USER'S GUIDE

Switched Rack PDU

Contents

Introduction

Product Description

Features of the Switched Rack PDU

The American Power Conversion (APC®) Switched Rack Power Distribution Unit (PDU) is a stand-alone, network-manageable device that monitors current and allows programmable control of eight, sixteen, or twenty-four power outlets (depending on the model).

You can manage a Switched Rack PDU through its Web interface, its control console, the InfraStruXure® Manager, or SNMP:

- Access the Web interface using HyperText Transfer Protocol (HTTP), or using HTTPS with Secure Sockets Layer (SSL).
- Access the control console through a serial connection, Telnet, or Secure SHell (SSH).
- Use InfraStruXure Manager to monitor and manage your Rack PDU.
- Use an SNMP browser and the APC PowerNet® Management Information Base (MIB) to manage your Rack PDU.

Switched Rack PDUs have these features:

- Monitors current per phase or bank
- Configurable alarm thresholds that provide network and visual alarms to help you prevent overloaded circuits
- Independent outlet control
- Configurable power delays
- 24 independent outlet user accounts

- Four levels of user access accounts—Administrator, Device User, Read-Only User, and Outlet User.
- 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, and FTP
- E-mail notifications for Rack PDU and system events
- SNMP traps, Syslog messages, and e-mail notifications based on the severity level or category of Rack PDU and system events
- A selection of security protocols for authentication and encryption

The Rack PDU does not provide power protection. Therefore, APC does not recommend plugging a unit directly into any unprotected power source, such as a wall outlet.

Initial setup

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

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

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

To configure the TCP/IP settings, see the *Installation and Quick Start* manual provided as a PDF file on the Switched Rack PDU *Utility* CD, and as a printed manual.

To use a DHCP server to configure the TCP/IP settings at a Rack PDU, see TCP/IP and Communication Settings.

Access Procedures

Overview

The Switched Rack PDU has two internal interfaces (control console and Web interface) that allow you to manage the Rack PDU.

For more information about the internal user interfaces, see Control Console and Web Interface.

The SNMP interface also allows you to use a SNMP browser with the PowerNet Management Information Base (MIB) to manage the Rack PDU.

To use the PowerNet MIB with a SNMP browser, see the *PowerNet SNMP Management Information Base (MIB) Reference Guide*, which is provided on the Switched Rack PDU *Utility* CD.

Access priority for logging on

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

- Local access to the control console from a computer with a direct serial connection to the Rack PDU.
- Telnet or Secure SHell (SSH) access to the control console from a remote computer.
- Web access, either directly or through the InfraStruXure Manager.

See SNMP for information about how SNMP access to the Switched Rack PDU is controlled.

Types of user accounts

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

- An Administrator can use all of the menus in the Web interface and control console. 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 and the event and data logs, accessible under the **Events** and **Data** headings on the left navigation menu of the **Logs** tab.
  - In the control console, the equivalent features and options. A Device User can also access the event log in the control console by pressing CTRL+L.

  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 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 are disabled, and the event and data logs display no button to clear the log.

  The default user name is **readonly**, and the default password is **apc**.
- An Outlet User has the following restricted access:
  - Access through the Web interface and control console.
  - Access to the same menus as a Device User, but with limited capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but are disabled except for the **Outlet Control** menu option that allows the user to access the assigned outlets as defined by the Administrator, and the event and data logs display no button to clear the log.

The user name and password are defined by the Administrator during the process of adding a new Outlet user.

To set **User Name** and **Password** values for Administrator, Device User, and Read-Only Users accounts, see Setting user access (Administration>Security>Local Users>options).

You must use the Web interface to configure values for the Read-Only User and Outlet User.

Recover From a Lost Password

You can use a local computer, a computer that connects to the Rack PDU or other device through the serial port, to access the control console.

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the serial cable (APC part number 940-0144A) to the selected port on the computer and to the configuration port at the Rack PDU.
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 as many times as necessary to redisplay the **User Name** prompt, then use the default, **apc,** for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must repeat step 5 and log on again.)

7. From the **Control Console** menu, select **System**, then **User Manager**.
8. Select **Administrator**, and change the **User Name** and **Password** settings, both of which are now defined as **apc**.
9. Press CTRL+C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Upgrading Firmware through a Serial Connection

For a complete description of how to download a firmware upgrade for your Rack PDU, see Upgrading Firmware: Methods and Tools. That section also explains how to use network-based file transfer tools, which complete a firmware upgrade more quickly than the XMODEM protocol described here, which uses a serial connection.

An administrator can use a local computer that connects to the Rack PDU through the serial port, on the front panel of the unit, to upgrade the firmware for the Rack PDU.

1. Select a serial port at the local computer, and disable any service which uses that port.
2. Use the supplied serial cable (APC part number 940-0144A) to connect the selected port to the serial port on the front panel of the Rack PDU.
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. Save the changes.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.
5. Enter your user name and password (both **apc**, by default) and press the ENTER key.
6. From the **Control Console** menu, select, in order, **System**, **Tools**, **File Transfer**, and **XMODEM**.
7. At the prompt **`Perform transfer with XMODEM-CRC?`** type **`YES`**, and press ENTER.

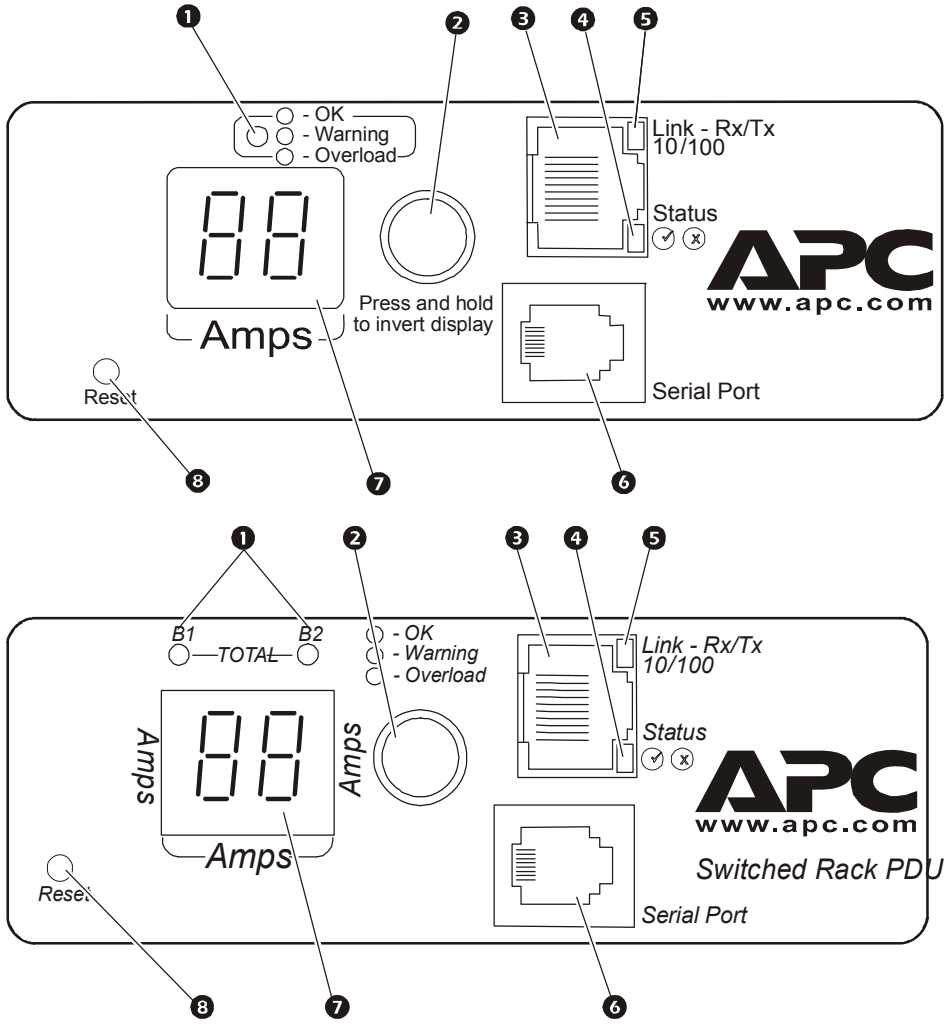
8. The system will then prompt you to choose a transfer rate and to change your terminal settings to match the transfer rate. Press ENTER to set the Switched Rack PDU to accept the download.
9. In the terminal program, send the file using the XMODEM protocol. When the transfer finishes, the console will prompt you to restore the baud rate to normal.

Do not interrupt the download.

Upgrading the firmware will not interfere with the operation of the outlets. The Rack PDU will restart when the download is complete.

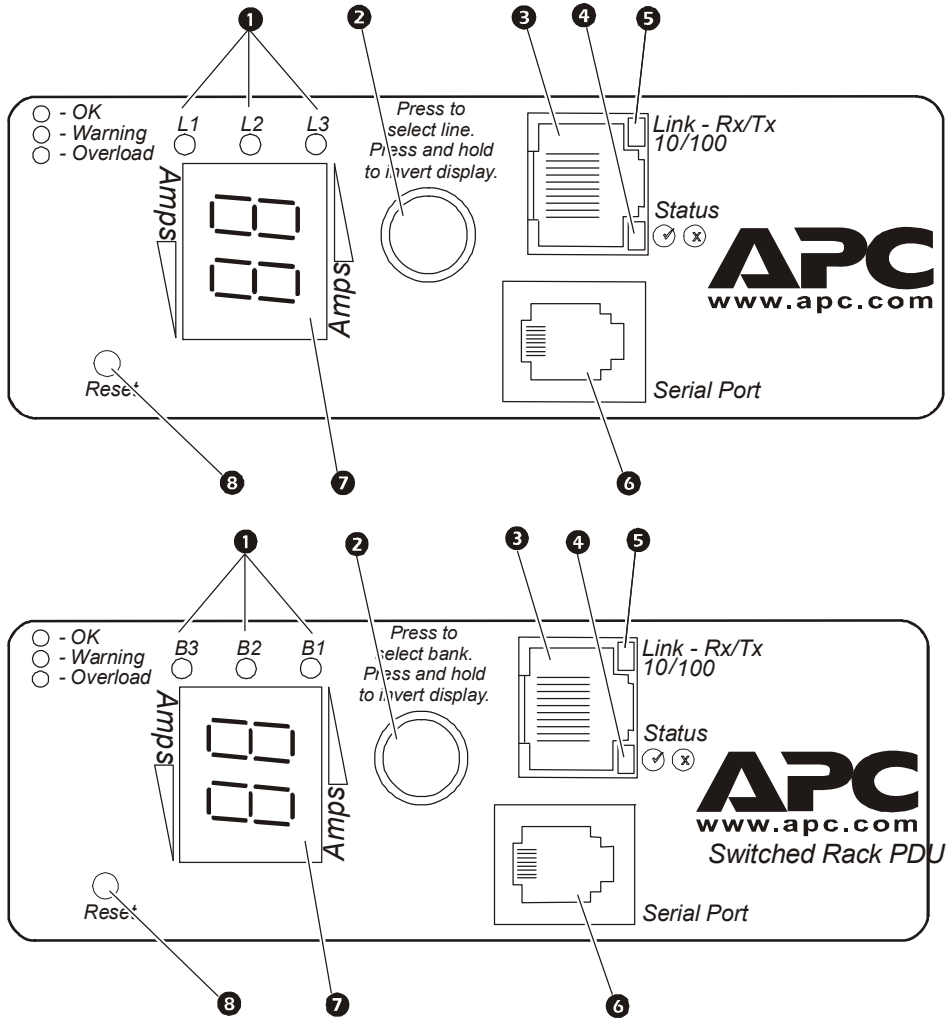
Front Panel

Single-phase



Three-phase

Three-phase Switched Rack PDUs have one of the following front panels:



