, accessible under the **Events** and **Data** headings on the left navigation menu of the **Logs** tab. The event and data logs display no button to clear the log.
 - In the command line interface, the equivalent features and options.

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

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

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



To set **User Name** and **Password** values for the three account types above, see “Setting user access” on page 55.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the Rack Power Filter 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 Rack Power Filter implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Rack Power Filter 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 Rack Power Filter does not restart if the network is quiet for 9.5 minutes, the Rack Power Filter attempts to contact the default gateway every 4.5 minutes. If the gateway is present, it responds to the Rack Power Filter, and the response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network and is on the subnet. The network traffic of that computer will restart the 9.5-minute time frequently enough to prevent the Rack Power Filter from restarting.

Getting Started

To start using the Rack Power Filter:

1. Install the Rack Power Filter. See the Installation and Operation guide included with the unit (APC part number 990-4316).
2. Apply power and connect to your network.
3. Establish network settings. (See “Establishing Network Settings” on this page.)
4. Begin using the Rack Power Filter by way of one of the following:
 - “Web Interface” on page 37
 - “Command Line Interface” on page 10
 - Use the display interface on the unit. See the Installation and Operation guide for details.

Establishing Network Settings

You must configure the following TCP/IP settings before the Rack Power Filter can operate on a network:

- IP address of the Rack Power Filter
- Subnet mask
- Default gateway



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



Caution: Do not use the loopback address (127.0.0.1) as the default gateway address for the Rack Power Filter. It disables the card and requires you to reset TCP/IP settings to their defaults using a local serial login.



See “Watchdog Features” on page 3 for more information about the watchdog role of the default gateway.

TCP/IP configuration methods

Use one of the following methods to define the TCP/IP settings needed by the Rack Power Filter:

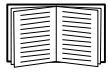
- “Device IP Configuration Wizard” on page 85
- “DHCP and BOOTP configuration” on page 5
- “Command Line Interface” on page 7

INI file utility

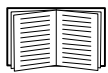
You can use the INI file export utility to export INI file settings from a configured Rack Power Filters to one or more unconfigured Rack Power Filters. For more information, see “Use an .ini File” on page 81.

DHCP and BOOTP configuration

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



A user configuration (INI) file can function as a BOOTP or DHCP boot file. For more information, see “Use an .ini File” on page 81.



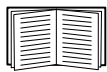
If neither of these servers is available, see “Device IP Configuration Wizard” on page 85 or “Command Line Interface” on page 7.

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

In the BOOTPTAB file of the BOOTP server, enter the Rack Power Filter’s MAC address, IP address, subnet mask, and default gateway, and, optionally, a bootup file name. Look for the MAC address on the bottom of the Rack Power Filter or on the Quality Assurance slip included in the package.

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

- If you specified a bootup file name, the Rack Power Filter attempts to transfer that file from the BOOTP server using TFTP or FTP. The Rack Power Filter assumes all settings specified in the bootup file.
- If you did not specify a bootup file name, you can configure the other settings of the Rack Power Filter remotely through its “Web Interface” on page 37 or “Command Line Interface” on page 7; the user name and password are both **apc**, by default.



To create a bootup file, see your BOOTP server documentation.

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



This section summarizes the Rack Power Filter’s communication with a DHCP server. For more detail about how a DHCP server can configure the network settings for a Rack Power Filter, see “DHCP response options” on page 61.

1. The Rack Power Filter sends out a DHCP request that uses the following to identify itself:
 - A Vendor Class Identifier (APC by default)
 - A Client Identifier (by default, the MAC address of the Rack Power Filter)
 - A User Class Identifier (by default, the identification of the application firmware installed on the Rack Power Filter)
2. A properly configured DHCP server responds with a DHCP offer that includes all the settings that the Rack Power Filter needs for network communication. The DHCP offer also includes the Vendor Specific Information option (DHCP option 43). The Rack Power Filter can be configured to ignore DHCP offers that do not encapsulate the APC cookie in DHCP option 43 using the following hexadecimal format. (The Rack Power Filter does not require this cookie by default.)

Option 43 = 01 04 31 41 50 43

Where:

- The first byte (01) is the code.
- The second byte (04) is the length.
- The remaining bytes (31 41 50 43) are the APC cookie.



See your DHCP server documentation to add code to the Vendor Specific Information option.



Note: By selecting the **Require vendor specific cookie to accept DHCP Address** check box in the Web interface, you can require the DHCP server to provide an “APC” cookie, which supplies information to the Rack Power Filter:
Administration > Network>TCP/IP>ipv4 settings.

Command Line Interface

1. Log on to the command line interface. See “Logging on to the Command Line Interface” on page 11.
2. Contact your network administrator to obtain the IP address, subnet mask, and default gateway for the Rack Power Filter.
3. Use these three commands to configure network settings. (Text in italics indicates a variable.)
 - a. `tcpip -i yourIPAddress`
 - b. `tcpip -s yourSubnetMask`
 - c. `tcpip -g yourDefaultGateway`

For each variable, type a numeric value that has the format `xxx.xxx.xxx.xxx`.

For example, to set a system IP address of 156.205.14.141, type the following command and press ENTER:

```
tcpip -i 156.205.14.141
```

4. Type `exit`. The Rack Power Filter restarts to apply the changes.

Recovering from a Lost Password

You can use a local computer (a computer that connects to the Rack Power Filter or other device through the serial port) to access the command line interface.

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the serial cable that is included with the unit, to the selected port on the computer and to the Serial port at the Rack Power Filter.
3. Run a terminal program (such as HyperTerminal[®]) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
 - The serial port is not in use by another application.
 - The terminal settings are correct as specified in step 3.
 - The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
6. Press ENTER, repeatedly if necessary, to display the **User Name** prompt again, then use the default, **apc**, for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is re-displayed, you must repeat step 5 and log on again.)
7. At the command line interface, use the following commands to change the **User Name** and **Password** settings, both of which are now **apc**:

```
user -an yourAdministratorName
user -ap yourAdministratorPassword
```

For example, to change the Administrator user name to **Admin**, type:

```
user -an Admin
```
8. Type quit or exit to log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Command Line Interface

About the Command Line Interface

Use the command line interface to view the status of and configure and manage the Rack Power Filter. In addition, the command line interface enables you to create scripts for automated operation. An Administrator has full access to the command line interface, a Device user has limited access, and a Read-Only user is completely restricted. (For additional details, see “Types of User Accounts” on page 2.)

Configure all parameters of a Rack Power Filter (including those for which there are not specific CLI commands) by using the CLI to transfer an INI file to the Rack Power Filter. The CLI uses XMODEM to perform the transfer. However, you cannot read the current INI file through XMODEM.

Logging on to the Command Line Interface

To access the command line interface, use either a local (serial) connection or a remote (Telnet or SSH) connection with a computer on the same network as the Rack Power Filter.

Remote access to the command line interface

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

To enable or disable these access methods, use 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.

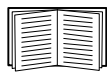
Telnet for basic access. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption.

To use Telnet to access the command line interface:

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

If the Rack Power Filter 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 don't 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).



If you cannot remember your user name or password, see “Recovering from a Lost Password” on page 8.

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 Rack Power Filter through the serial port to access the command line interface:

1. Select a serial port at the computer and disable any service that uses that port.
2. Connect a serial cable from the selected serial port on the computer to the **Serial** port on the Rack Power Filter.
3. Run a terminal program (e.g., HyperTerminal) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER. At the prompts, enter your user name and password.

About the Main Screen

Following is an example of the main screen, which is displayed when you log on to the command line interface of a Rack Power Filter.

```
American Power Conversion          Network Management Card AOS vx.x.x
(c)Copyright 2010 All Rights Reserved  Pro AV 2                x.x.x
-----
Name      : RackProAV                      Date : 12/30/2010
Contact   : Don Adams                     Time : 5:58:30
Location  : Building 3                    User  : Administrator
Up Time   : 45 Days, 21 Hours, 21 Minutes  Stat  : P+ N4+ N6+ A+

APC>
```

- Two fields identify the APC operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the type of device that connects to the network. In the example above, the application firmware for the Rack Power Filter is displayed.

```
Network Management Card AOS  vx.x.x
Pro AV                       vx.x.x
```

- Three fields identify the system name, contact person, and location of the Rack Power Filter.

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

- An **Up Time** field reports how long the Rack Power Filter has been running since it was last turned on or reset.

```
Up Time   : 45 Days, 21 Hours, 21 Minutes
```

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

```
Date : 12/30/2010
Time : 5:52:30
```

- The **User** field identifies whether you logged in through the **Administrator** or **Device Manager** account. (The **Read Only User** account cannot access the command line interface.)

```
User : Administrator
```

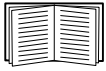
- A **Stat** field reports the Rack Power Filter status.

Stat : P+ N4+ N6+ A+

P+	The APC operating system (AOS) is functioning properly.
----	---

IPv4 only	IPv6 only	IPv4 and IPv6*	Description
N+	N+	N4+ N6+	The network is functioning properly.
N?	N6?	N4? N6?	A BOOTP request cycle is in progress.
N-	N6-	N4- N6-	The Rack Power Filter failed to connect to the network.
N!	N6!	N4! N6!	Another device is using the Rack Power Filter 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 staff.

Using the Command Line Interface

At the command line interface, use commands to configure the Rack Power Filter. To use a command, type the command and press ENTER. Commands and arguments are valid in lowercase, uppercase, or mixed case. Options are case-sensitive.

While using the command line interface, you can also do the following:

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

```
radius ?
```

```
or
```

```
radius help
```

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

Command Syntax

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

Example of a command that supports multiple options:

```
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

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

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

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

```
alarmcount -p critical
```

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

Command Response Codes

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

The CLI reports all command operations with the following format:

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

Code	Message
E000	Success
E001	Successfully Issued
E002	Reboot required for change to take effect
E100	Command failed
E101	Command not found
E102	Parameter Error
E103	Command Line Error
E104	User Level Denial
E105	Command Prefill
E106	Data Not Available
E107	Serial communication with the Rack Power Filter has been lost

Network Management Card Command Descriptions

?

Access: Administrator, Device User, Outlet User

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

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

```
alarmcount ?
```

about

Access: Administrator, Device User, Outlet User

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

alarmcount

Access: Administrator, Device User, Outlet User

Description:

Option	Arguments	Description
-p	all	View the number of active alarms reported by the Rack Power Filter. 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
```

appli

Access: Administrator, Device User, Outlet User

Description: Access the AP79XX series Rack PDU Command Line Interface. See AP79XX product documentation for command details.

boot

Access: Administrator only

Description: Define how the Rack Power Filter 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 Rack Power Filter turns on, resets, or restarts. See “TCP/IP and Communication Settings” on page 60 for information about each boot mode setting.
-c	enable disable	dhcp and dhcpBootp boot modes only. Enable or disable the requirement that the DHCP server provide the APC cookie.
The default values for these three settings generally do not need to be changed: -v <vendor class>: APC -i <client id>: The MAC address of the Rack Power Filter, which uniquely identifies it on the network -u <user class>: The name of the application firmware module		

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

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

cd

Access: Administrator, Device User, Outlet User

Description: Navigate to a folder in the directory structure of the Rack Power Filter.