Item	Function
❶ Load Indicator LED	Identifies overload and warning conditions for the displayed phase, bank, or outlet. See Load indicator LED.
❷ Input Selector	On 3-phase models, press the input selector to monitor the current of the next phase or bank. For either 1- or 3-phase units, press and hold the input selector to display the IP address of the Rack PDU or to invert the display. At five seconds, the IP address is displayed; at ten seconds, the displayed numbers invert.
❸ 10/100 Base-T Connector	Connects the Rack PDU to the network.
❹ Status LED	See Status LED.
❺ Link-RX/TX LED	See Link-RX/TX (10/100) LED.
❻ RJ-12 Serial Port	Connects the Rack PDU to a terminal emulator program for local access to the control console. Use the supplied serial cable (APC part number 940-0144A).
❼ Digital Display	Displays the current (amps) for the phase or bank indicated by the illuminated Load Indicator LED. On 3-phase models, the Digital Display will cycle through the phases, banks, or outlets, displaying the current for each for 3 seconds. If an internal communication or power supply failure occurs (for either a 1- or 3-phase model), the Digital Display displays **Er**, which you can clear by pressing the input selector.
❽ Reset Button	Resets the Rack PDU without effecting the outlet status. **Warning:** Do not press the Input Selector button at any time while the unit is rebooting, this will effect the status of the outlets.

Link-RX/TX (10/100) LED

This LED indicates the network status.

Condition	Description
Off	The device that connects the Rack PDU to the network is off or not operating correctly.
Flashing Green	The Rack PDU is receiving data packets from the network at 10 Megabits per second (Mbps).
Flashing Orange	The Rack PDU is receiving data packets from the network at 100 Megabits per second (Mbps).
Solid Green or Orange	The Rack PDU is not receiving any network traffic.

Status LED

This LED indicates the network status of the Rack PDU.

Condition	Description
Off	The Rack PDU has no power.
Solid Green	The Rack PDU has valid TCP/IP settings.
Flashing Green	The Rack PDU does not have valid TCP/IP settings.†
Solid Orange	A hardware failure has been detected in the Rack PDU. Contact APC Worldwide Customer Support.
Flashing Orange	The Rack PDU is making BOOTP requests.
Flashing Orange and Green (alternating)	The Rack PDU is making DHCP requests.

† If you do not use a BOOTP or DHCP server, see the *Installation and Quick Start* manual, provided as a PDF on the Switched Rack PDU *Utility* CD, to configure the TCP/IP settings.

Load indicator LED

The load indicator LED identifies overload and warning conditions for the displayed phase or bank.

Condition	Description
Solid Green	The current of the displayed phase or bank is under normal conditions and is between **Near Lowload** and **Near Overload** thresholds.
Yellow	The displayed phase or bank is in a **Near Overload Warning** condition. The current is above the **Near Overload Warning** threshold.
Red	The displayed phase or bank is in an Overload condition. The current is above the **Overload Alarm** threshold.

Watchdog Features

Overview

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

Network interface watchdog mechanism

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

Resetting the network timer

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

Control Console

Log On

Overview

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection to access the control console.

Use case-sensitive **User Name** and **Password** entries to log on (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device User). A Read-Only User has no access to the control console.

If you cannot remember your user name or password, see Recover From a Lost Password.

Remote access to the control console

You can access the control console through Telnet or Secure SHell (SSH). Telnet is enabled by default. Enabling SSH disables Telnet.

To enable or disable these access methods:

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

Telnet for basic access. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption. To use Telnet to access the control console:

1. From a computer on the same network as the Rack PDU, at a command prompt, type **`telnet`** and the System IP address for the Rack PDU (for example `telnet 139.225.6.133`, when the Rack PDU uses the default Telnet port of 23), and press ENTER.

If the PDU uses a non-default port number (from 5000 to 32768), you must include a colon or a space, depending on your Telnet client, between the IP address (or DNS name) and the port number.

2. Enter the user name and password (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device User).

SSH for high-security access. If you use the high security of SSL for the Web interface, use Secure SHell (SSH) for access to the control console. SSH encrypts user names, passwords and transmitted data. The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet, but to use SSH, you must first configure SSH and have a SSH client program installed on your computer.

Local access to the control console

For local access, use a computer connected by serial cable to the Rack PDU through the serial port on the front panel of the unit:

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Use the supplied serial cable (APC part number 940-0144A) to connect the selected port to the serial port on the front panel of the Rack PDU.
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. Save the changes.
4. Press ENTER, and at the prompts, enter your user name and password.

Main Screen

Example main screen

The main screen that is displayed when you log on to the control console of a Rack PDU:

```
User Name : apc
Password  : ***


American Power Conversion               Network Management Card AOS    vx.x.x
(c) Copyright 2006 All Rights Reserved  Rack PDU APP                   vx.x.x
-------------------------------------------------------------------------------
Name      : MS3 Test Unit                                Date : 12/11/2006
Contact   : Bill Cooper                                  Time : 10:16:58
Location  : Testing Lab                                   User : Administrator
Up Time   : 0 Days 0 Hours 43 Minutes                    Stat : P+ N+ A+

Switched Rack PDU: Communication Established

------- Control Console -----------------------------------------------------

     1- Device Manager
     2- Network
     3- System
     4- Logout

<ESC>- Main Menu, <ENTER>- Refresh, <CTRL-L>- Event Log
```

Information and status fields

Main screen information fields.

- 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 preceding example, the application firmware for the Rack PDU is displayed.

```
Network Management Card AOS      vx.x.x
Rack PDU APP                     vx.x.x
```

- Three fields identify the system name, contact person, and location of the Rack PDU. (In the control console, use the **System** menu to set these values.)

```
Name         : MS3 Test Unit
Contact      : Bill Cooper
Location     : Testing Lab
```

- An **Up Time** field reports how long the Rack PDU has been running since it was last reset or since power was applied.

```
Up Time      : 0 Days 0 Hours 43 Minutes
```

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

```
Date : 12/11/2006
Time : 10:16:58
```

- A **User** field identifies whether you logged in through the **Administrator** or **Device User** account. (The **Read-Only User** account cannot access the control console.)

```
User : Administrator
```

Main screen status fields.

- A **Stat** field reports the Rack PDU status.

```
Stat : P+ N+ A+
```

P+	The APC operating system (AOS) is functioning properly.
N+	The network is functioning properly.
N?	A BOOTP request cycle is in progress.
N–	The Rack PDU failed to connect to the network.
N!	Another device is using the IP address of the Rack PDU.
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. See APC Worldwide Customer Support.

- A Rack PDU model and name field reports the operating status of the Rack PDU.

```
Switched Rack PDU: Communication Established
```

Control Console Menus

How to use control console menus

The menus in the control console list options by number and name. To use an option, type the option's number, press ENTER, and follow any on-screen instructions. If you use an option that changes a setting or value, select **Accept Changes** to save your change before you exit the menu.

While in a menu, you can also do the following:

- Type ? and press ENTER to access brief menu option descriptions (if the menu has help available).
- Press ENTER to refresh the menu.
- Press ESC to go back to the menu from which you accessed the current menu.
- Press CTRL+C to return to the main (**Control Console**) menu.
- Press CTRL+L to access the event log (**Administrator** and **Device Manager** only).

For information about the event log, see Indirect Notification Through Logs or Queries.

Main Menu

Use the main **Control Console** menu to access the control console's management features:

```
1- Device Manager
2- Network
3- System
4- Logout
```

When you log on as Device Manager or Outlet User, (equivalent to Device User in the Web interface), you can access only the **Device Manager** menus and the **Logout** menu.

Device Manager option

Select the **Device Manager** menu then select the components to manage from this menu. To perform any of the following tasks, see Device and Outlet Management Menus:

- Configure the load thresholds for each phase or bank.
- Configure and control the outlets.
- View the status of the power supply.

Network option

To perform any of the following tasks, see Administration: Network Features:

- Configure the TCP/IP settings for the Rack PDU or, when the Rack PDU will obtain its TCP/IP settings from a server, configure the settings for the type of server (DHCP or BOOTP) to be used.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet, Web interface and SSL, SNMP, e-mail, DNS, and Syslog features of the Switched Rack PDU.
- Enable or disable the ISX Protocol.

System option

To perform any of the following tasks, see Administration: General Options:

- Control **Administrator** and **Device Manager** access. (You can control **Read-Only User** access by using the Web interface only.)
- Define the **Name**, **Contact**, and **Location** values for the system.
- Set the date and time used by the Rack PDU.
- Through the **Tools** option:
  - Restart the Rack PDU.
  - Reset parameters to their default values.
  - Delete SSH host keys and SSL certificates.

  - Upload an initialization file (.ini file) that has been downloaded from another Rack PDU. The current Rack PDU then uses the values in that .ini file to configure its own settings.
- Access and configure RADIUS information.
- Access system information about the Rack PDU.

Web Interface

Introduction

Supported Web browsers

You can use Microsoft® Internet Explorer (IE) 5.5 and higher (on Windows® operating systems only), Firefox, version 1.x, by Mozilla Corporation (on all operating systems), or Netscape® 7.x and higher (on all operating systems) to access the Rack PDU through its Web interface. Other commonly available browsers also may work but have not been fully tested by APC.

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

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

Log On

Overview

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

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

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

There is no default password for Outlet User accounts. (An Administrator must define the password and other account characteristics for an Outlet User.)

If you are using HTTPS 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 Rack PDU. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

See Web (Administration>Network>Web>options) to select, enable, and disable the protocols that control access to the Web interface and to define the Web-server ports for the protocols.

For information about the Web page that appears when you log on to the Web interface, see Home Page.

URL address formats

Type the Rack PDU DNS name or IP address 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 login.

Error Message	Cause of the Error	Browser
"You are not authorized to view this page" or "Someone is currently logged in..."	Someone else is logged on	Internet Explorer, Netscape, Firefox

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

URL format examples.

- For a DNS name of Web1, the entry would be one of the following:
  - **`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, when the Rack PDU uses the default port (80) at the Web server, the entry would be one of the following:
  - **`http://139.225.6.133`** if HTTP is your access mode
  - **`https//139.225.6.133`** if HTTPS is your access mode
- For a System IP address of 139.225.6.133, when the Rack PDU uses a non-default port (5000, in this example) at the Web server, the entry would be one of the following:
  - **`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

Tabs, Menus, and Links

Tabs

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

- **Device Manager**: Display Rack PDU status, issue Rack PDU control commands, configure Rack PDU parameters, run diagnostic tests, configure and schedule shutdowns, control and configure outlets, assign external device Web links to outlets, modify outlet group configurations, configure outlet schedules and actions, and create and maintain Outlet Users.
- **Logs**: View and configure event and data logs.
- **Administration**: Configure security, network connection, notification, and general settings.

Menus

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

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

Top menu bar. The **Home** and **Administration** tabs have a selection of menu options on the top menu bar. The **Security** option is selected by default when you click the **Administration** tab and the **Overview** option is selected when you click the **Home** tab.

Clicking an option on the top menu bar displays the left navigation menu for that option, with the first menu item selected by default.

Quick Links

See Configure Links (Administration>General>Quick Links) to access the menu to three configurable links that are shown at the lower left on each page of the Web interface.

Home Page

Overview

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

Quick status icons

At the upper right corner of every page, one or more icons and accompanying text indicate the current operating status of the Rack PDU:

	**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 Rack PDU is operating normally.

The Web interface displays the same icons currently displayed on the **Home** page to report Rack PDU 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 **Home** page to view its summary of Rack PDU status, including the active alarms, click a quick status icon on any page of the interface.

Active Alarms

The **Active Alarms** section displays any alarms present. If no alarms are present, "No Device-Level Alarms Present" will be displayed. If an alarm is present, the alarm and its description will be displayed. Click the displayed alarm to view the **Device Alarm Status** page, which includes a description and severity level for each alarm present. The **Device Alarm Status** page can also be accessed through the **Home** page top menu bar.

Load Status

On the **Home** page, **Load Status** displays a graph depicting the current load status of the Rack PDU. The colors green, yellow, and red signify the **Load Thresholds** set by the user. The graphic is accompanied by the measurement of the load in Amps, and a link to **Load Management** in the **Device Manager** tab.

Outlet Status

The **Outlet Status** section shows the outlet's number, phase or bank (for 3-phase models), state (on or off), and name of the outlet.

Switched Rack PDU Parameters

The **Switched Rack PDU Parameters** section displays the name, contact information, location of the PDU, its current rating, the type of user account accessing the Rack PDU, and the amount of time the Rack PDU has been operating.

Recent Device Events

On the **Home** page, **Recent Device Events** displays, in reverse chronological order, the events that occurred most recently and the dates and times they occurred. Click **More Events** to view the entire event log.

Additional information on Home page

The IP address displays in the upper left corner.

A context-sensitive **Help** link and **Log off** link are displayed in the upper right corner of every page.

Selecting a menu to perform a task

- To do the following, see Configure Load Thresholds:
  - Configure the overload thresholds for each phase or bank.
  - Set the **Name**, **Location**, and **Coldstart Delay** for the Rack PDU.
  - Set the names and associated Web links for the outlets.
- To do the following, see Configure and Control Outlet Groups
  - Apply power to and remove power from the outlets.
  - Set **Power On Delay**, **Power Off Delay**, and **Reboot Duration** for the outlets.
  - Set the names and associated links for the outlets.
  - Create, enable, and use synchronized outlet groups.
- To do the following, see Configuring event actions:
  - Access the event log.
  - Configure the actions to be taken based on the severity level of an event.
  - Configure **SNMP Trap Receiver** settings for sending event-based traps.
  - Define who receives e-mail notification and Syslog messages for events.
  - Test e-mail settings.
- To do the following, see Data log (Logs>Data>options):
  - Access the data log.
  - Define the log interval (how often data will be sampled and recorded) for the data log.
- To do the following, see Administration: Network Features:
  - Configure new TCP/IP settings for the Rack PDU.

  - Identify the Domain Name System (DNS) Server, test its network connection, and enable or disable DNS Reverse Lookup Event Logging (which logs the domain name of the device associated with each event).
  - Define settings for FTP, Telnet, SSH, HTTP and HTTPS, SNMP, and e-mail.
  - Configure the Rack PDU's Syslog message feature.
- To do the following, see Administration: General Options:
  - Control **Administrator**, **Device User**, **Outlet User**, and **Read-Only User** access.
  - Define the system **Name**, **Contact**, and **Location** values.
  - Set the date and time used by the Rack PDU.
  - Restart the Rack PDU.
  - Reset network settings to default settings.
  - Define the URL addresses of the user links and APC logo links in the Web interface, as described in Configure Links (Administration>General>Quick Links).

Help menu

Click **Help** from any Web interface page to view help text for that page.

Switched Rack PDU Settings

Configure Load Thresholds

Web interface.

1. Select the **Device Manager** tab and then the **Load Management** left navigation menu.
2. Set **Overload Alarm Threshold**, **Near Overload Warning Threshold**, **Low Load Warning Threshold**, and **Overload Outlet Restrictions** for each phase or bank.
3. Click **Apply** in that section to set the selected values.

Control console.

1. Select **Phase Management** from the **Device Manager** menu.
2. Select **Overload Alarm Threshold (amps)**, **Near Overload Warning Threshold (amps)**, or **Low Load Warning Threshold (amps)**.
3. Select **Accept Changes**.

To set the overload outlet restriction, select **Outlet Restriction Configuration** on the **Device Manager** menu. For 3-phase units, select a phase or bank to display and change the **Outlet Phase/Bank Restriction**.

Setting	Description
Overload Alarm Threshold	Set the number of amps that will cause an overload of this phase or bank.
Near Overload Warning Threshold	Set the number of amps at which to generate a warning that the Rack PDU is nearing overload of a phase or bank.
Low Load Warning Threshold	Set the low threshold, in amps, for the current drawn from this phase or bank during normal operation. A load below this level generates a warning, if the load is equal to this threshold, a warning alarm is not generated.
Overload Outlet Restriction	Prevent users from applying power to outlets during an overload condition. You can set the following restrictions for each outlet: • **None**: You can apply power to outlets regardless of an Overload Alarm or Near Overload Warning. • **On Warning**: You cannot apply power to an outlet on the selected phase or bank if the current for that phase or bank has exceeded the Near Overload Warning threshold. • **On Overload**: You cannot apply power to an outlet on the selected phase or bank if the current for that phase or bank has exceeded the Overload Alarm threshold.
Coldstart Delay	The time that the Switched Rack PDU delays applying power to the outlets after AC power has been applied to the Rack PDU.

Configure Device Settings

Web interface. Select the **Administration** tab and select **General** from the top menu bar. Select **Identification** from the left navigation menu to configure the **Device Name, Device Contact,** and **Device Location** fields for the Rack PDU (which are equivalent to the **Name** and **Location** fields in the control console).

Control console.

To change the **Contact** field (the name of the person to contact about the Rack PDU) in addition to the **Name** and **Location** fields in the control console, see Administration: General Options.

Setting	Description
Name	Set the name of the Rack PDU.
Location	Set the location of the Rack PDU.
Contact	Set the name of the person to contact about the Rack PDU.

View Power Supply Status (control console only)

Select **Power Supply Status** from the **Device Manager** menu to display the status of the power supply for the Switched Rack PDU.

Device and Outlet Management Menus

Device Manager Tab

The **Device Manager** tab contains load and outlet configurations and settings for your Rack PDU. The **Load Management** option is selected by default.

Load management

The top menu bar option **Load Management** displays the current load status and configurable fields to set the **Load Thresholds** for the banks or phases of the Rack PDU.

The current load of the Rack PDU is displayed as a graph. The graph is accompanied by the measurement of the load in Amps. Alarms associated with the current load are displayed next to the graph.

The following alarms can be set through the **Load Management** menu: **Overload Alarm**, **Near Overload Warning**, **Low Load Warning**, **Overload Outlet Restriction**, and **Cold Start Delay**.

Configure and Control Outlet Groups

Outlet group terminology

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

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

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

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

Purpose and benefits of outlet groups

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

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

System requirements for outlet groups

To set up and use synchronized outlet control groups:

- You need a 10/100Base-T TCP/IP network, with an Ethernet hub or switch that has a power source not shared by the computers or other devices being synchronized.
- If outlet groups are to be synchronized across multiple Switched Rack PDUs, those Switched Rack PDUs must meet the following requirements:
  - They must be on the same subnet.
  - They must use firmware that has the same version number, which must be 3.3.1 or higher for both the APC Operating System (AOS) module and the application module.
- You need a computer that can initiate synchronized control operations through the Web interface or control console of the Switched Rack PDUs or through SNMP.
- Outlet groups you synchronize must have the same Multicast IP address. Make sure each Ethernet switch that connects Switched Rack PDUs allows Multicast network traffic for that Multicast IP address.

Rules for configuring outlet groups

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

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

Enable outlet groups

Click the **Device Manager** tab and select **Group Configuration** from the **Outlet Groups** left navigation menu. Configure the following parameters, and click **Apply**.

Enable creation of outlet groups.

Parameter	Description
Device Level Outlet Group	To create an outlet group, you must enable this parameter. It is disabled by default.

Enable support for global outlet groups (linked groups).

Parameter	Description
Multicast Name	To link outlet groups on multiple Switched Rack PDUs, you must define the same Multicast name and Multicast IP address on each of those Rack PDUs. **NOTE:** A maximum of four devices can be configured with the same Multicast name and Multicast IP address.
Multicast IP	

Enabling encryption and authentication of outlet groups.

Parameter	Description
Authentication Phrase	A phrase of 15 to 32 ASCII characters that verifies that the device is communicating with other devices, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time.
Encryption Phrase	A phrase of 15 to 32 ASCII characters that ensures the privacy of the data (by means of encryption).

Setting outlet group port.

Parameter	Description
Outlet Group Port	The port number on which the device will communicate with other devices.