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

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

Example 2: To return to the main directory folder, type:

```
cd ..
```


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 <code>disable</code> command to prevent access. Enabling SSH enables SCP and disables Telnet.
-pt	<telnet port n>	Define the Telnet port used to communicate with the Rack Power Filter (23 by default).
-ps	<SSH port n>	Define the SSH port used to communicate with the Rack Power Filter (22 by default).
-b	2400 9600 19200 38400	Configure the speed of the serial port connection (9600 bps by default).

Example 1: To enable SSH access to the command line interface, type:

```
console -S ssh
```

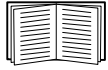
Example 2: To change the Telnet port to 5000, type:

```
console -pt 5000
```

date

Access: Administrator only

Definition: Configure the date used by the Rack Power Filter.



To configure an NTP server to define the date and time for the Rack Power Filter, see “Set the Date and Time” on page 80.

Option	Argument	Description
-d	<“datestring”>	Set the current date. Use the date format specified by the <code>date -f</code> 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 synchronize with other people in different time zones.

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

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

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

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

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

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

delete

Access: Administrator only

Description: Delete a file in the file system.

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

dir

Access: Administrator, Device User, Outlet User

Description: View the files and folders stored on the Rack Power Filter.

dns

Access: Administrator only

Definition: 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, Outlet User

Description: View the date and time you retrieved the event log and the status of the Rack Power Filter. 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.
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.

exit

Access: Administrator, Device User, Outlet User

Description: Exit from the command line interface session.

format

Access: Administrator only

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



Note: To reset the Rack Power Filter to its default configuration, use the `resetToDef` command.

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 from 5001 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 Rack Power Filter (21 by default). The FTP server uses both the specified port and the port one number lower than the specified port.
-S	enable disable	Configure access to the FTP server.

Example: To change the TCP/IP port to 5001, type:
`ftp -p 5001`

help

Access: Administrator, Device User, Outlet User

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

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

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

netstat

Access: Administrator, Device User, Outlet User

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

ntp

Access: Administrator

Description: View and configure the network time protocol parameters.

Option	Argument	Definition
-OM	enable disable	Override the manual settings.
-p	<primary NTP server>	Specify the primary server.
-s	<secondary NTP server>	Specify the secondary server.

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

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

ping

Access: Administrator, Device User

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

Argument	Description
<IP address or DNS name>	Type an IP address with the format <code>xxx.xxx.xxx.xxx</code> , or the DNS name configured by the DNS server.

Example: To determine whether a device with an IP address of 150.250.6.10 is connected to the network, type:

```
ping 150.250.6.10
```

portSpeed

Access: Administrator

Description:

Option	Arguments	Description
-s	auto 10H 10F 100H 100 F	Define the communication speed of the Ethernet port. The <code>auto</code> command enables the Ethernet devices to negotiate to transmit at the highest possible speed. See “Port Speed” on page 63 for more information about the port speed settings.

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

```
portspeed -s 100H
```

prompt

Access: Administrator, Device User

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

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

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

```
prompt -s long
```

quit

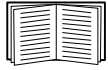
Access: Administrator, Device User, Outlet User

Description: Exit from the command line interface session (this works the same as the `exit` command).

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 “RADIUS” on page 57.

Additional authentication parameters for RADIUS servers are available at the Web interface of the Rack Power Filter. See “RADIUS” on page 57 for more information.

For detailed information about configuring your RADIUS server, see the *Security Handbook*, available at 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.
-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 Rack Power Filter.
-t1 -t2	<server timeout>	The time in seconds that the Rack Power Filter waits for a response from the primary or secondary RADIUS server.

Example 1:

To view the existing RADIUS settings for the Rack Power Filter, type `radius` and press ENTER.

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

```
radius -a radiusLocal
```

Example 3: 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 Rack Power Filter.

resetToDef

Access: Administrator only

Description: Reset all parameters to their default.

Option	Arguments	Description
-p	all keepip	Reset all configuration changes, including event actions, device settings, and, optionally, TCP/IP configuration settings.

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

```
resetToDef -p keepip
```

snmp, snmpv3

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:

```
snmp -S enable
```

system

Access: Administrator only

Description: View and set the system name, the contact, the location and view up time as well as the date and time, the logged-on user, and the high-level system status P, N, A (see “About the Main Screen” on page 12 for more information about system status).

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 Rack Power Filter’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 Rack Power Filter:

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

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

Example 2: To manually configure an IP address of 150.250.6.10 for the Rack Power Filter, type:
`tcpip -i 150.250.6.10`

tcpip6

Access: Administrator only

Description: Enable IPv6 and view and manually configure these network settings for the Rack Power Filter:

Option	Argument	Description
-S	enable disable	Enable or disable IPv6.
-man	enable disable	Enable manual addressing for the IPv6 address of the Rack Power Filter.
-auto	enable disable	Enable the Rack Power Filter to automatically configure the IPv6 address.
-i	<IPv6 address>	Set the IPv6 address of the Rack Power Filter.
-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.

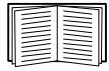
Example 1: To view the network settings of the Rack Power Filter, type `tcpip6` and press ENTER.

Example 2: To manually configure an IPv6 address of 2001:0:0:0:0:FFD3:0:57ab for the Rack Power Filter, type:
`tcpip -i 2001:0:0:0:0:FFD3:0:57ab`

user

Access: Administrator only

Description: Configure the user name, password, and inactivity timeout for the Administrator, Device User, and Read-Only User account types.



For information on the permissions granted to each account type, see “Types of User Accounts” on page 2.

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
```

Example 2: To change the log off time to 10 minutes, type:

```
user -t 10
```

web

Access: Administrator only

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 to 32768. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114, type:

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

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 #>	Define the TCP/IP port used by HTTP to communicate with the Rack Power Filter (80 by default).
-ps	<https port #>	Define the TCP/IP port used by HTTPS to communicate with the Rack Power Filter (443 by default).

Example: To prevent all access to the Web interface, type:

```
web -S disable
```

xferINI

Access: Administrator only

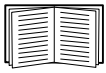
Description: Use XMODEM to upload an INI file while you are accessing the command line interface through a serial connection. After the upload completes:

- 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 Rack Power Filter, you must reset the baud rate to the default to reestablish communication with the Rack Power Filter.

xferStatus

Access: Administrator only

Description: View the result of the last file transfer.



See “Verifying Upgrades and Updates” on page 99 for descriptions of the transfer result codes.

Device Command Descriptions

devEnergySvd

Access: Administrator, Device User

Description: Set or view the amount of energy saved, the amount of money saved, the date of the last reset, the utility rate. Enable or disable the power-saving feature.

Example: View and reset the utility rate.

```
apc> DevEnergySvd

E000: Success
Energy Saved: 0.5 kWh
Money Saved: $ 1.19
Last Reset: 01/01/2010
Utility Rate: 12 Cents/kWh
Power Saving: Enabled
Master Standby Threshold: 10 W
```

```
apc> DevEnergySvd -rate 23
E000: Success
```

```
apc> DevEnergySvd -thrs 15
E000: Success
```

```
apc> DevEnergySvd
E000: Success
Energy Saved: 0.0 kWh
Money Saved: $ 0
Last Reset: 01/01/2010
Utility Rate: 23 Cents/kWh
Power Saving: Enabled
Master Standby Threshold: 15 W
```

devLowVolt

Access: Administrator, Device User

Description: View or set the low voltage warning threshold.

Example1: View the threshold of the low voltage warning.

```
apc> devLowVolt
E000: Success
Low Voltage Threshold: 92 VAC
```

Example 2. Set the low voltage warning threshold to 94 V.

```
apc> devLowVolt 94
E000: Success
```

devOverVolt

Access: Administrator, Device User

Description: View or set the over-voltage warning threshold.

Example1: View the threshold of the high voltage warning.

```
apc> devOverVolt
E000: Success
Over Voltage Threshold: 140 VAC
```

Example 2. Set the low voltage warning threshold to 139 V.

```
apc> devOverVolt 139
E000: Success
```

devReading

Access: Administrator, Device User

Description: View the total energy being used by the device.

Example: View the current (Amps), total power (Watts), input voltage (V), and input frequency (Hz).

```
apc> devReading pwr
E000: Success
Output Power: 5.2 W
```

```
apc> devReading cur
E000: Success
Output Current: 0.3 A
```

```
apc> devReading volt
E000: Success
Line Voltage: 124 V
```

```
apc> devReading freq
E000: Success
Line Frequency: 60 Hz
```

```
apc> devReading ?
Display the output power readings and input source readings
devReading [pwr | cur | volt | freq]
bkLowLoad
```

devStatus

Access: Administrator, Device User

Description: View the status of the device.

Example:

```
apc> devStatus
E000: Success
Line OK: Good
Wiring OK: Good
```

Protection Working: Good

olAutoRbt

Access: Administrator, Device User

Description: Set or view the auto-reboot setting for one or more outlets.

Option	Argument	Description
-c	<Enable/Disable>	Enable or disable Auto-Rebooting feature
-r	<Enable/Disable>	Enable or disable Retry after 24 hours option
-t	<Target host ip address>	Format must be xxx.xxx.xxx.xxx
-s	<Interval between successful ping>	[1 – 6000]
-u	< Interval between failed ping>	[1 – 6000]
-f	<Failed pings before reboot>	[1 – 255]
-d	<Ping Delay after reboot>	[0 – 6000]
-m	<Max retry attempts>	[1 - 255]

Example 1: Enable the auto-reboot function for outlet 3.