Devices wishing to synchronize with Outlet Groups on other devices must all have the same Authentication Phrase, Encryption Phrase, and Group Port number. The values are hidden to the user.

Create a local outlet group (Web interface)

1. From the **Device Manager** tab, select **Information** from the **Outlet Groups** left navigation menu.
2. Make sure outlet groups are enabled.

See Enable outlet groups.

3. Click **Create Local Outlet Group**.
4. Under **Configure Local Outlet Group**, select each outlet that will be in the group and assign the group a name in the **Outlet Group Name** field. You must select at least two outlets.

Create multiple global outlet groups (Web interface)

To set up multiple global outlet groups that link to outlet groups on other Switched Rack PDUs:

1. From the **Device Manager** tab, select **Information** from the **Outlet Groups** left navigation menu.
2. Make sure outlet groups are enabled and that the Multicast parameters (name

and IP address) are the same for all Rack PDUs to be linked.

See Enable outlet groups.

3. Click **Create Global Outlet Groups**.
4. For each global outlet group you create, select an outlet by clicking on its checkbox. Then click **Apply**. For example, select five outlets to create five outlet groups, each consisting of one global outlet.
5. To add outlets to any of the global outlet groups you created, see Edit or delete an outlet group.

Edit or delete an outlet group

1. From the **Device Manager** tab, select **Information** from the **Outlet Groups** left navigation menu.
2. Under **Configured Outlet Groups**, click on the number or name of the outlet group to edit or delete.
3. When editing an outlet group you can do any of the following:

–Rename the outlet group.

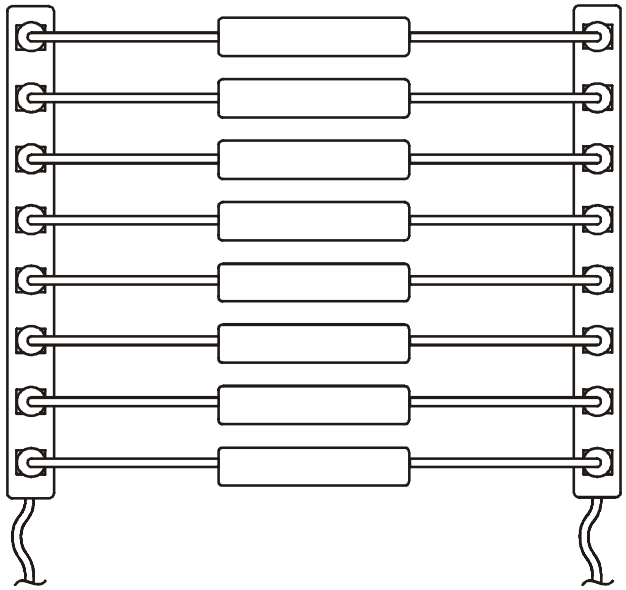
–Add or remove outlets by clicking the checkboxes to mark or unmark them.

You cannot remove an outlet from an outlet group that contains only two outlets unless the remaining outlet is a global outlet.

4. To delete the outlet group, click **Delete Outlet Group**.

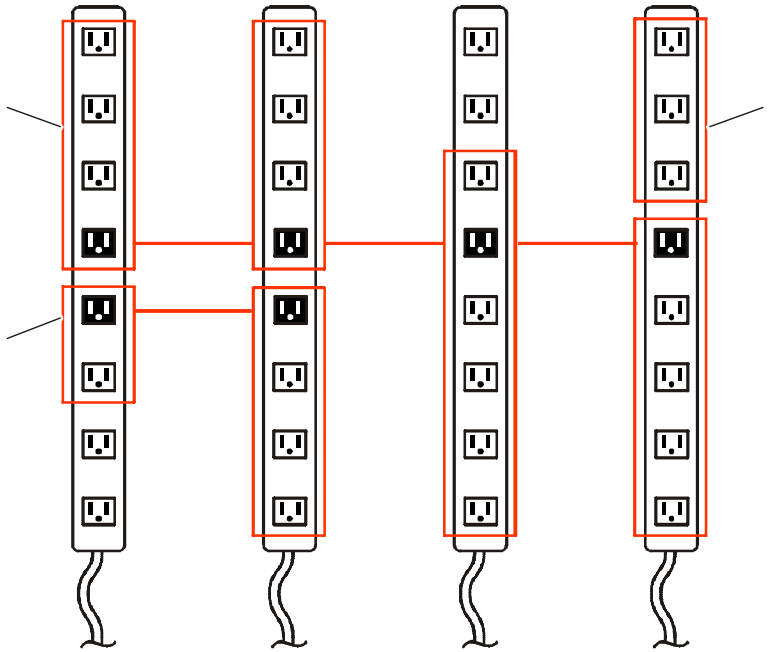
Typical outlet group configurations

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



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

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



Verify your setup and configuration for global outlet groups

To ensure that your setup meets all system requirements for outlet groups and that you have configured the outlet groups correctly, select **Information** from the **Outlet Groups** left navigation menu in the Web interface to view the groups and their connections:

- The **Configured Outlet Groups** section displays the following:
  - All configured outlet groups on the current Switched Rack PDU.
  - The outlets in each group by outlet number.
  - Any outlet groups on other Switched Rack PDUs with which a global outlet group is synchronized. Each Switched Rack PDU is identified by its IP address, and each global outlet is displayed in bold text.
- The **Global Outlet Overview** section displays the following:
  - The IP address of the current Switched Rack PDU.
  - The IP address of any Switched Rack PDUs that contain global outlets that are available to be synchronized with outlet groups on other Switched Rack PDUs.
  - All global outlets configured on the Switched Rack PDUs, regardless of whether they are synchronized with outlet groups on the current Switched Rack PDU.

Outlet Settings for Outlets and Outlet Groups

Initiate a control action

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

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

Web interface. To control the outlets on your Switched Rack PDU:

1. From the **Device Manager** tab, select **Control** from the left navigation menu.
2. Mark the checkboxes for each individual outlet or outlet group to control, or select the **All Outlets** checkbox.
3. Select a **Control Action** from the list, and click **Next >>**. On the confirmation page that explains the action, choose to apply or cancel it.

Control Console. Select **Outlet Control/Configuration** from the **Device Manager** menu to display a list of outlets. For each outlet, the list indicates whether it is a member of an outlet group.

1. Choose either of the following:
   - –To control one outlet and the outlet group, if any, to which it belongs, select the number of the outlet, and then select **Control Outlet**.
   - –To control all outlets, select **Master Control/Configuration**, and then **Control of ALL Outlets**.
2. Select a control action.
3. On the confirmation screen that describes the action to be executed, type `Yes` at the prompt to perform the action.

Control actions you can select.

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

† If a local outlet group is selected, only the configured delays and reboot duration of the lowest-numbered outlet of the group are used. If a global outlet group is selected, only the configured delays and reboot duration of the global outlet are used.

Configure outlet settings and the outlet name

Settings that you can configure. The following settings are available in both the Web interface and control console unless otherwise indicated:

Setting	Description
Name (Web interface) Outlet Name (control console)	Set the name for one or more outlets. The name is displayed next to the outlet number on status screens.
Link (Web interface)	Define an HTTP or HTTPS link to a Web site or IP address. • **http://www.apc.com** links the outlet to the home page of the APC Web site. • **http://*pdu_ip_address***, where ***pdu_ip_address*** is the IP address of the Switched Rack PDU and links the outlet to the Web interface of the Switched Rack PDU at the IP address, enabling authorized users to log on.
Power On Delay	Set the number of seconds that the Rack PDU waits after a command is issued before applying power to an outlet. **NOTE:** To configure an outlet to remain off at all times, check the **Never** checkbox next to **Power On Delay** in the Web interface, or configure a value of **–1** for **Power On Delay** in the control console.
Power Off Delay	Set the number of seconds that the Rack PDU waits after a command is issued before removing power from an outlet. **NOTE:** To configure an outlet to remain on at all times, check the **Never** check box next to **Power Off Delay** in the Web interface, or configure a value of **–1** for **Power Off Delay** in the control console.
Reboot Duration	Set the number of seconds an outlet remains off before restarting.

Web interface. To configure the outlet settings or outlet names, select the **Device Manager** tab and then **Configuration** from the left navigation menu. Click the **Configure Multiple Outlets** button in the **Outlet Configuration** section or click on the outlet name.

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

Control console. To configure the outlet settings and outlet name:

1. Select **Outlet Management** from the **Device Manager** menu.
2. Select **Outlet Control/Configuration** from the **Outlet Management** menu.
3. Choose the number of the outlet you want to control, and press ENTER.
4. Choose **Configure Outlet** to display and change the values for **Outlet Name**, **Power On Delay**, **Power Off Delay**, and **Reboot Duration**.

Scheduling Outlet Actions (Web Interface Only)

Actions you can schedule

To configure values for **Power On Delay**, **Power Off Delay**, and **Reboot Duration** for each outlet, see Configure outlet settings and the outlet name. Although you must use the Web interface to schedule outlet actions, you can set these values in either the Web or control console interfaces.

For an action to be applied to an outlet group, you must have outlet groups enabled at the beginning of the scheduled action. For example, if **Off Delayed** is scheduled for 4:00 p.m., the **Power Off Delay** begins at 4:00 p.m. Even if you then enable outlet groups during that **Power Off Delay** before any of the outlets are scheduled to turn off, the action will be applied only to the individual outlet and not the outlet group.

For any outlets you select, you can schedule any of the actions listed in the following table to occur daily; at intervals of one, two, four, or eight weeks; or only once.

Option	Description
No Action	Do nothing.
On Immediate	Apply power to the selected outlets.
On Delayed	Apply power to each selected outlet according to its value for **Power On Delay**.†
Off Immediate	Remove power from the selected outlets.
Off Delayed	Remove power from each selected outlet according to its value for **Power Off Delay**.†

† If an outlet group is selected, the configured delays and reboot duration of the lowest-numbered outlet (for a local outlet group) or of the global outlet (for a global outlet group that is initiating the action) are used.

Option	Description
Reboot PDU Immediate	Remove power from each selected outlet. Then apply power to each of these outlets according to its value for **Reboot Duration**.†
Reboot PDU Delayed	Remove power from each selected outlet according to its value for **Power Off Delay**. Wait until all outlets are off (the highest value for **Reboot Duration**), and then apply power to each outlet according to its value for **Power On Delay**.†

† If an outlet group is selected, the configured delays and reboot duration of the lowest-numbered outlet (for a local outlet group) or of the global outlet (for a global outlet group that is initiating the action) are used.