```
apc> olAutoRbt 3 -c enable -t www.apc.com
E000: Success
```

olCancelCmd

Access: Administrator, Device User

Description: Cancel a pending command for any outlet.

Example 1: Cancel a pending command for outlet 3.

```
apc> olCancelCmd3
E000: Success
```

olCtrlType

Access: Administrator, Device User

Description: View or set the control mode of an outlet.

Example 1: View the control mode of outlets 3, 5, 6, and 7.

```
apc> olCtrlType 3,5-7
E000: Success
Outlet 3: Master
Outlet 5: Controlled by Master
Outlet 6: Controlled by Master
Outlet 7: Controlled manually
```

Example 2. Set the control mode of outlet 3 to Reboot Only.

```
apc> olCtrlType 3 RebootOnly
```

E000: Success

oIDlyOff

Access: Administrator, Device User

Description: Switch off one or more outlets after the power on/off delay; or switch off all outlets in sequence.

Example 1: Switch off outlet 3.

```
apc> oIDlyOff 3
```

E000: Success

Example 2. Switch off all outlets in sequence.

```
apc> oIDlyOff all
```

E000: Success

oIDlyOn

Access: Administrator, Device User

Description: Switch on one or more outlets after the power on/off delay; or switch on all outlets in sequence.

Example 1: Switch on outlet 3.

```
apc> oIDlyOn 3
```

E000: Success

Example 2. Switch off all of the outlets.

```
apc> oIDlyOn all
```

E000: Success

oIName

Access: Administrator, Device User

Description: View or assign a name to an outlet.

Example 1: View the name assigned to outlet 3.

```
apc> oIName 3
```

E000: Success

Outlet 3: Web Server

Example 2. Assign the name Web Server 2 to outlet 2.

```
apc> oIName 1 "Web Server 2"
```

E000: Success

oIOff

Access: Administrator, Device User

Description: Switch the outlets off.

Example 1: Switch off outlet 3.

```
apc> olOff 3
E000: Success
```

Example 2. Switch off all of the outlets.

```
apc> olOff all
E000: Success
```

olOn

Access: Administrator, Device User

Description: Switch one or more outlets on with no delay.

Example 1: Switch on outlet 3.

```
apc> olOn 3
E000: Success
```

Example 2: Switch on all outlets.

```
apc> olOn all
E000: SuccessolOnOffDly
```

Access: Administrator, Device User

Description: View or set the power on time delay of an outlet.

Example 1: View the delay out outlets 3 and 6.

```
apc> olOnOffDly 3 6
E000: Success
```

Example 2. Set the delay of outlet 3 to six seconds.

```
apc> olOnOffDly 3
E000: Success
Outlet 3: 6 sec
```

olRbootTime

Access: Administrator, Device User

Description: View or set the reboot duration time of one or more outlets, or all outlets.

Example 1: View the reboot duration time of outlet 3.

```
apc> olRbootTime 3
E000: Success
Outlet 3: 4 sec
```

Example 2. Set the reboot duration time of outlet 3 to 10 seconds.

```
apc> olRbootTime 3 10
E000: Success
```

```
apc> olRbootTime 3
E000: Success
```


Outlet 3: 10 sec

olReading

Access: Administrator, Device User

Description: View current (Amps) or the total power (Watts) of an outlet or group of outlets.

Example 1: View the current (Amps) of outlet 3.

```
apc> olReading 3 cur
E000: Success
Outlet 3: 4 A
```

Example 2. View the total power (W) of all the outlets.

```
apc> olReading all pwr
E000: Success
Outlet 3: 100 W
```

olReboot

Access: Administrator, Device User

Description: Perform a power cycle to an outlet or group of outlets.

Example 1: Perform a power cycle to outlet 3.

```
apc> olReboot 3
E000: Success
```

olStatus

Access: Administrator, Device User

Description: View the status of one or more outlets.

Example 1: View the status of outlet 3, 6-7

```
apc> olStatus 3,6-7
E000: Success
Outlet 3: ON*
Outlet 6: OFF
Outlet 7: ON
```

prodInfo

Access: Administrator, Device User, ReadOnly

Description: View information about the Rack Power Filter.

Example 1:

```
apc> prodInfo
E000: Success
AOS v5.1.0
G-Type Rack Power Filter v5.1.0
Model: G50NETB
Present Outlets: 8
```

Switched Outlets: 7
Metered Outlets:5
Max Current:18 A
Phase: 1

vendInfo

Access: Administrator, Device User

Description: View contact information for APC

Example 1:

```
apc> vendInfo  
E000: Success  
Company: APC  
Contact Name: apcav  
Website: www.APCAV.COM  
Phone: 1-888-882-7228
```

Web Interface

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 Power Filter through its Web interface. Other commonly available browsers may work but have not been fully tested by APC.

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

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

Logging On to the Web Interface

Overview

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

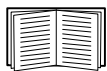
- **apc** for an Administrator
- **device** for a Device User
- **readonly** for a Read-Only User

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

You can set your user interface language as you log on by choosing a language from the **Language** drop-down box.



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



For information about the Web page displayed when you log on, see “About the Device Summary Tab” on page 41.

URL address formats

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

Common browser error messages at log-on.

Error Message	Browser	Cause of the Error
"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
- For a System IPv6 address of 2001:db8:1::2c0:b7ff:fe00:1100 and a non-default Web server port (5000):
 - `http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` if HTTP is your access mode

Web Interface Features

Read the following to familiarize yourself with basic Web interface features for your Power Filter.




Tabs

The following tabs are available:

- **Device Summary:** Appears when you log on. View active alarms, the load status of the Power Filter, and the most recent device events. For more information, see “About the Device Summary Tab” on page 53.
- **Status:** View utility source status, view total load status, view outlets status and power-saving feature status. Reset the accumulated saved energy. For more information, see “About the Device Manager Tab” on page 56.
- **Configuration and Control:** Control the outlets. Configure the unit, and outlets. For more information, see “About configuration and control Tab on page xx.
- **Logs:** View event, data, and system logs.
- **Administration:** Configure security, network connection, notification, and general settings.

Device status icons

One or more icons and accompanying text indicate the current operating status of the Power Filter:

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

At the upper right corner of every page, the Web interface displays the same icons currently displayed on the **Device Summary** page to report Power Filter status:

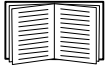
- The **No Alarms** icon if no alarms exist.
- One or both of the other icons (**Critical** and **Warning**) if any alarms exist, and after each icon, the number of active alarms of that severity.

To return to the **Device Summary** tab to view its summary of the Power Filter status, including the active alarms, click a quick status icon on any page of the interface.

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:** The APC download link: <http://www.apc.com/download>.



To reconfigure the links, see “Configure Links” on page 83.

Other Web interface features

- The IP address appears in the upper left corner.
- A context-sensitive **Help** link and **Log off** link are located in the upper right corner.

About the Device Summary Tab

Path: Device Summary

Use the **Device Summary** tab to view active alarms, the load status of the Rack Power Filter, and the most recent device events.

The top left of the page indicates the NMC module name and the location information.

Any existing alarms are indicated with a link to the **Alarm Status** view, where you can view descriptions of each alarm.

In **Status Overview**, you can view various indicators of the status of your UPS including the utility source in VAC and Hz, the total load for the device, etc.

Click **More Status** to access the **Status** tab in order to view more details on the device status including any outlet information, the power-saving status, and to reset the accumulated saved energy and money saved data.

In the **Recent Device Events** area, view, in reverse chronological order, the events that occurred most recently and the dates and times they occurred. A maximum of five events are shown at one time. Click **More Events** to access the **Logs** tab to view the entire event log.

About the Status Tab

Path: Status

Use Status tab to display:

- the utility source's voltage in VAC and frequency in Hz
- total power in KW and total current in AMPS of device.
- outlets' status
- real-time power in KW and current in AMPS on each outlet
- the status of the power saving functions
- and to reset the accumulated saved energy and money

The default starting date for **Energy Saved** and **Money Saved** is 01/01/2010.

The new starting date after clicking the **Reset Now** button is the system date in the NMC. This date can be changed using the **Administration** tab.

About the Configuration and Control Tab

Path: Configuration and Control

Use the Configuration and Control tab to:

- control and configure your outlets
- configure the input cutoff settings
- configure the power-saving threshold or enable smart power tracking
- enable or disable the power-saving function
- configure the AC utility power rate
- configure the company name, the vendor name, the company website, and the company phone number
- view the status of the auto-reboot function for each outlet
- change the outlet name, the power on and off delay, and the reboot duration
- configure the auto-reboot feature

Controlling the outlets

PATH: Configuration and Control > Control

When you apply an outlet control action, the following delays are used for the action:

- For an individual outlet, the action uses the **Power On/Off** delay periods and the **Reboot Duration** configured for that outlet.
- Outlet 1 and 2 are not Switched and only accept the reboot command.
- If the outlet is ON, any **On immediate /Delay** commands to it are rejected.
- If the outlet is OFF, any **OFF immediate/Delayed** and **Reboot Immediate/Delay** commands to it are rejected
- If the outlet is rebooting, any **OFF immediate/Delayed** and **ON immediate/Delayed** commands to it are rejected
- If a command is sent to several outlets, and one outlet rejects it, the command is cancelled to other outlets.
- If an Outlet Type is configured as **Reboot Only**, it cannot be turned on or off.
- If the **All Outlets** check box is selected, selecting an individual outlet is ignored.

Controlling the outlets on your Rack Power Filter:

1. From the **Configuration and Control** tab, select **Control** from the left navigation menu.
2. Select the check boxes for each individual outlet to control, or select the **All Outlets** check box.
3. Select a **Control Action** from the drop-down box, and click **Next >>**. On the confirmation page that explains the action, choose to apply or cancel it.

Control actions you can select

Option	Description
No Action	Do nothing.
On Immediate	Apply power to the selected outlets.
On Delayed	Apply power to each selected outlet according to its value for Power On Delay.
Off Immediate	Remove power from the selected outlets.
Off Delayed	Remove power from each selected outlet according to its value for Power On/Off Delay
Reboot Immediate	Remove power from each selected outlet. Then apply power to each of these outlets according to its value for Reboot Duration.
Reboot Delayed	Remove power from each selected outlet according to its value for Power On/Off Delay Wait until all outlets are off (the highest value for Reboot Duration), and then apply power to each outlet according to its value for Power On/Off Delay.
Cancel Pending Commands	Cancel all commands pending for the selected outlets and keep them in their present state.



Note: 1. If either outlet 1 or 2 is rebooting, sending a Cancel Pending Commands to them causes them to be turned on immediately. This is because outlets 1 and 2 are un-Switched outlets.

Configuring your device settings

Path: Configuration and Control > Configuration > device

For the **Input Cutoff Setting** field:

- the high-voltage threshold range is from 132 to 140
- the low-voltage threshold range is from 92 to 100

Configuring the **Power-Saving Feature**

The range of the **Master Power-On** threshold is from 10 to 85.

The **Master Power-Off** threshold should be **Master Power-On** threshold minus 5. For example, if the Master Power-On threshold is 15 V, and the Master Power-Off threshold should be 10 V.

Steps to enable or disable the **Power-Saving Feature**:

1. From the **Configuration and Control** tab, select **Configuration** and **device**.
2. Select the Enable check box or clear it to enable or disable the power saving feature
3. Click the **Apply** button to make the setting effective

Steps to configure the **Power-Saving** threshold:

1. From the **Configuration and Control** tab, select **Configuration** and **device**.
2. Select the **Watts [10 to 85]** radio button, and then input the threshold. Alternatively, select the **Smart Power Tracking** radio button
3. Click the **Apply** button.

Configuring the **Utility Rate**

The input range of utility rate is from 1 to 254: no decimals are accepted.

Steps to configure the **Utility Rate**:

1. From the **Configuration and Control** tab, select **Configuration** and **device**.
2. Input your utility rate in the box.
3. Click the **Apply** button.

Configuring your **Contact Information**

The maximum length of company, contact name, website, and phone is 16. Any special characters like as “<”, “>” are not accepted.

Steps to configure the contact information:

1. From the **Configuration and Control** tab, select **Configuration** and **device**.
2. Input your company name, contact name, website, and phone in the corresponding input boxes
3. Click the **Apply** button.

Configuring Outlet settings

Path: Configuration and Control > Configuration > outlets

General information:

- The **Power On** and **Power Off Delay** values are not applicable to outlets 1 and 2 and outlet 3.
- Outlet 3 cannot be configured as **Controlled by Master**.
- Outlets 1 and 2 are non-Switched outlet, and only support **Reboot Only**.
- Only outlet 4 can be configured as **Master**.
- Outlets 5 to 8 can be configured as **Controlled by Master**.

Displaying the outlet configuration parameters:

Under **Configuration Summary** area, click on outlet name in the Name column, and the configuration parameters for that outlet display in the bottom half of the screen page.

Configure the outlet setting or outlet name

The following settings are available:

Setting	Description
Name	Set the name for one outlet. The name is displayed next to the outlet number on status screens.
Outlet Type	Set the control type of one outlet
On/Off Delay	Set the number of seconds that the Rack Power Filter waits after a command is issued before applying/Removing power to an outlet.
Reboot Duration	Set the number of seconds an outlet remains off before restarting.

Steps to configure outlet setting or outlet name:

Select the Configuration and Control tab, and then outlet sub-menu under configuration menu from the left navigation menu.

1. From the **Configuration and Control** tab, select **Configuration** and **outlets**.
2. Enter values for Name, Power On/Off Delay, or Reboot Duration, and select the setting of Outlet Type from the drop-list option.
3. Click the **Apply** button.

Configuring the **Auto-Reboot** feature

When the Auto-Reboot feature is enabled, ProAV will operate in Automatic Reboot mode. In this mode, ProAV is configured to periodically confirm that another IP device (such as a server, a computer, a router) is working by sending ping requests to the device.

ProAV expects a response after each ping. If a pre-set number of ping requests fail, it is assumed that the device is not functioning properly. ProAV attempts to return the device to normal operation by rebooting it.

In Automatic Reboot mode, you still have the ability to manually reboot the device from a remote location over the network. When Auto-Reboot feature is disabled, ProAV operates in Normal mode. In Normal mode, ProAV will only change the state of the outputs when commanded by a user.

Notes:

- If the Auto-Reboot feature is enabled on outlet 1 and 2, then they will reboot at same time after a set of pings fail.
- If both the Auto-Reboot and the power saving features are enabled on outlet 4, all the controlled outlet will be turned off by the Master when outlet 4 is rebooting.
- When the outlet is OFF, the ping will be suspended.
- Successful ping will reset Auto-Reboot feature.

Detecting the **target host**

There are hree kind of status for the target host:

Setting	Descriptions
Unknown	The status of target host is unknown. Before sending ping request to the target host, the host status is unknown
Active	Ping response has been received within 1 second after sending out ping request, the target host is active in the network
Inactive	No ping response received within 1 second after sending out ping request, the target host is inactive in the network

Steps to detect the target host

1. From the **Configuration and Control** tab, select **Configuration** and **outlets**.
2. Click the link on the outlet name, and then navigate to the outlet configuration page
3. Enter the value of Target Host IP Address, and click the test button.
The status of the target host is detected and displayed

Configuring the **Auto-Reboot Setting**

The below available setting for Auto-Reboot Configuration for one specified outlet

Setting	Descriptions
Auto-Reboot Enable	By selecting or clearing this check box, you can enable or disable the auto-reboot feature on one specific outlet.
Try again after 24 hours	Retry pinging the target IP after one day after the ProAV failed to reboot the target IP device.
Target Host IP Address	This is the IP address that NMC will ping. This is typically the IP address of the device that will be re-booted upon failure (such as a server, router, computer). It could however, be the address of a device on the opposite side of a communications link when NMC is used to reboot a communication device that does not have an IP address such as a CSU/DSU, satellite modem, router, etc.
Successful Ping Period	This is the time interval (in seconds) between successful ping requests. This time can be set from 1 to 60000 seconds (1000 minutes or 16.666 hours). The factory default for this setting is 60 seconds.

Setting	Descriptions
Unsuccessful Ping Period	When a ping request fails (that is, it gets no response from a device), it may be desirable to begin pinging at a shorter time interval. This enables the ProAV to more quickly determine that the device is not functioning. After each unsuccessful ping, ProAV will wait this time interval (in seconds) before the next ping attempt. This time can be set from 1 to 60000 seconds (1000 minutes or 16.666 hours). The factory default for this setting is 10 seconds
Delay Before First Ping After Reboot	When ProAV is first turned on, it will wait this time interval (in seconds) before beginning to ping the device. This time delay allows the device to boot before being pinged. This time can be set from 0 to 60000 seconds (1000 minutes or 16.666 hours). The factory default for this setting is 120 seconds.
Failed Ping Before Reboot	The device will re-boot after this number of ping failures. This number can range from 1 to 255. The factory default for this setting is 5.
Max. Reboot Attempts	After the device has been re-booted this number of times without any successful pings, it is assumed that there are problems with the device and ProAV will no longer attempt to re-boot the device.

Steps to Configure Auto-Reboot Setting

1. From the **Configuration and Control** tab, select **Configuration** and **outlets**.
2. Click the link on the outlet name, and then navigate to the outlet configuration parameters at the bottom of the page.
3. Enter values for Target Host IP Address, Interval Between Successful Pings, Interval Between Failed Pings, Failed Pings Before Reboot, Ping Delay After Reboot, Max Reboot Attempts , and Check/Uncheck the check box for Auto-Reboot, Enable to retry after 24 hours.
4. Click the **Apply** button.

View the ProAV and Contact information

Path: Configuration and Control > About

The page shows the ProAV device information including device model name, device serial number, device PIC firmware revision, device rating current and device manufacture date

This page also shows the contact information including company name, contact name, website, and phone.

Logs

Using 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.



See “Configuring by event” on page 73.

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

- By default, view the event log as a page of the Web interface. The most recent event is recorded on page 1. In the navigation bar below the log:
 - Click a page number to open a specific page of the log.
 - Click **Previous** or **Next** to view the events recorded immediately before or after the events listed on the open page.
 - Click << to return to the first page or click >> to view the last page of the log.
- 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 Secure CoPy (SCP) to view the event log. See “How to use FTP or SCP to retrieve log files” on page 53.

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

- **Filtering 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 Rack Power Filter 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 Rack Power Filter restarts.

- **Filtering the log by event:** To specify the events that display in the log, click **Filter Log**. Clear the checkbox 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 Rack Power Filter restarts.

To remove an active filter, click **Filter Log**, then **Clear Filter (Show All)**.



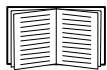
Note: Events are processed through the filter using **OR** logic.

Events that you do not select from the **Filter By Severity** list never display in the filtered event log, even if the event occurs in a category you selected from the **Filter by Category** list.

Events that you do not select from the **Filter by Category** list never display in the filtered event log, even if devices in the category enter an alarm state you selected from the **Filter by Severity** list.

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

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 disable the logging of events based on their assigned severity level or their event category, see “Configuring by event” on page 73.

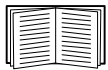
To configure reverse lookup (Logs > Events > reverse lookup):

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.

To resize the event log (Logs > Events > size):

By default, the event log stores 400 events. You can change the number of events the log stores. When you resize the event log, all existing log entries are deleted. To avoid losing log data, use FTP or SCP to retrieve the log before you enter a new value in the **Event Log Size** field.



See “How to use FTP or SCP to retrieve log files” on page 53.

When the log is full, the older entries are deleted.

Data log

Path: **Logs > Data > options**

The data log records the current and power for the device, phase, and banks, as well as temperature and humidity at the specified time interval. Each entry is listed by the date and time the data was recorded.

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

- By default, view the data log as a page of the Web interface. The most recent data item is recorded on page 1. From the navigation menu below the log:
 - Click a page number to open a specific page of the log.
 - Click **Previous** or **Next** to view the data recorded immediately before or after the data that is listed on the open page.
 - Click << to return to the first page of the log, or click >> to view the last page of the log.
- 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.



Alternatively, you can use FTP or SCP to view the data log. See “How to use FTP or SCP to retrieve log files” on page 53.

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

To display the entire 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 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).
Delay <i>X</i> hours between uploads	The number of hours between uploads of data to the file.
Upload every <i>X</i> minutes	The number of minutes between attempts to upload data to the file after an upload failure.
Up to <i>X</i> 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 resize the data log (Logs > Data > size):

By default, the data log stores 1000 records. You can change the number of records the log stores. When you resize the data log, all existing log records are deleted. To avoid losing records, use FTP or SCP to retrieve the log before you enter a new value in the **Data Log Size** field.



See “How to use FTP or SCP to retrieve log files” on page 53.

When the log is full, the older entries are deleted.

How to use FTP or SCP to retrieve log files

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

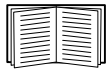
- The file reports all events or data recorded since the log was last deleted or (for the data log) truncated because it reached maximum size.
- The file includes information that the event log or data log does not display.
 - The version of the file format (first field)
 - The date and time the file was retrieved
 - The **Name**, **Contact**, and **Location** values and IP address of the Rack Power Filter
 - The unique **Event Code** for each recorded event (*event.txt* file only)



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

If you are using the encryption-based security protocols for your system, use SCP to retrieve the log file.

If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.



See the *Security Handbook*, available at www.apc.com, for information on available protocols and methods for setting up the type of security you need.

To use SCP to retrieve the files. To 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:

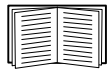
```
scp username@hostname_or_ip_address:data.txt ./data.txt
```

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 Rack Power Filter, and press ENTER.

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