Schedule an outlet event

1. At the Web interface, select the **Device Manager** tab and then **Scheduling** from the left navigation menu.
2. On the **Outlet Scheduling** page, select how often the event will occur (**One-Time**, **Daily**, or **Weekly**), and click the **Next** button.

   If you select **Weekly**, you can choose to have the event occur once every week or once every two, four, or eight weeks.

3. On the **Schedule a Daily Action** page, in the **Name of event** text box, replace the default name, `Outlet Event`, with a name that will identify your new event.
4. Use the drop-down lists to select the type of event and when it will occur.

   The date format for one-time events is *mm*/*dd*, and the time format for all events is *hh*/*mm*, with the two-digit hour specified in 24-hour time.

   - An event that is scheduled daily or at one of the intervals available in the **Weekly** selection continues to occur at the scheduled interval until the event is deleted or disabled.
   - You can schedule a one-time event to occur only on a date within 12 months of the date on which you perform the scheduling. For example, on December 26, 2006, you could schedule a one-time event on any date from the current date until December 26, 2007.

5. Use the checkboxes to select which outlets will be affected by the action. You can select one or more individual outlets or **All Outlets**.
6. Click **Apply** to confirm the scheduling of the event, or **Cancel** to clear it.

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

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

1. At the Web interface, select the **Device Manager** tab and then **Scheduling** from the left navigation menu.
2. In the event list in the **Scheduled Outlet Action** section of the **Scheduling** page, click on the name of the event.
3. On the **Daily/Weekly scheduled action detail** page, you can do any of the following:

– Change details of the event, such as the name of the event, when it is scheduled to occur, and which outlets are affected.

– Under **Status of event** at the top of the page you can perform the following tasks:

- Disable the event, leaving all its details configured so that it can be re-enabled later. A disabled event will not occur. An event is enabled by default when you create it.
- Enable the event, if it was previously set to **Disable**.
- Delete the event, removing the event completely from the system. A deleted event cannot be retrieved.

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

Outlet Manager Menu

Create and configure outlet user accounts. Individual outlets can be assigned a user with an Outlet User account. An Outlet User account allows control only to the outlets assigned. The configuration of outlets is allowed to those with Administrator rights. The Device Manager has limited outlet configuration rights.

Configure outlet user

1. At the Web interface, select the **Device Manager** tab and then **Outlet Manager** from the left navigational menu.
2. Click the **Add New User** button.

3. Type in the information for the following options and click **Apply** to confirm the changes.

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

Administration: Security

Local Users

Setting user access (Administration>Security>Local Users>*options*)

You set the case-sensitive user name and password for each account type in the same manner. Maximum length of the username is 10 characters and the password is 32 characters.

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

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

Remote Users

Authentication (Administration>Security>Remote Users>Authentication Method)

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

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

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

- When a user accesses the Switched Rack PDU or another 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 Switched Rack PDU are limited to 32 characters.

Select one of the following:

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

If **RADIUS Only** is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, you must use a serial connection to the control console and change the **Access** setting to **Local Authentication Only** or **RADIUS, then Local Authentication** to regain access.

RADIUS (Administration>Security>Remote Users>RADIUS)

Use this option to do the following:

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

RADIUS Setting	Definition
RADIUS Server	The server name or IP address of the RADIUS server. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.
Secret	The shared secret between the RADIUS server and the Rack PDU.
Timeout	The time, in seconds, that the Rack PDU waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path.
Switch Server Priority	Change which RADIUS server will authenticate users if two configured servers are listed and **RADIUS, then Local Authentication** or **RADIUS Only** is the enabled authentication method.

Configuring the RADIUS Server

Summary of the configuration procedure

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

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

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

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

3. Vendor Specific Attributes (VSAs) can be used instead of the Service-Type attributes provided by the RADIUS server. VSAs 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 password against /etc/passwd. The following example is for users **`bconners`** and **`thawk`**:

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

Supported RADIUS servers

APC supports FreeRADIUS, Microsoft Windows 2000 Server®, and Microsoft Windows 2000 RADIUS Server. Other commonly available RADIUS applications may work but have not been fully tested by APC.

Inactivity Timeout (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.

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

Administration: Network Features

TCP/IP and Communication Settings

TCP/IP settings (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 IP address, subnet mask, default gateway, and MAC address of the Switched Rack PDU.

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

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

Setting	Description
Manual	The IP address, subnet mask, and default gateway must be configured manually. Click **Next>>**, and enter the new values.
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Rack PDU requests network assignment from any BOOTP server: • If it receives a valid response, it starts the network services. • If it finds a BOOTP server, but a request to that server fails or times out, the Rack PDU stops requesting network settings until it is restarted. • By default, if previously configured network settings exist, and it receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible. Click **Next>>** to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail [1]: • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. • **If retries fail**: Select **Use prior settings** (the default) or **Stop BOOTP request**.
DHCP	At 32-second intervals, the Rack PDU requests network assignment from any DHCP server. By default, the number of retries is unlimited. • If it receives a valid response, by default it requires the APC cookie from the DHCP server in order to accept the lease and start the network services. • If it finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted. To change these values, click **Next>>** for the **DHCP Configuration** page[1]: • **Require vendor specific cookie to accept DHCP Address**: Disable or enable the requirement that the DHCP server provide the APC cookie. • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.

1. The default values for these three settings on the configuration pages generally do not need to be changed:
   •**Vendor Class**: APC
   •**Client ID**: The MAC address of the Switched Rack PDU, which uniquely identifies it on the local area network (LAN)
   •**User Class**: The name of the application firmware module

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

1. The default values for these three settings on the configuration pages generally do not need to be changed:
   - **Vendor Class**: APC
   - **Client ID**: The MAC address of the Switched Rack PDU, which uniquely identifies it on the local area network (LAN)
   - **User Class**: The name of the application firmware module

DHCP response options

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

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

- **APC Cookie. Tag 1, Len 4, Data "1APC"**
  Option 43 communicates to the Rack PDU that a DHCP server is configured to service APC devices. By default, this DHCP response option must contain the APC cookie for the Rack PDU to accept the lease.

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

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

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

- **Boot Mode Transition. Tag 2, Len 1, Data 1/2**
  This option 43 setting enables or disables the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**, which, by default, is disabled.
  - A data value of 1 enables the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. Whenever the Rack PDU reboots, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.
  - A data value of 2 disables the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. The **TCP/IP Configuration** setting option switches to **DHCP** when the Rack PDU accepts the DHCP response. Whenever the Rack PDU reboots, it will request its network assignment from a DHCP server only.

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

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

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

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

- **Rebinding Time, T2** (option 59): The time that the Rack PDU must wait after an IP address lease is assigned before it can seek to rebind that lease.

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

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

Port Speed (Administration>Network>Port Speed)

It is necessary to be on the upstream network (server) before you power on the Rack PDU.

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 (the default mode is half-duplex).

- 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 (Administration>Network>DNS>*options*)

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

Servers. Select **servers** to specify the IP addresses of the primary and optional secondary DNS server. For the Rack PDU to send e-mail, at least the IP address of the primary DNS server must be defined.

- The Switched Rack PDU waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the Rack PDU does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the Rack PDU or on a nearby segment (but not across a wide-area network [WAN]).

To verify that DNS is working correctly after you define the IP addresses of the DNS servers, see Test.

Naming. Select **naming** to define the host name and domain name of the Rack PDU:

- **Host Name**: After you configure a host name here and a domain name in the **Domain Name** field, users can enter a host name in any field in the Rack PDU interface (except e-mail addresses) that accepts a domain name.
- **Domain Name**: You need to configure the domain name here only. In all other fields in the Switched Rack PDU interface (except e-mail addresses) that accept domain names, the Switched Rack PDU adds this domain name when only a host name is entered.
  - To override all instances of the expansion of a specified host name by the addition of the domain name, set the domain name field to its default, `somedomain.com`, or to `0.0.0.0`.

– To override the expansion of a specific host name entry (for example, when defining a trap receiver), include a trailing period. The Rack PDU recognizes a host name with a trailing period (such as *mySnmpServer.*) as if it were a fully qualified domain name and does not append the domain name.

Test. Select **test** to send a DNS query that tests the setup of your DNS servers:

- As **Query Type**, select the method to use for the DNS query:
  - **by Host**: the URL name of the server
  - **by FQDN**: the fully qualified domain name
  - **by IP**: the IP address of the server
  - **by MX**: the Mail Exchange used by the server
- As **Query Question**, identify the value to be used for the selected query type:

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

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

Web (Administration>Network>Web>*options*)

Option	Description

access	To activate changes to any of these selections, log off from the Rack PDU:
	• **Disable**: Disables access to the Web interface. (You must use the control console to re-enable access. Select **Network** and **Web/SSL/TLS**. Then for HTTP, select **Access** and **Enabled**. For HTTPS access, also select **Web/SSL** and **Enabled**.)
	• **Enable HTTP** (the default): Enables Hypertext Transfer Protocol (HTTP), which provides Web access by user name and password, but does not encrypt user names, passwords, and data during transmission.
	• **Enable HTTPS**: Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL). SSL encrypts user names, passwords, and data during transmission, and authenticates the Rack PDU by digital certificate. When HTTPS is enabled, your browser displays a small lock icon.
	See "Creating and Installing Digital Certificates" in the *Security Handbook* on the Switched Rack PDU *Utility* CD to choose among the several methods for using digital certificates.
	HTTP Port: The TCP/IP port (80 by default) used to communicate by HTTP with the Rack PDU.
	HTTPS Port: The TCP/IP port (443 by default) used to communicate by HTTPS with the Rack PDU.
	For either of these ports, you can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

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

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

Console (Administration>Network>Console>*options*)

Option	Description
access	Choose one of the following for access by Telnet or SSH: • **Disable**: Disables all access to the control console. • **Enable Telnet** (the default): Telnet transmits user names, passwords, and data without encryption. • **Enable SSH v1 and v2**: Do not enable both versions 1 and 2 of SSH unless you require both. They use extensive processing power. • **Enable SSH v1 only**: SSH version 1 encrypts user names, passwords, and data for transmission. There is little or no delay as you log on. • **Enable SSH v2 only**: SSH version 2 transmits user names, passwords, and data in encrypted form with more protection than version 1 from attempts to intercept, forge, or alter data during transmission. There is a noticeable delay as you log on. Configure the ports to be used by these protocols: • **Telnet Port**: The Telnet port used to communicate with the Rack PDU (23 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) or a space, as required by your Telnet client program, to specify the non-default port. For example, for port 5000 and an IP address of 152.214.12.114, your Telnet client requires one of the these commands: `telnet 152.214.12.114:5000` `telnet 152.214.12.114:5000` • **SSH Port**: The SSH port used to communicate with the Rack PDU (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port.
ssh encryption	Enable or disable encryption algorithms (block ciphers) compatible with SSH version 1 or version 2 clients: If your SSH v1 client cannot use **Blowfish**, you must also enable **DES**. Your SSH v2 client selects the enabled algorithm that provides the highest security. If the client cannot use the default algorithms (**3DES** or **Blowfish**), enable an AES algorithm that it can use (**AES 128** or **AES 256**).