```
ftp>open ip_address port_number
```



To set a non-default port value to enhance security for the FTP Server, see “FTP Server” on page 71. You can specify any port from 5001 to 32768.

2. Use the case-sensitive **User Name** and **Password** for Administrator or Device User to log on. For Administrator, **apc** is the default for **User Name** and **Password**. For the Device User, the defaults are **device** for **User Name** and **apc** for **Password**.
3. Use the **get** command to transmit the text of a log to your local drive.

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

or

```
ftp>get data.txt
```
4. Type `quit` at the `ftp>` prompt to exit from FTP.

Administration: Security

Local Users

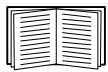
Setting user access

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

The Administrator user account always has access to the Rack Power Filter.

The Device User accounts are enabled by default. To disable the Device User or Read-Only User accounts, select the user account from the left navigation menu, then clear the **Enable** checkbox.

You set the case-sensitive user name and password for each account type in the same manner. Maximum length is 64 characters for a user name and 64 characters for a password. Blank passwords (passwords with no characters) are not allowed.



For information on the permissions granted to each account type (Administrator, Device User, and Read-Only User), see “Types of User Accounts” on page 2.

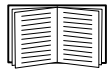
Account Type	Default User Name	Default Password	Permitted Access
Administrator	apc	apc	Web interface and command line interface
Device User	device	apc	
Read-Only User	readonly	apc	Web interface only

Remote Users

Authentication

Path: Administration > Security > Remote Users > Authentication Method

Use this option to select how to administer remote access to the Rack Power Filter.]



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

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

- When a user accesses the Rack Power Filter or other network-enabled device that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user's permission level.
- RADIUS user names used with the Rack Power Filter 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, remote access is unavailable to all users. You must use a serial connection to the command line interface and change the **access** setting to **local** or **radiusLocal** to regain access. For example, the command to change the access setting to **local** would be:
radius -a local

RADIUS

Path: Administration > Security > Remote Users > RADIUS

Use this option to do the following:

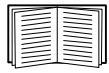
- List the RADIUS servers (a maximum of two) available to the Rack Power Filter and the time-out period for each.
- Click on a link, and configure the parameters for authentication by a new RADIUS server.
- Click a listed RADIUS server to display and modify its parameters.

RADIUS Setting	Definition
RADIUS Server	The server name or IP address (IPv4 or IPv6) of the RADIUS server. Click on a link to configure the server. Note:RADIUS servers use port 1812 by default to authenticate users. 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 Rack Power Filter.
Timeout	The time in seconds that the Rack Power Filter 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.

Configuring the RADIUS Server

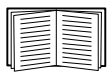
Summary of the configuration procedure

You must configure your RADIUS server to work with the Rack Power Filter.



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

1. Add the IP address of the Rack Power Filter 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 *Security Handbook* for an example.

3. VSAs can be used instead of the Service-Type attributes provided by the RADIUS server. VSAs require a dictionary entry and a RADIUS users file. In the dictionary file, define the names for the ATTRIBUTE and VALUE keywords, but not for the numeric values. If you change numeric values, RADIUS authentication and authorization will fail. VSAs take precedence over standard RADIUS attributes.

Configuring a RADIUS server on UNIX[®] with shadow passwords

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

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