Option	Description
ssh host key	**Status** indicates the status of the host key (private key): • **SSH Disabled: No host key in use:** When disabled, SSH cannot use a host key. • **Generating**: The Rack PDU is creating a host key because no valid host key was found. • **Loading**: A host key is being activated on the Rack PDU. • **Valid**: One of the following valid host keys is in the **/sec** directory (the required location on the Switched Rack PDU): •A 1024-bit host key created by the APC Security Wizard •A 768-bit RSA host key generated by the Switched Rack PDU **Add or Replace**: Browse to and upload a host key file created by the Security Wizard: If you use FTP or SCP instead to transfer the host key file, you must specify the **/sec** directory as the target location in the command. To use the APC Security Wizard, see the *Security Handbook* on the Switched Rack PDU *Utility* CD. **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 PDU takes up to 5 minutes to create a host key, and the SSH server is not accessible during that time.** **Remove**: Remove the current host key.

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

ISX Protocol (control console only)

Use this option to enable (the default) or disable the APC InfraStruXure (ISX) Protocol. The APC InfraStruXure (ISX) Protocol allows the Switched Rack PDU to communicate with other APC devices, including the InfraStruXure Manager, if your system includes one.

SNMP

SNMPv1 (Administration>Network>SNMPv1>*options*)

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

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

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

Option	Description
access	**Enable SNMPv1 Access:** Enables SNMP version 1 as a method of communication with this device.

Option	Description
access control	You can configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four available SNMPv1 communities, but you can edit these settings to apply more than one entry to any community to grant access by several specific IP addresses, host names, or IP address masks. To edit the access control settings for a community, click its community name. • If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network. • If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device. **Community Name:** The name that a Network Management System (NMS) must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are "public," "private," "public2," and "private2." **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows: • 149.225.12.255: Access only by a NMS on the 149.225.12 segment. • 149.225.255.255: Access only by a NMS on the 149.225 segment. • 149.255.255.255: Access only by a NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. **Access Type**: The actions a NMS can perform through the community. • **Read**: GETS only, at any time. • **Write**: GETS at any time, and SETS when no user is logged onto the Web interface or Control Console. • **Write+**: GETS and SETS at any time. • **Disabled**: No GETS or SETS at any time.

SNMPv3 (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.

To use SNMPv3, you must have a MIB program that supports SNMPv3.

The Switched Rack PDU supports only MD5 authentication and DES encryption.

Option	Description
access	**SNMPv3 Access:** Enables SNMPv3 as a method of communication with this device.
user profiles	By default, lists the settings of four user profiles, configured with the user names "apc snmp profile1" through "apc snmp profile 4," and no authentication and no privacy (no encryption of data). To edit the following settings for a user profile, click a user name in the list. **User Name:** The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters. **Authentication Passphrase:** A phrase of 15 to 32 ASCII characters that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time. **Privacy Passphrase:** A phrase of 15 to 32 ASCII characters that ensures the privacy of the data (by means of encryption) that a NMS is sending to this device or receiving from this device through SNMP v3. **Authentication Protocol**: The APC implementation of SNMPv3 supports MD5 authentication. Authentication will not occur unless MD5 is selected here. **Privacy Protocol:** The APC implementation of SNMPv3 supports DES as the protocol for encrypting and decrypting data. Privacy of transmitted data requires that DES is selected here. **Note:** You cannot select the privacy protocol if no authentication protocol is selected.

Option	Description
access control	You can configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles, but you can edit these settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks. • If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device. • If you configure multiple access entries for one user profile, the limit of four entries requires that one or more of the other user profiles must have no access control entry. If no access control entry is listed for a user profile, no NMS that uses that profile has any access to this device. To edit the access control settings for a user profile, click its user name. **Access:** Mark the "Enable" checkbox to activate the access control specified by the parameters in this access control entry. **User Name:** Select from the drop-down list the user profile to which this access control entry will apply. The choices available are the four user names that you configure through the "user profiles" option on the left navigation menu. **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contain 255 restricts access as follows: • 149.225.12.255: Access only by an NMS on the 149.225.12 segment. • 149.225.255.255: Access only by an NMS on the 149.225 segment. • 149.255.255.255: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

FTP Server (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 PDU. The FTP server uses both the specified port and the port one number lower than the specified port.

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

FTP transfers files without encryption. For higher security, disable the FTP server, and transfer files with SCP. Selecting and configuring SSH enables SCP automatically.

At any time that you want a Switched Rack PDU to be accessible for management by InfraStruXure Manager, FTP Server must be enabled.

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

Administration: Notification and Logging

Event Actions (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
  - SNMPv1 and SNMPv3 traps
  - Syslog notification
- Indirect notification in the event log. If no direct notification is configured, users must check the log to determine which events have occurred.

For another method of indirect notification, see SNMP for SNMPv1 and SNMPv3 setup and configuration. SNMPv1 enables a NMS to perform informational queries. Configuring the most restrictive SNMP access type, READ, enables informational queries without the risk of allowing remote configuration changes. SNMPv3 uses a system of user profiles to communicate with a MIB software program to perform GETs, SETs, and receive traps.

You can also log system performance data to use for device monitoring. See Data log (Logs>Data>options) for information on how to configure and use this data logging option.

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, 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.

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, trap receivers, or paging recipients, but you cannot add or remove recipients or receivers. To add or remove recipients or receivers, see the following:

- Identifying Syslog Servers (Logs>Syslog>servers)
- E-mail recipients (Administration>Notification>E-mail>recipients)
- Indirect Notification Through Logs or Queries
- Trap Receivers (Administration>Notification>SNMP Traps>trap receivers)

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 (Administration>Network>DNS>options).

- The IP address or DNS name for **SMTP Server** and **From Address.**

See SMTP (Administration>Notification>E-mail>server).

- The e-mail addresses for a maximum of four recipients.

See E-mail recipients (Administration>Notification>E-mail>recipients).

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

SMTP (Administration>Notification>E-mail>server).

Setting	Description
Local SMTP Server	The IP address or DNS name of the local SMTP server. **NOTE:** This definition is required only when **SMTP Server** is set to **Local**. See E-mail recipients (Administration>Notification>E-mail>recipients).
From Address	The contents of the **From** field in e-mail messages sent by the Rack PDU: • In the format *user*@ [*IP_address*] (if an IP address is specified as **Local SMTP Server**). • In the format *user@domain* (if a 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 (Administration>Notification>E-mail>recipients). Identify up to four e-mail recipients.

Setting	Description
To Address	The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, **myacct100@skytel.com**). The pager gateway will generate the page. To bypass the DNS lookup of the mail server's IP address, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly. **NOTE:** The recipient's pager must be able to use text-based messaging.

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

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

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

SNMP traps

Trap Receivers (Administration>Notification>SNMP Traps>trap receivers). This option lists, by NMS IP/Host Name, up to the maximum number (six) of trap receivers allowed.

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

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

SNMPv1 option.

Community Name	The name ("public" by default) used as an identifier when SNMPv1 traps are sent to this trap receiver.
Authenticate Traps	When this option is enabled (the default), the NMS identified by the NMS IP/Host Name setting will receive authentication traps (traps generated by invalid attempts to log on to this device). To disable that ability, unmark the checkbox.

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

See SNMPv3 (Administration>Network>SNMPv3>options) for information on creating user profiles and selecting authentication and encryption methods.

SNMP Trap Test (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 of the following are true:

- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver is enabled.

If a host name is selected for the **To** address, that host name can be mapped to a valid IP address.

To. Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver was ever configured, a link to the **Trap Receiver** configuration page is displayed. (If a trap receiver was deleted, or was reset to its default values by this or any other management application, the default values for its trap type are listed.)

Syslog (Logs>Syslog>*options*)

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

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

Identifying Syslog Servers (Logs>Syslog>servers).

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

Syslog Settings (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 PDU's Syslog messages (**User**, by default). **NOTE: User** best defines the Syslog messages sent by the Rack PDU. **Do not** change this selection unless advised to do so by the Syslog network or system administrator.

Setting	Definition
Severity Mapping	Maps each severity level of Rack PDU events to available Syslog priorities. You should not need to change the mappings. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the **Local Priority** settings: • **Severe** is mapped to **Critical.** • **Warning** is mapped to **Warning.** • **Informational** is mapped to **Info.** **NOTE:** To disable Syslog messages, see Configuring event actions.

Syslog Test and Format Example (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 PDU.

– The Header: A time stamp and the IP address of the Rack PDU.

– The message (MSG) part:

- The TAG field, followed by a colon and space, identifies the event type.
- The CONTENT field is the event text, followed (optionally) by a space and the event code.

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

Indirect Notification Through Logs or Queries

Event log (Logs>Events>*options*)

Displaying and using the event log (Logs>Events>log). View or delete the event log. The log displays events recorded since it was last deleted, in reverse chronological order. By default, all events are logged:

- You can view the event log as a page of the Web interface (the default view) or, to see more of the listed events without scrolling, click **Launch Log in New Window** from that page to display a full-screen view of the log.

  You can also use FTP or SCP to view the event log. See How to use FTP or SCP to retrieve log files.

- To delete all events recorded in the log, click **Clear Event 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 group.

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.

Reverse Lookup (Logs>Events>reverse lookup). Reverse lookup is disabled by default. Enable this feature unless you have no DNS server configured or have poor network performance because of heavy network traffic.

With reverse lookup enabled, when a network-related event occurs, both the IP address and the domain name for the networked device associated with the event are logged in the event log. If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change less frequently than IP addresses, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events.

Data log (Logs>Data>*options*)

Displaying and using the data log (Logs>Data>log). View a log of measurements of the present load, including the minimum and maximum load current for each phase. Switched Rack PDU units for Blade servers will also display minimum and maximum load current for each outlet. Each entry is listed by the date and time the data was recorded.

- You can view the data log as a page of the Web interface (the default view) or, to see more of the data without scrolling, click **Launch Log in New Window** from that page to display a full-screen view of the log.

  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.

- 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.

Setting 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.

Configuring 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 retrieve data from the repository file.
Password	The password required to retrieve data from the repository file.
File Path	The path to the repository file.
File Name	The name of the repository file (an ASCII text file).
Automatically Upload Every	The number of hours between uploads of data to the file.
Maximum Retries	The maximum number of times the upload will be attempted after initial failure.
Failure Wait Time	How long in minutes before an attempt to upload data times out.