```
DEFAULT      Auth-Type = System
              APC-Service-Type = Admin
```

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

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

Supported RADIUS servers

FreeRADIUS and Microsoft IAS 2003 are supported. Other commonly available RADIUS applications may work but have not been fully tested.

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 can log on until the time specified as **Minutes of Inactivity** expires. For example, with the default value for **Minutes of Inactivity**, if a user closes the browser window without logging off, no user can log on for 3 minutes.

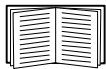
Administration: Network Features

TCP/IP and Communication Settings

TCP/IP settings

Path: Administration > Network > TCP/IP

The **TCP/IP** option on the left navigation menu, selected by default when you choose **Network** on the top menu bar, displays the current IPv4 address, subnet mask, default gateway, MAC address, and boot mode of the Rack Power Filter.



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

Setting	Description
Enable	Enable or disable IPv4 with this check box.
Manual	Configure IPv4 manually by entering the IP address, subnet mask, and default gateway.
BOOTP	<p>A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Rack Power Filter requests network assignment from any BOOTP server:</p> <ul style="list-style-type: none">• If the Rack Power Filter receives a valid response, it starts the network services.• If the Rack Power Filter finds a BOOTP server, but a request to that server fails or times out, the Rack Power Filter stops requesting network settings until it is restarted.• By default, if previously configured network settings exist, and the Rack Power Filter receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible. <p>Click Next>> to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail :¹</p> <ul style="list-style-type: none">• Maximum retries: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.• If retries fail: Select Use prior settings (the default) or Stop BOOTP request.
DHCP	<p>The default setting. At 32-second intervals, the Rack Power Filter requests network assignment from any DHCP server.</p> <ul style="list-style-type: none">• If the Rack Power Filter receives a valid response, it does not (as previously) require the APC cookie from the DHCP server in order to accept the lease and start the network services.• If the Rack Power Filter finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted.¹• Require vendor specific cookie to accept DHCP Address: By selecting this check box, you can require the DHCP server to provide a cookie which supplies information to the Rack Power Filter.
<p>¹. The default values for these three settings on the configuration pages generally do not need to be changed:</p> <ul style="list-style-type: none">• Vendor Class: APC• Client ID: The MAC address of the Rack Power Filter, which uniquely identifies it on the local area network (LAN)• User Class: The name of the application firmware module	

DHCP response options

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

Vendor Specific Information (option 43). The Rack Power Filter uses this option in a DHCP response to determine whether the DHCP response is valid. This option contains an APC-specific options in a TAG/LEN/DATA format, called the APC Cookie. This is disabled by default.

- **APC Cookie. Tag 1, Len 4, Data “1APC”**

Option 43 communicates to the Rack Power Filter that a DHCP server is configured to service devices.

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie:

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

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

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

Other options. The Rack Power Filter 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 Rack Power Filter can use.
- **Time Offset** (option 2): The offset of the Rack Power Filter'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 Rack Power Filter can use.
- **Host Name** (option 12): The host name that the Rack Power Filter will use (32-character maximum length).

- **Domain Name** (option 15): The domain name that the Rack Power Filter will use (64-character maximum length).
- **Boot File Name** (from the **file** field of the DHCP response, described in **RFC2131**): The fully qualified directory-path to a user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the Rack Power Filter will download the .ini file. After the download, the Rack Power Filter uses the .ini file as a boot file to reconfigure its settings.

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

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

Ping Response

Path: Administration > Network > Ping Response

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

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** to configure and test the Domain Name System (DNS):

- Select **Primary DNS Server** or **Secondary DNS Server** to specify the IPv4 or IPv6 addresses of the primary and optional secondary DNS server. For the Rack Power Filter to send e-mail, you must at least define the IP address of the primary DNS server.
 - The Rack Power Filter 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 Rack Power Filter does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the Rack Power Filter 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.
- **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 NMC interface (except e-mail addresses) that accepts a domain name.
- **Domain Name (IPv4):** You need to configure the domain name here only. In all other fields in the NMC interface (except e-mail addresses) that accept domain names, the NMC 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 (for example, when defining a trap receiver), include a trailing period. The NMC recognizes a host name with a trailing period (such as `mySnmpServer.`) as if it were a fully-qualified domain name and does not append the domain name.
- **Domain Name (IPv6):** Specify the IPv6 domain name here.
- 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, <code>my_server.my_domain</code>
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	<p>To activate changes to any of these selections, log off from the Rack Power Filter:</p> <ul style="list-style-type: none">• Disable: Disables access to the Web interface. (To re-enable access, log in to the command line interface, then type the command <code>http -S enable</code>. For HTTPS access, type <code>https -S enable</code>.)• 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 Rack Power Filter by digital certificate. When HTTPS is enabled, your browser displays a small lock icon. <p>See “Creating and Installing Digital Certificates” in the <i>Security Handbook</i>, available at www.apc.com.</p> <p>HTTP Port: The TCP/IP port (80 by default) used to communicate by HTTP with the Rack Power Filter.</p> <p>HTTPS Port: The TCP/IP port (443 by default) used to communicate by HTTPS with the Rack Power Filter.</p> <p>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:</p> <pre>http://152.214.12.114:5000 https://152.214.12.114:5000</pre>

Option	Description
ssl certificate	<p>Add, replace, or remove a security certificate.</p> <p>Status:</p> <ul style="list-style-type: none"> • Not installed: A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Using Add or Replace Certificate File installs the certificate to the correct location, /ssl on the Rack Power Filter. • Generating: The Rack Power Filter is generating a certificate because no valid certificate was found. • Loading: A certificate is being activated on the Rack Power Filter. • Valid certificate: A valid certificate was installed or was generated by the Rack Power Filter. Click on this link to view the contents of the certificate. <p>If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the Rack Power Filter generates a default certificate, a process which delays access to the interface for up to one minute. You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on.</p> <p>Add or Replace Certificate File: Enter or browse to the certificate file created with the Security Wizard.</p> <p>See “Creating and Installing Digital Certificates” in the <i>Security Handbook</i>, available at www.apc.com, to choose a method for using digital certificates created by the Security Wizard or generated by the Rack Power Filter.</p> <p>Remove: Delete the current certificate.</p>

Console

Path: Administration > Network > Console > *options*

Option	Description
access	<p>Choose one of the following for access by Telnet or Secure SHell (SSH):</p> <ul style="list-style-type: none"> • Disable: Disables all access to the command line interface. • Enable Telnet (the default): Telnet transmits user names, passwords, and data without encryption. • Enable SSH: SSH transmits user names, passwords, and data in encrypted form, providing protection from attempts to intercept, forge, or alter data during transmission. <p>Configure the ports to be used by these protocols:</p> <ul style="list-style-type: none"> • Telnet Port: The Telnet port used to communicate with the Rack Power Filter (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: <pre style="margin-left: 40px;">telnet 152.214.12.114 :5000 telnet 152.214.12.114 5000</pre> • SSH Port: The SSH port used to communicate with the Rack Power Filter (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port.
ssh host key	<p>Status indicates the status of the host key (private key):</p> <ul style="list-style-type: none"> • SSH Disabled: No host key in use: When disabled, SSH cannot use a host key. • Generating: The Rack Power Filter is creating a host key because no valid host key was found. • Loading: A host key is being activated on the Rack Power Filter. • Valid: One of the following valid host keys is in the <code>/ssh</code> directory (the required location on the Rack Power Filter): <ul style="list-style-type: none"> • A 1024-bit or 2048-bit host key created by the Security Wizard • A 2048-bit RSA host key generated by the Rack Power Filter <p>Add or Replace: Browse to and upload a host key file created by the Security Wizard.</p> <p>To use the APC Security Wizard, see the <i>Security Handbook</i>, available at www.apc.com.</p> <p>Note: To reduce the time required to enable SSH, create and upload a host key in advance. If you enable SSH with no host key loaded, the Rack Power Filter takes up to one minute to create a host key, and the SSH server is not accessible during that time.</p> <p>Remove: Remove the current host key.</p>



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

SNMP

All user names, passwords, and community names for SNMP are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMP access or set the access for each community to Read. (A community with Read access can receive status information and use SNMP traps.)

When using InfraStruxure Central to manage a Rack Power Filter on the public network of an InfraStruxure system, you must have SNMP enabled in the Rack Power Filter interface. Read access will allow the InfraStruxure device to receive traps from the Rack Power Filter, but Write access is required while you use the interface of the Rack Power Filter to set the InfraStruxure device as a trap receiver.



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

SNMPv1

Path: Administration > Network > SNMPv1 > options

Option	Description
access	Enable SNMPv1 Access: Enables SNMP version 1 as a method of communication with this device.
access control	<p>You can configure up to four access control entries to specify which Network Management Systems (NMSs) have access to this device. The opening page for access control, by default, assigns one entry to each of the four available SNMPv1 communities, but you can edit these settings to apply more than one entry to any community to grant access by several specific IPv4 and IPv6 addresses, host names, or IP address masks. To edit the access control settings for a community, click its community name.</p> <ul style="list-style-type: none"> • 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. <p>Community Name: The name that an NMS must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are <code>public</code>, <code>private</code>, <code>public2</code>, and <code>private2</code>.</p> <p>NMS IP/Host Name: The IPv4 or IPv6 address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows:</p> <ul style="list-style-type: none"> • 149.225.12.255: Access only by an NMS on the 149.225.12 segment. • 149.225.255.255: Access only by an NMS on the 149.225 segment. • 149.255.255.255: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. <p>Access Type: The actions an NMS can perform through the community.</p> <ul style="list-style-type: none"> • Read: GETS only, at any time • Write: GETS at any time, and SETS when no user is logged onto the Web interface or command line interface. • Write+: GETS and SETS at any time. • Disable: 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 Rack Power Filter supports SHA or MD5 authentication and AES or DES encryption.

Option	Description
access	SNMPv3 Access: Enables SNMPv3 as a method of communication with this device.
user profiles	<p>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.</p> <p>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.</p> <p>Authentication Passphrase: A phrase of 15 to 32 ASCII characters (<code>apc auth passphrase</code>, 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.</p> <p>Privacy Passphrase: A phrase of 15 to 32 ASCII characters (<code>apc crypt passphrase</code>, 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.</p> <p>Authentication Protocol: The APC implementation of SNMPv3 supports SHA and MD5 authentication. Authentication will not occur unless an authentication protocol is selected.</p> <p>Privacy Protocol: The implementation of SNMPv3 supports AES and DES as the protocols for encrypting and decrypting data. Privacy of transmitted data requires that a privacy protocol is selected and that a privacy passphrase is provided in the request from the NMS. When a privacy protocol is enabled but the NMS does not provide a privacy passphrase, the SNMP request is not encrypted.</p> <p>Note: You cannot select the privacy protocol if no authentication protocol is selected.</p>

Option	Description
access control	<p>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.</p> <ul style="list-style-type: none"> • 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. <p>To edit the access control settings for a user profile, click its user name.</p> <p>Access: Mark the Enable checkbox to activate the access control specified by the parameters in this access control entry.</p> <p>User Name: From the drop-down list, select the user profile to which this access control entry will apply. The choices available are the four user names that you configure through the user profiles option on the left navigation menu.</p> <p>NMS IP/Host Name: The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows:</p> <ul style="list-style-type: none"> • 149.225.12.255: Access only by an NMS on the 149.225.12 segment. • 149.225.255.255: Access only by an NMS on the 149.225 segment. • 149.255.255.255: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default 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

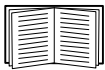