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

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

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

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

See the *Security Handbook*, available on the Switched Rack PDU *Utility* CD and on the APC Web site (**www.apc.com**) for information on available protocols and methods for setting up the type of security you need.

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

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

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

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

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

1. At a command prompt, type `ftp` and the Rack PDU's IP address, 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 Firmware file transfer methods. You can specify any port from 5001 to 32768.

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

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

   or

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

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

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

   or

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

   You will not be asked to confirm the deletion.
   - –If you clear the data log, the event log records a deleted-log event.
   - –If you clear the event log, a new *event.txt* file records the event.
5. Type **`quit`** at the **`ftp>`** prompt to exit from FTP.

Queries (SNMP GETs)

See SNMP for a description of SNMP access types that enable a NMS to perform informational queries. Configuring the most restrictive SNMP access type, READ, enables informational queries without allowing remote configuration changes.

Administration: General Options

Identification (Administration>General>Identification)

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

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

Set the Date and Time

Method (Administration>General>Date & Time>mode)

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

- **Manual Mode**: Do one of the following:
  - Enter the date and time for the Rack PDU.
  - 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 PDU.

Setting	Definition
Primary NTP Server	Enter the IP address or domain name of the primary NTP server.
Secondary NTP Server	Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.

Setting	Definition
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 PDU accesses the NTP Server for an update. *Minimum*: 1; *Maximum*: 8760 (1 year).
Update Using NTP Now	Initiate an immediate update of date and time by the NTP Server.

Daylight saving (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 (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 (Administration>General>User Config File)

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

Status	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 PDU can use it to set its own configuration.

To retrieve and customize the file of a configured Rack PDU, see Retrieving and Exporting the .ini File.

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

Temperature Units (Administration>General>Unit Preference)

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

Reset the Interface (Administration>General>Reset/Reboot)

Action	Definition
Reboot Management Interface	Restarts the interface of the Rack PDU.
Reset All[1]	Checkmark **Include TCP/IP** to reset all configuration values; unmark **Include TCP/IP** 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 PDU receive its TCP/IP settings from a DHCP or BOOTP server. See TCP/IP settings (Administration>Network>TCP/IP).
	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. The Rack PDU name and output voltage settings will not be reset.	

Configure Links (Administration>General>Quick Links)

Select the **Administration** tab, **General** on the top menu bar, and **Quick Links** on the left navigation menu to view and change the URL links displayed at the bottom left of each page of the interface.

By default, these links access the following Web pages:

- **Link 1**: The home page of the APC Web site.
- **Link 2**: A page where you can use samples of APC Web-enabled products.
- **Link 3**: The home page of the APC Remote Monitoring Service.

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

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

About the Rack PDU (Administration>General>About)

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

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

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

APC Device IP Configuration Wizard

Capabilities, Requirements, and Installation

How to use the Wizard to configure TCP/IP settings

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

- Remotely over your TCP/IP network to discover and configure unconfigured Network Management Cards 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 Network Management Card or device to configure or reconfigure it.

System requirements

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

Installation

To install the Wizard from the APC Switched Rack PDU *Utility* CD:

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

To install the Wizard from a downloaded executable file:

1. Go to **www.apc/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 PDUs.

Launch the Wizard

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

Configure the basic TCP/IP settings remotely

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

1. Contact your network administrator to obtain valid TCP/IP settings.
2. If you are configuring multiple unconfigured Network Management Cards 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.)

   –For a Network Management Card that you install, the MAC address is on a label on the bottom of the card.

   –For a network-enabled device (with an embedded Network Management Card), the MAC address is on a label on the device.

   You can also obtain the MAC address from the Quality Assurance slip that came with the Network Management Card or device.

Run the Wizard to perform the configuration. To discover and configure unconfigured Network Management Cards or network-enabled devices over the network:

1. From the **Start** menu, launch the Wizard. The Wizard detects the first Network Management Card 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 Network Management Card or device identified by the MAC address. Click **Next >**.

on the **Transmit Current Settings Remotely** screen, if you checkmark **Start a Web browser when finished**, the default Web browser connects to the Network Management Card 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 Network Management Card or device, it displays the screen to enter TCP/IP settings. Repeat this procedure beginning at step 3, or to skip the Network Management Card 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 serial configuration cable (which came with the Network Management Card or device) from an available communications port on your computer to the serial port of the card or device. Make sure no other application is using the computer port.
3. From the **Start** menu, launch the Wizard application.
4. If the Network Management Card 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 Network Management Card or device, and click **Next >**.
7. On the **Transmit Current Settings Remotely** screen, if you checkmark **Start a Web browser when finished**, the default Web browser connects to the Network Management Card 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 7, you can now configure other parameters through the Web interface of the card or device.

How to Export Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

As an Administrator, you can retrieve a dynamically generated .ini file of a Switched Rack PDU's current configuration and export that file to another Switched Rack PDU or to multiple Switched Rack PDUs.

1. Configure a Switched Rack PDU to have the settings you want to export.
2. Retrieve the .ini file from that Rack PDU.
3. Customize the .ini file (to change at least the TCP/IP settings) and make a copy to export.
4. Use any of the file transfer protocols supported by the Switched Rack PDU to transfer the copied file to one or more additional Rack PDUs. (To transfer the file to multiple Rack PDUs simultaneously, write an FTP or SCP script that repeats the steps for transferring the file to a single Rack PDU.)
5. Each receiving Switched Rack PDU stores the file temporarily in its flash memory, uses it to reconfigure its own Rack PDU settings, and then deletes the file.

Contents of the .ini file

The config.ini file that you retrieve from a Switched Rack PDU contains the following:

- *Section headings*, which are category names enclosed in brackets ([ ]), and under each section heading, *keywords,* which are labels describing specific Rack PDU settings.

  Only section headings and keywords supported for the specific device associated with the Rack PDU from which you retrieve the file are included.

- Each keyword is followed by an equals sign and the current *value* for that parameter's setting, either the default value (if the value has not been specifically configured) or the configured value.
  - The **`Override`** keyword, with its default value, prevents one or more keywords and their device-specific values from being exported. In the **`[NetworkTCP/IP]`** section, the default value for **`Override`** (the MAC address of the Rack PDU) blocks the exporting of the values for the keywords **`SystemIP`**, **`SubnetMask`**, **`DefaultGateway`**, and **`BootMode`**.
  - You must edit the section **`[SystemDate/Time]`** if you want to set the system date and time of a receiving Rack PDU or cause that Rack PDU to use a NTP Server to set its date and time.

    See Method (Administration>General>Date & Time>mode) for configuration guidelines for date and time settings.

Detailed procedures

Use the following procedures to retrieve the settings of one Switched Rack PDU and export them to one or more other Switched Rack PDUs.

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

1. Configure a Rack PDU with the settings you want to export.

   To avoid errors, configure the Rack PDU by using its Web interface or control console whenever possible. Directly editing the .ini file risks introducing errors.

2. Use FTP to retrieve the file config.ini from the Rack PDU you configured:
   a. Open a connection to the Rack PDU, using its IP Address. For example:

      ```
      ftp> open 158.165.2.132
      ```

   b. Log on, using the Administrator user name and password configured for the Rack PDU.
   c. Retrieve the config.ini file containing the Rack PDU's current settings:

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

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

To create batch files and use an APC utility to retrieve configuration settings from multiple Rack PDUs and export them to other Rack PDUs, see *Release Notes: ini File Utility, version 1.0* on the APC Switched Rack PDU *Utility* CD.

Customizing. You must customize the file to change at least the TCP/IP settings 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.

– To define values, opening and closing quotation marks are optional, except to enclose values that contain leading or trailing spaces or values which are already enclosed in quotation marks. (Leading or trailing spaces not within the opening and closing quotation marks are ignored.)

– To export a specific system date and time or any scheduled events, you must configure the values directly in the .ini file.

- To export a specific system time, export only the configured **`[SystemDate/Time]`** section as a separate .ini file. (The time necessary to export a large file would cause the configured time to be significantly inaccurate.)
- For greater accuracy, if the Switched Rack PDUs receiving the file can access a Network Time Protocol (NTP) Server, set the value for the **`NTPEnable`** keyword as follows:

```
NTPEnable=enabled
```

– Add comments about changes that you made. The first printable character of a comment line must be a semicolon (**`;`**).

2. Copy the customized file to another file name in the same folder:

– The copy, which you will export to other Rack PDUs, can have any file name up to 64 characters and must have the .ini file suffix.

– Retain the original customized file for future use. **The file that you retain is the only record of your comments.** They are removed automatically from the file that you export.

Exporting the file to a single Rack PDU. To export the .ini file to another Switched Rack PDU, use any of the file transfer protocols supported by Switched Rack PDUs (including FTP, FTP Client, SCP, and TFTP). The following example uses FTP:

1. From the folder containing the customized .ini file and its copy, use FTP to log in to the Rack PDU to which you are exporting the .ini file. For example:

```
ftp> open 158.165.4.135
```

2. Export the copy of the customized .ini file. The receiving Rack PDU accepts any file name that has the .ini suffix, is no more than 64 characters in length, and is exported to its root directory.

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

Exporting the file to multiple Rack PDUs. To export the .ini file to multiple Switched Rack PDUs:

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

To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* on the APC Switched Rack PDU *Utility* CD.

The Upload Event and Error Messages

The event and its error messages

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

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

This event has no default severity level.

If a keyword, section name, or value is invalid, the event text is extended to include notification of the following errors.

The export to and the subsequent upload by the receiving Rack PDU succeeds even if there are errors.

Event text	Description
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number.*	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number*.	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, the Rack PDU stores and processes what it can, but ignores what it cannot. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in config.ini

A feature might not be supported for the device from which you retrieve the configuration settings or might not be supported for the device to which you export the configuration settings. In this case, the user configuration file contains, under the section name for that feature, a message stating that the feature is not supported. No keywords and values are listed, and that feature will not be configured on any device to which you export the user configuration file.

Errors generated by overridden values

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

See Contents of the .ini file for information about which values are overridden.

The overridden values are device-specific and not appropriate to export to other Rack PDUs. Therefore, you can ignore these error messages. To prevent these error messages from occurring, you can delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Using the APC Device IP Configuration Wizard

On Windows operating systems, instead of using the preceding procedure for exporting .ini files, you can choose to update the basic TCP/IP settings of Rack PDUs by using the APC Device IP Configuration Wizard.

See APC Device IP Configuration Wizard for a detailed description of how to discover and configure unconfigured Switched Rack PDUs remotely over your TCP/IP network or configure or reconfigure a Switched Rack PDU through a direct connection from the serial port of your computer to the Switched Rack PDU.

File Transfers

Introduction

Overview

The Switched Rack PDU automatically recognizes binary firmware files. Each of these files contains a header and one or more Cyclical Redundancy Checks (CRCs) to ensure that the data contained in the file is not corrupted before or during the transfer operation.

To transfer a firmware file to a Rack PDU, see Upgrading Firmware: Methods and Tools.

To verify a file transfer, see Verifying Upgrades and Updates.

Upgrading Firmware: Methods and Tools

Benefits of upgrading firmware

Upgrading the firmware on the Switched Rack PDU has the following benefits:

- New firmware has 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 Switched Rack PDUs support the same features in the same manner.

Firmware files (Switched Rack PDU)

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module.

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

`apc_hw0x_type_version.bin`

- **apc**: Indicates that this is an APC file.
- **hw0*x***: Identifies the version of the Switched Rack PDU that will run this binary file.
- *type*: Identifies whether the file is for the APC Operating System (AOS) or the application module (APP) for the Switched Rack PDU.
- *version*: The version number of the application file. For example, a code of 331 would indicate version 3.3.1.
- **bin**: Indicates that this is a binary file.

Obtain the latest firmware version

Automated upgrade tool for Microsoft Windows systems. An automated self-extracting executable tool combines the firmware modules that you need to automate your upgrades on any supported Windows operating system.

- You can obtain an updated version of the tool at no cost from the support section of the APC Web site **www.apc.com/tools/download**. At this Web page, find the latest firmware release for your APC product (in this case, your Rack PDU) and download the automated tool, not the individual firmware modules.

Each upgrade tool is specific to an APC product type. If you use a version of the tool from the APC Web site, make sure that you use the upgrade tool that corresponds with your APC product type.

Manual upgrades, primarily for Linux systems. If all computers on your network are running Linux, you must upgrade the firmware of your Rack PDUs manually, i.e., by using the separate APC firmware modules (AOS module and application module).

If you have a networked computer running a supported Microsoft Windows operating system on your network, you can use the tool described in Automated upgrade tool for Microsoft Windows systems to upgrade the firmware of a Switched Rack PDU automatically over the network. This tool automates the entire upgrade process.

You can obtain the individual firmware modules you need for a manual firmware upgrade from the support section of the APC Web site, **www.apc.com/tools/download**.

Firmware file transfer methods

To upgrade the firmware of a Switched Rack PDU:

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

When you transfer individual firmware modules and do not use the automated firmware upgrade tool to upgrade the firmware for a Rack PDU, you must transfer the APC Operating System (AOS) module to the Rack PDU before you transfer the application module.

For more information about the firmware modules, see Firmware files (Switched Rack PDU).

Use FTP or SCP to upgrade one Rack PDU

Instructions for using FTP. For you to be able to use FTP to upgrade a single Switched Rack PDU over the network:

- The Switched Rack PDU must be connected to the network.
- The FTP server must be enabled at the Switched Rack PDU.
- The Switched Rack PDU must have its TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway** addresses) configured.

To use FTP to upgrade the Rack PDU:

1. Open an MS-DOS command prompt window on a computer that is connected to the network. Go to the directory that contains the firmware upgrade files, and list the files. For the directory **`C:\apc`**, the commands would be those shown in **bold**:

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

   Files listed for a Switched Rack PDU, for example, might be the following:

   – **`apc_hw02_aos_XXX.bin`**

   – **`apc_hw02_app_XXX.bin`**

2. Open an FTP client session:

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

3. Type **`open`** and the Switched Rack PDU's IP address, and press ENTER. If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default of **21**, you must use the non-default value in the FTP command.

   a. For some FTP clients, use a colon to add the port number to the end of the IP address.

   b. For Windows FTP clients, separate the port number from the IP address by a space. For example, if the Rack PDU's **FTP Server Port** setting has been changed from its default of **21**, such as to **21000**, you would use the following command for a Windows FTP client transferring a file to a Rack PDU with an IP

address of 150.250.6.10.

```
ftp> open 150.250.6.10 21000
```

4. Log on using the Administrator user name and password. (**apc** is the default for both.)
5. Upgrade the AOS. For example:

```
ftp> bin
ftp> put apc_hw02_aos_XXX.bin
```

6. When FTP confirms the transfer, type **Quit** to close the session.
7. Wait 20 seconds, and then repeat step 2 through step 6, but in step 5, use the application module file name instead of the AOS module.

Instructions for using SCP. To use Secure CoPy (SCP) to upgrade the firmware for one Rack PDU:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the Rack PDU. The following example assumes a Rack PDU IP address of 158.205.6.185, and an AOS module of **apc_hw02_aos_*XXX*.bin**.)

```
scp apc_hw02_aos_XXX.bin apc@158.205.6.185:apc_hw02_aos_XXX.bin
```

3. Use a similar SCP command line, with the name of the application module instead of the AOS module, to transfer the application module to the Rack PDU.

How to upgrade multiple Rack PDUs

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

See *Release Notes: ini File Utility, version 1.0* on the APC Switched Rack PDU *Utility* CD.

Use FTP or SCP to upgrade multiple Rack PDUs. To upgrade multiple Switched Rack PDUs using an FTP client or using SCP, write a script which automatically performs the procedure. For FTP, use the steps in Use FTP or SCP to upgrade one Rack PDU.

Use XMODEM to upgrade one Rack PDU

To use XMODEM to upgrade the firmware for a single Switched Rack PDU that is not on the network:

1. Obtain the individual firmware modules (the AOS module and the application module) from the support section of the APC Web site **www.apc.com/tools/download**.
2. Select a serial port at the local computer and disable any service that uses the port.
3. Connect the advanced signaling cable that came with the Rack PDU to the selected port and to the serial port at the Rack PDU.
4. Run a terminal program such as HyperTerminal, and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control, and save the changes.
5. Press ENTER to display the **User Name** prompt.
6. Enter your Administrator user name and password (**apc** by default for both).
7. From the **Control Console** menu, select **System**, then **Tools**, then **File Transfer**, then **XMODEM**; and type **`Yes`** at the prompt to continue.
8. Select a baud rate, change the terminal program's baud rate to match your selection, and press ENTER. A higher baud rate causes faster upgrades.
9. From the terminal program's menu, select the binary AOS file to transfer using XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600. The Rack PDU automatically restarts.
10. Repeat **step 4** through **step 9** to install the application module. In **step 9**,

substitute the application module file name for the AOS module file name.

For information about the format used for application modules, see Firmware files (Switched Rack PDU).

Note: Upgrading the firmware will not interfere with the operation of the outlets. The Rack PDU will restart when the download is complete.

Verifying Upgrades and Updates

Verify the success or failure of the transfer

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

Last Transfer Result codes

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

Verify the version numbers of installed firmware

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

Product Information

Two-Year Factory Warranty

This warranty applies only to the products you purchase for your use in accordance with this manual.

Terms of warranty

APC warrants its products to be free from defects in materials and workmanship for a period of two years from the date of purchase. APC will repair or replace defective products covered by this warranty. This warranty does not apply to equipment that has been damaged by accident, negligence or misapplication or has been altered or modified in any way. Repair or replacement of a defective product or part thereof does not extend the original warranty period. Any parts furnished under this warranty may be new or factory-remanufactured.

Non-transferable warranty

This warranty extends only to the original purchaser who must have properly registered the product. The product may be registered at the APC Web site, **www.apc.com**.

Exclusions

APC shall not be liable under the warranty if its testing and examination disclose that the alleged defect in the product does not exist or was caused by end user's or any third person's misuse, negligence, improper installation or testing. Further, APC shall not be liable under the warranty for unauthorized attempts to repair or modify wrong or inadequate electrical voltage or connection, inappropriate on-site operation conditions, corrosive atmosphere, repair, installation, exposure to the elements, Acts of God, fire, theft, or installation contrary to APC recommendations or specifications or in any event if the APC serial number has been altered, defaced, or removed, or any other cause beyond the range of the intended use.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, BY OPERATION OF LAW OR OTHERWISE, OF PRODUCTS SOLD, SERVICED OR FURNISHED UNDER THIS AGREEMENT OR IN CONNECTION HEREWITH. APC DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTION AND FITNESS FOR A PARTICULAR PURPOSE. APC EXPRESS WARRANTIES WILL NOT BE ENLARGED, DIMINISHED, OR AFFECTED BY AND NO OBLIGATION OR LIABILITY WILL ARISE OUT OF, APC RENDERING OF TECHNICAL OR OTHER ADVICE OR SERVICE IN CONNECTION WITH THE PRODUCTS. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES AND REMEDIES. THE WARRANTIES SET FORTH ABOVE CONSTITUTE APC'S SOLE LIABILITY AND PURCHASER'S EXCLUSIVE REMEDY FOR ANY BREACH OF SUCH WARRANTIES. APC WARRANTIES EXTEND ONLY TO PURCHASER AND ARE NOT EXTENDED TO ANY THIRD PARTIES.

IN NO EVENT SHALL APC, ITS OFFICERS, DIRECTORS, AFFILIATES OR EMPLOYEES BE LIABLE FOR ANY FORM OF INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, ARISING OUT OF THE USE, SERVICE OR INSTALLATION, OF THE PRODUCTS, WHETHER SUCH DAMAGES ARISE IN CONTRACT OR TORT, IRRESPECTIVE OF FAULT, NEGLIGENCE OR STRICT LIABILITY OR WHETHER APC HAS BEEN ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES. SPECIFICALLY, APC IS NOT LIABLE FOR ANY COSTS, SUCH AS LOST PROFITS OR REVENUE, LOSS OF EQUIPMENT, LOSS OF USE OF EQUIPMENT, LOSS OF SOFTWARE, LOSS OF DATA, COSTS OF SUBSTITUENTS, CLAIMS BY THIRD PARTIES, OR OTHERWISE.

NO SALESMAN, EMPLOYEE OR AGENT OF APC IS AUTHORIZED TO ADD TO OR VARY THE TERMS OF THIS WARRANTY. WARRANTY TERMS MAY BE MODIFIED, IF AT ALL, ONLY IN WRITING SIGNED BY AN APC OFFICER AND LEGAL DEPARTMENT.

Warranty claims

Customers with warranty claims issues may access the APC customer support network through the Support page of the APC Web site, **www.apc.com/support**. Select your country from the country selection pull-down menu at the top of the Web page. Select the Support tab to obtain contact information for customer support in your region.

Index

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

W

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.

Copyright

990-1368F-001 **10/2008**