The **FTP Server** settings enable (by default) or disable access to the FTP server and specify the TCP/IP port (21 by default) that the FTP server uses to communicate with the Rack Power Filter. The FTP server uses both the specified port and the port one number lower than the specified port.

You can change the **Port** setting to the number of any unused port from 5001 to 32768 for added security. Users must then use a colon (:) to specify the non-default port number. For example, for port 5001 and IP address 152.214.12.114, the command would be `ftp 152.214.12.114:5001`.



Note: FTP transfers files without encryption. For higher security, disable the FTP server, and transfer files with SCP. Selecting and configuring Secure SHell (SSH) enables SCP automatically.

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



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

Administration: Notification

Event Actions

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

Types of notification

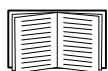
You can configure event actions to occur in response to an event or group of events. These actions notify users of the event in any of several ways:

- Active, automatic notification. The specified users or monitoring devices are contacted directly.
 - E-mail notification
 - SNMP traps
 - Syslog notification
- Indirect notification
 - Event log. If no direct notification is configured, users must check the log to determine which events have occurred



You can also log system performance data to use for device monitoring. See “Data log” on page 51 for information on how to configure and use this data logging option.

- Queries (SNMP GETs)



For more information, see “SNMP” on page 68. SNMP enables an NMS to perform informational queries. For SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without the risk of allowing remote configuration changes.

Configuring 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.

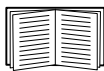
Parameter	Description
Delay x time before sending	If the event persists for the specified time, a notification is sent. If the condition clears before the time expires, no notification is sent.
Repeat at an interval of x time	The notification is sent at the specified interval (e.g., every 2 minutes).
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.

Configuring 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 paging, 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” on page 78
- “E-mail recipients” on page 74
- “Trap Receivers” on page 76

Configuring 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” on page 64.)
- The IP address or DNS name for **SMTP Server** and **From Address**. (See “SMTP” on page 74.)
- The e-mail addresses for a maximum of four recipients. (See “E-mail recipients” on page 74.)



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 IPv4/IPv6 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” on page 74.
From Address	The contents of the From field in e-mail messages sent by the Rack Power Filter: <ul style="list-style-type: none">• In the format <i>user@ [IP_address]</i> (if an IP address is specified as Local SMTP Server)• In the format <i>user@domain</i> (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, <i>myacct100@skytel.com</i>). 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 <i>jsmith@[xxx.xxx.x.xxx]</i> instead of <i>jsmith@company.com</i> . This is useful when DNS lookups are not working correctly. Note: The recipient’s pager must be able to use text-based messaging.
E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.

Setting	Description
SMTP Server	<p>Select one of the following methods for routing e-mail:</p> <ul style="list-style-type: none"> • Local: Through the Rack Power Filter's SMTP server. This setting (recommended) ensures that the e-mail is sent before the Rack Power Filter's 20-second time-out, and, if necessary, is retried several times. Also do one of the following: <ul style="list-style-type: none"> • Enable forwarding at the Rack Power Filter'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 Rack Power Filter to forward e-mail to an external mail account. • Recipient: Directly to the recipient's SMTP server. With this setting, the Rack Power Filter 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. <p>When the recipient uses the Rack Power Filter's SMTP server, this setting has no effect.</p>
Format	<p>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.</p>
Language	<p>Chose a language from the drop-down list and any mails will be sent in that language. It is possible to use different languages for different users.</p>
User Name Password Confirm Password	<p>If your mail server requires authentication, type your user name and password here. This performs a simple authentication, not SSI.</p>

E-mail test.

Path: 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 configure 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 IPv4/IPv6 address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.
Language	Choose a language from the drop-down list. This can differ from the UI and from other trap receivers.

SNMPv1 option.

Item	Definition
Community Name	The name (<code>public</code> 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” on page 69 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:

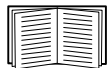
- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver is enabled.
- If a host name is selected for the **To** address, that host name can be mapped to a valid IP address.

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

Syslog

Path: Logs > Syslog > *options*

The Rack Power Filter 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 IPv4/IPv6 addresses or host names to identify from one to four servers to receive Syslog messages sent by the Rack Power Filter.
Port	The user datagram protocol (UDP) port that the Rack Power Filter will use to send Syslog messages. The default is 514 , the UDP port assigned to Syslog.
Protocol	Choose between UDP and TCP.
Language	Choose the language for any Syslog messages.

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 Rack Power Filter's Syslog messages (User , by default). Note: User best defines the Syslog messages sent by the Rack Power Filter. Do not change this selection unless advised to do so by the Syslog network or system administrator.
Severity Mapping	Maps each severity level of Rack Power Filter or Environment events to available Syslog priorities. You should not need to change the mappings. The following definitions are from RFC3164: <ul style="list-style-type: none">• 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 Local Priority settings: <ul style="list-style-type: none">• Severe is mapped to Critical• Warning is mapped to Warning• Informational is mapped to Info Note:To disable Syslog messages, see “Configuring event actions” on page 72.

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 Rack Power Filter.
 - The Header: a time stamp and the IP address of the Rack Power Filter.
 - 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.

Administration: General Options

Identification

Path: Administration > General > Identification

Define the **Name** (the device name), **Location** (the physical location), and **Contact** (the person responsible for the device) used by InfraStruxure Central and the SNMP agent of the Rack Power Filter. 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 at www.apc.com.

Set the Date and Time

Mode

Path: Administration > General > Date & Time > mode

Set the time and date used by the Rack Power Filter. 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 Rack Power Filter.
 - Mark the checkbox **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 Rack Power Filter.



Note: By default, any Rack Power Filter on the private side of an InfraStruxure Central obtains its time settings by using InfraStruxure Central as an NTP server.

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 Rack Power Filter accesses the NTP Server for an update. <i>Minimum:</i> 1; <i>Maximum:</i> 8760 (1 year).
Update Using NTP Now	Initiate an immediate update of the 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

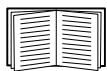
Select the numerical format in which to display all dates in this user interface. In the selections, each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.

Use an .ini File

Path: Administration > General > User Config File

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

Status	Reports the progress of the upload. The upload succeeds even if the file contains errors, but a system event reports the errors in the event log.
Upload	Browse to the customized file and upload it so that the current Rack Power Filter can use it to set its own configuration.



To retrieve and customize the file of a configured Rack Power Filter, see “How to Export Configuration Settings” on page 88.

Instead of uploading the file to one Rack Power Filter, you can export the file to multiple Rack Power Filters by using an FTP or SCP script or a batch file and the .ini file utility, available at www.apc.com/tools/download.

Event Log and Temperature Units

Path: Administration > General > Preferences

Color-code event log text

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

Text Color	Alarm Severity
Red	Critical: A critical alarm exists, which requires immediate action.
Orange	Warning: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
Green	Alarm Cleared: The conditions that caused the alarm have improved.
Black	Normal: No alarms are present. The Rack Power Filter and all connected devices are operating normally.

Change the default temperature scale

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

Reset the Rack Power Filter

Path: Administration > General > Reset/Reboot

Action	Definition
Reboot Management Interface	Restarts the interface of the Rack Power Filter.
Reset All ¹	Clear the Exclude TCP/IP checkbox to reset all configuration values; mark the Exclude TCP/IP checkbox to reset all values except TCP/IP.
Reset Only ¹	TCP/IP settings: Set TCP/IP Configuration to DHCP & BOOTP , its default setting, requiring that the Rack Power Filter receive its TCP/IP settings from a DHCP or BOOTP server. See “TCP/IP and Communication Settings” on page 60.
	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.	

Configure 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 Web-enabled products.
- **Link 3:** The APC download link: <http://www.apc.com/download>.

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 Rack Power Filter

Path: Administration > General > About

The hardware information is useful to APC Customer Support for troubleshooting problems with the Rack Power Filter. The serial number and MAC address are also available on the Rack Power Filter itself.

Firmware information for the Application Module, APC OS (AOS), and APC Boot Monitor indicates the name, the firmware version, and the date and time each firmware module was created. This information is also useful in troubleshooting and enables you to determine if updated firmware is available at the APC Web site.

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

Device IP Configuration Wizard

Capabilities, Requirements, and Installation

How to use the Wizard to configure TCP/IP settings

The Device IP Configuration Wizard configures the IP address, subnet mask, and default gateway of one or more Rack Power Filters or network-enabled devices (devices containing an embedded APC Network Management Card [NMC]). You can use the Wizard in either of the following ways:

- Remotely over your TCP/IP network to discover and configure unconfigured Rack Power Filters or devices on the same network segment as the computer running the Wizard.
- Through a direct connection from a serial port of your computer to a Rack Power Filter or device to configure or reconfigure it.

System requirements

The Wizard runs on Microsoft Windows 2000, Windows Server[®] 2003, and Windows XP operating systems.

Installation

To install the Wizard from a downloaded executable file:

1. Go to **www.apc/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

Most software firewalls must be temporarily disabled for the Wizard to discover unconfigured Rack Power Filters.

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 Rack Power Filters or network-enabled devices, 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 can be found:
 - On a label on the device
 - On the Quality Assurance slip that came with the Rack Power Filter or device

Run the Wizard to perform the configuration. To discover and configure the unconfigured Rack Power Filters or network-enabled devices over the network:

1. From the **Start** menu, launch the Wizard. The Wizard detects the first Rack Power Filter or network-enabled device 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 Rack Power Filter or device identified by the MAC address. Click **Next >**.

On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the Rack Power Filter or device 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 Rack Power Filter or device, it displays the screen to enter TCP/IP settings. Repeat this procedure beginning at step 3, or to skip the Rack Power Filter or device 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 provided serial configuration cable (APC part number 940-0299) from an available communications port on your computer to the serial port of the Rack Power Filter or device. Make sure no other application is using the computer port.
3. From the **Start** menu, launch the Wizard application.
4. If the Rack Power Filter or network-enabled device 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 Rack Power Filter or device, and click **Next >**.
7. On the **Transmit Current Settings Remotely** screen, if you select **Start a Web browser when finished**, the default Web browser connects to the Rack Power Filter or device 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 6, you can now configure other parameters through the Web interface of the Rack Power Filter or device.

How to Export Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

An Administrator can retrieve the .ini file of a Rack Power Filter and export it to another Rack Power Filter or to multiple Rack Power Filters.

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

Each receiving Rack Power Filter uses the file to reconfigure its own settings and then deletes it.

Contents of the .ini file

The config.ini file you retrieve from a Rack Power Filter 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 Rack Power Filter settings. Each keyword is followed by an equals sign and a value (either the default or a configured value).
- The `Override` keyword: With its default value, this keyword prevents the exporting of one or more keywords and their device-specific values. For example, in the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the Rack Power Filter) 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:

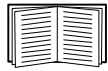
1. If possible, use the interface of a Rack Power Filter to configure it with the settings to export. Directly editing the .ini file risks introducing errors.
2. To use FTP to retrieve config.ini from the configured Rack Power Filter:
 - a. Open a connection to the Rack Power Filter, using its IP address:

```
ftp> open ip_address
```

- b. Log on using the Administrator user name and password.
- c. Retrieve the config.ini file containing the Rack Power Filter's settings:

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

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



To retrieve configuration settings from multiple Rack Power Filters and export them to other Rack Power Filters, see *Release Notes: ini File Utility, version 1.0*, available at 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 Rack Power Filters 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 Rack Power Filter. To transfer the .ini file to another Rack Power Filter, do either of the following:

- From the Web interface of the receiving Rack Power Filter, 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 Rack Power Filters, 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 Rack Power Filter to which you are exporting the .ini file:

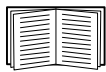
```
ftp> open ip_address
```

- b. Export the copy of the customized .ini file to the root directory of the receiving Rack Power Filter:

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

Exporting the file to multiple Rack Power Filters. To export the .ini file to multiple Rack Power Filters:

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



To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0*, available at www.apc.com.

The Upload Event and Error Messages

The event and its error messages

The following event occurs when the receiving Rack Power Filter completes using the .ini file to update its settings.

Configuration file upload complete, with *number* valid values

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

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

Messages in config.ini

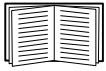
A Rack Power Filter from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the Rack Power Filter is not present or is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values. For example:

```
Rack Power Filter not discovered
```

If you did not intend to export the configuration of the Rack Power Filter as part of the .ini file import, ignore these messages.

Errors generated by overridden values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values.

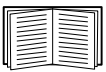


See “Contents of the .ini file” on page 88 for information about which values are overridden.

Because the overridden values are device-specific and not appropriate to export to other Rack Power Filters, ignore these error messages. To prevent these error messages, delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Related Topics

On Windows operating systems, instead of transferring .ini files, you can use the APC Device IP Configuration Wizard to update the basic TCP/IP settings of the Rack Power Filter and configure other settings through its user interface.



See “Device IP Configuration Wizard” on page 85.

File Transfers

How to Upgrade Firmware

Benefits of upgrading firmware

When you upgrade the firmware on the Rack Power Filter:

- 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 Rack Power Filters support the same features in the same manner.

Firmware files

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

The APC Operating System (AOS), application, and boot monitor module files used with the Rack Power Filter 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 the APC Operating System (AOS) module, the application module, or the boot monitor module for the Rack Power Filter.
- ***version***: The version number of the file.
- ***bin***: Indicates that this is a binary file.

Obtaining the latest firmware version



Note: In a manual upgrade, you can skip the bootmon installation if there are no updates. With the Firmware Upgrade Utility, any bootmon update is automatic.

Firmware Upgrade Utility for Microsoft Windows systems. The Firmware Upgrade Utility automates the transferring of the firmware modules on any supported Windows operating system. Obtain the latest version of the utility at no cost from www.apcc.com/tools/download. At this Web page, find the latest firmware release for your product and, included in it, the automated utility. **Never** use a utility designated for one product to upgrade the firmware of another product.

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 Rack Power Filters by using the separate AOS and application firmware modules.



Note: In manual upgrades, load the boot monitor first, then the APC operating system module, and finally, the application module.

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



Warning: Before attempting a firmware upgrade, turn off any connected appliances.

To upgrade the firmware of a Rack Power Filter, use one of these methods below:

- From a networked computer running a Microsoft Windows operating system, use the firmware upgrade tool downloaded from the APC Web site.



Note: The tool only works with a Rack Power Filter that has an IPv4 address.

- From a networked computer on any supported operating system, use FTP or SCP to transfer the individual AOS and application firmware modules.
- For a Rack Power Filter that is not on your network, use XMODEM through a serial connection to transfer the individual firmware modules from your computer to the Rack Power Filter.



Warning: When you transfer individual firmware modules, **you must** transfer the APC Operating System (AOS) module to the Rack Power Filter before you transfer the application module.

Using FTP or SCP to upgrade one Rack Power Filter

FTP. To use FTP to upgrade one Rack Power Filter over the network:

- The Rack Power Filter 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 Rack Power Filter.
- The firmware files must be extracted from the firmware upgrade tool (see “To extract the firmware files:” on page 94).

To transfer the files:

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

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

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

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

- `apc_hw05_aos_xxx.bin`
- `apc_hw05_application_xxx.bin`

2. Open an FTP client session:

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

3. Type `open` and the IP address of the Rack Power Filter, 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_hw05_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 the Rack Power Filter:

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 Rack Power Filter. The following example uses *xxx* to represent the version number of the AOS module:

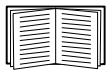
```
scp apc_hw05_aos_xxx.bin apc@158.205.6.185:apc_hw05_aos_xxx.bin
```

3. Use a similar SCP command line, with the name of the application module, to transfer the application firmware module to the Rack Power Filter.

How to upgrade multiple Rack Power Filters

Firmware Upgrade Utility. Use this for multiple firmware updates in IPv4 if you have Windows. The utility records all upgrade steps in a log as a good reference to validate the upgrade.

Export configuration settings. You can create batch files and use a utility to retrieve configuration settings from multiple Rack Power Filters and export them to other Rack Power Filters.



See *Release Notes: ini File Utility, version 1.0*, available at www.apc.com.

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

Using the Firmware Upgrade Utility for multiple upgrades

After downloading from the APC website, double click on the .exe file to run the utility (which ONLY works with IPv4) and follow these steps to upgrade your Rack Power Filter firmware:

1. Type in an IP address, a user name, and a password, and choose the **Ping** button if you need to verify an IP address.
2. Choose the **Device List** button to open the `iplist.txt` file. This should list any device IP, user name, and password, for example,
SystemIP=192.168.0.1
SystemUserName=apc
SystemPassword=apc

The new utility works fine with any existing `iplist.txt` file that you have used with the old version of the utility.

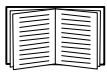
3. Select the **Upgrade From Device List** check box to use the `iplist.txt` file. Clear this check box to upgrade the firmware using the IP, user name and password you typed on the dialog box.
4. Choose the **Upgrade Now** button to start the firmware version update(s).
5. Choose **View Log** to verify any upgrade.

Using XMODEM to upgrade one Rack Power Filter

To use XMODEM to upgrade one Rack Power Filter that is not on the network, you must extract the firmware files from the firmware upgrade tool (see “To extract the firmware files:” on page 94).

To transfer the files:

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect the provided serial configuration cable (APC part number 940-0144A) to the selected port and to the serial port at the Rack Power Filter.
3. Run a terminal program such as HyperTerminal, and configure the selected port for 57600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press the RESET button on the Rack Power Filter, then immediately press the ENTER key twice, or until the Boot Monitor prompt displays: `BM>`
5. Type `XMODEM`, then press ENTER.
6. From the terminal program’s menu, select XMODEM, then select the binary AOS firmware file to transfer using XMODEM. After the XMODEM transfer is complete, the Boot Monitor prompt returns.
7. To install the application module, repeat step 5 and step 6. In step 6, use the application module file name.
8. Type `reset` or press the Reset button to restart the Rack Power Filter.



For information about the format used for firmware modules, see “Firmware files” on page 93.

Verifying Upgrades and Updates

Verify the success or failure of the transfer

To verify whether a firmware upgrade succeeded, use the `xferStatus` command in the command line interface to view the last transfer result, or use an SNMP GET to the `mfiletransferStatusLastTransferResult` OID.

Last Transfer Result codes

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. In the command line interface, use the `about` command.

Troubleshooting

Rack Power Filter Access Problems

Problem	Solution
Unable to ping the Rack Power Filter	<p>If the Rack Power Filter's Status LED is green, try to ping another node on the same network segment as the Rack Power Filter. If that fails, it is not a problem with the Rack Power Filter. If the Status LED is not green, or if the ping test succeeds, perform the following checks:</p> <ul style="list-style-type: none">• Verify all network connections.• Verify the IP addresses of the Rack Power Filter and the NMS.• If the NMS is on a different physical network (or subnetwork) from the Rack Power Filter, verify the IP address of the default gateway (or router).• Verify the number of subnet bits for the Rack Power Filter's subnet mask.
Cannot allocate the communications port through a terminal program	<p>Before you can use a terminal program to configure the Rack Power Filter, you must shut down any application, service, or program using the communications port.</p>
Cannot access the command line interface through a serial connection	<p>Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.</p>
Cannot access the command line interface remotely	<ul style="list-style-type: none">• Make sure you are using the correct access method, Telnet or Secure Shell (SSH). An Administrator can enable these access methods. By default, Telnet is enabled. Enabling SSH automatically disables Telnet.• For SSH, the Rack Power Filter may be creating a host key. The Rack Power Filter can take up to one minute to create the host key, and SSH is inaccessible for that time.
Cannot access the Web interface	<ul style="list-style-type: none">• Verify that HTTP or HTTPS access is enabled.• Make sure you are specifying the correct URL — one that is consistent with the security system used by the Rack Power Filter. SSL requires https, not http, at the beginning of the URL.• Verify that you can ping the Rack Power Filter.• Verify that you are using a Web browser supported for the Rack Power Filter. See "Supported Web Browsers" on page 37.• If the Rack Power Filter has just restarted and SSL security is being set up, the Rack Power Filter may be generating a server certificate. The Rack Power Filter can take up to one minute to create this certificate, and the SSL server is not available during that time.

The unit will not turn on

There is no input power, or insufficient input power from the wall outlet.	Use a voltmeter to check the output of the wall outlet. Use a device that is known to work properly to check the outlet. Note: The unit will not turn on if the input utility power is out of the acceptable range.
A circuit breaker has been tripped.	<ul style="list-style-type: none"> • Check the building circuit breakers and the unit's circuit breaker. If the circuit breaker on the unit has been tripped, the center post will protrude from the unit. To reset the breaker, push the center post into the unit. If it trips again, unplug one of the components plugged into the unit and reset the breaker. • The unit is rated for 15 Amps, however, the National Electric Code (NEC) dictates that any home circuit should not be loaded to more than 80% of its rating. Note: If the breaker is tripped again after trying this solution, contact APC Technical Support.
Power is not supplied to some outlets.	Power to the CONTROLLED outlets has intentionally been turned off.
The CONTROLLED outlets are not supplying power, even though the master device is not in sleep mode.	The MASTER Outlet threshold may be incorrectly set.

The Overload indicator is illuminated

The unit is overloaded. The overload LED is flashing.	The Overload LED on the front of the unit will illuminate red if the unit is overloaded. Reduce the load by disconnecting one or more components from the back of the unit. When the load is below 95%, the LED will stop flashing.
---	---

The Wiring OK indicator is not illuminated

<ul style="list-style-type: none"> • The wall outlet polarity is reversed. • The neutral wire is overloaded. • The earth ground is not connected at the wall outlet. 	Contact an electrician to inspect the building wiring. WARNING: Do not operate the unit if any of these conditions exist. The unit may not be providing surge protection.
The unit is on, but none of the LEDs are illuminated.	Push UP or DOWN several times. The LEDs should illuminate. If they do not illuminate, contact APC Technical Support.

Appendix A: List of Supported Commands

Network Management Card Command Descriptions

?

about

alarmcount

[-p [all | warning | critical]]

appcli

boot

[-b <dhcpBootp | dhcp | bootp | manual>]

[-c <dhcp cookie> [enable | disable]]

[-v <vendor class>]

[-i <client id>]

[-u <user class>]

cd

console

[-S <disable | telnet | ssh>]

[-pt <<telnet port n>]

[-ps <SSH port n>]

[-b <2400 | 9600 | 19200 | 38400>]

date

[-d <“datestring”>]

[-t <00:00:00>]

[-f <mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd>]

[-z <time zone offset>]

delete

dir

dns

[-OM [enable | disable]]

[-p <primary DNS server>]

[-s <secondary DNS server>]

[-d <domain name>]

[-n <domain name IPv6>]

[-h <host name>]

eventlog

exit

format

ftp

[-p <port number>]

[-S <enable | disable>]

help

netstat

ntp
 [-OM [enable | disable]]
 [-p <primary NTP server>]
 [-s <secondary NTP server>]

ping
 [<IP address or DNS name>]

portspeed
 [-s [auto | 10H | 10F | 100H | 100F]]

prompt
 [-s [long | short]]

quit

radius
 [-a <access> [local | radiusLocal | radius]]
 [-p# <server IP>]
 [-s# <server secret>]
 [-t# <server timeout>]

reboot

resetToDef
 [-p [all | keepip]]

snmp, snmp3
 [-S [enable | disable]]

system
 [-n <system name>]
 [-c <system contact>]
 [-l <system location>]

tcpip
 [-i <IP address>]
 [-s <subnet mask>]
 [-g <gateway>]
 [-d <domain name>]
 [-h <host name>]

tcpip6
 [-S [enable | disable]]
 [-man [enable | disable]]
 [-auto [enable | disable]]
 [-i <IPv6 address>]
 [-g <IPv6 gateway>]
 [-d6 [router | stateful | stateless | never]]

user
 [-an <Administrator name>]
 [-dn <Device User name>]
 [-rn <Read-Only User name>]
 [-ap <Administrator password>]
 [-dp <Device User password>]
 [-rp <Read-Only User password>]
 [-t <inactivity timeout in minutes>]

web
[-S <disable | http | https>]
[-ph <http port #>]
[-ps <https port #>]
xferINI
xferStatus

Device Command Descriptions

devEnergySvd
devLowVolt
devOverVolt
devReading
devStatus
olAutoRbt
[-s <<successful ping period>]
[-u <unsuccessful ping period>]
[-d <delay before first pint after reboot>]
[-r <reboot pulse time>]
[-f <failed pings before reboot>]
[-m <max reboot attempts>]
[-t <host name or ip>]
olCancelCmd
olCtrlType
olDlyOff
olDlyOn
olName
olOff
olOn
olRbootTime
olReading
olReboot
olStatus
prodInfo
vendInfo

APC Worldwide Customer Support

Customer support for this or any other APC product is available at no charge in any of the following ways:

- Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
 - **www.apc.com** (Corporate Headquarters)
Connect to localized APC Web sites for specific countries, each of which provides customer support information.
 - **www.apc.com/support/**
Global support searching APC Knowledge Base and using e-support.
- Contact the APC Customer Support Center by telephone or e-mail.
 - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

For information on how to obtain local customer support, contact the APC representative or other distributors from whom you purchased your APC product.

© 2011 APC by Schneider Electric. APC and the APC logo are owned by Schneider Electric Industries S.A.S., American Power Conversion Corporation, or their affiliated companies. All other trademarks are property of their respective owners.