User Guide

Modular Power Distribution Unit 480V:240V with Auto-transformer

PDPM288G6H

Contents

Introduction

Product Features

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

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

Initial setup

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

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

NOTICE

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

To configure the TCP/IP settings, see the Modular PDU *Installation and Start-Up Manual*, available in printed form and on the APC Web site, **www.apc.com**.
For detailed information on how to use a DHCP server to configure the TCP/IP settings at the Modular PDU, see “TCP/IP and Communication Settings” on page 23.

Network management features

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

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

Internal Management Features

Overview

Use the Web interface or the control console interface to manage the Modular PDU.

Access priority for logging on

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

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

Types of user accounts

The Modular PDU has three levels of access (Administrator, Device User, and Read-Only User), which are protected by user name and password requirements. During authentication, the user's credentials are compared against the Local User Database and/or are validated against a RADIUS server (depending on configuration). If valid, access with appropriate permissions is granted to the web interface. To set User Name and Password values for the three account types, see “Setting user access” on page 19.

- An Administrator can use all the menus in the Web interface. The default user name and password are both **apc**.
- The default user name for the Device User is **device**, and the default password is **apc**. A Device User can access the menus on the **Home**, **Power Distribution**, **Contacts/Relays**, **Alarms**, and **Logs** tabs and the event and data logs in the Web interface.
- A Read-Only User has access through the Web interface only. You must use the Web interface to configure values for the Read-Only User. The Read-Only User has access to the same tabs and menus as a Device User, but without any capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled, and the event and data logs display no button to clear the log. The default user name is **readonly**, and the default password is **apc**.

How to Recover from a Lost Password

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

1. At the local computer, select a serial port, and disable any service that uses it.
2. Connect the provided serial cable from the selected port on the computer to the configuration port at the Modular 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 **command line interface** 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.

Watchdog Features

Overview

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

Network interface watchdog mechanism

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

Resetting the network timer

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

Control Console

Log On

Use either a local (serial) connection or a remote (Telnet or SSH) connection with a computer on the same network (LAN) as the Modular PDU 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.

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

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

Local access to the control console

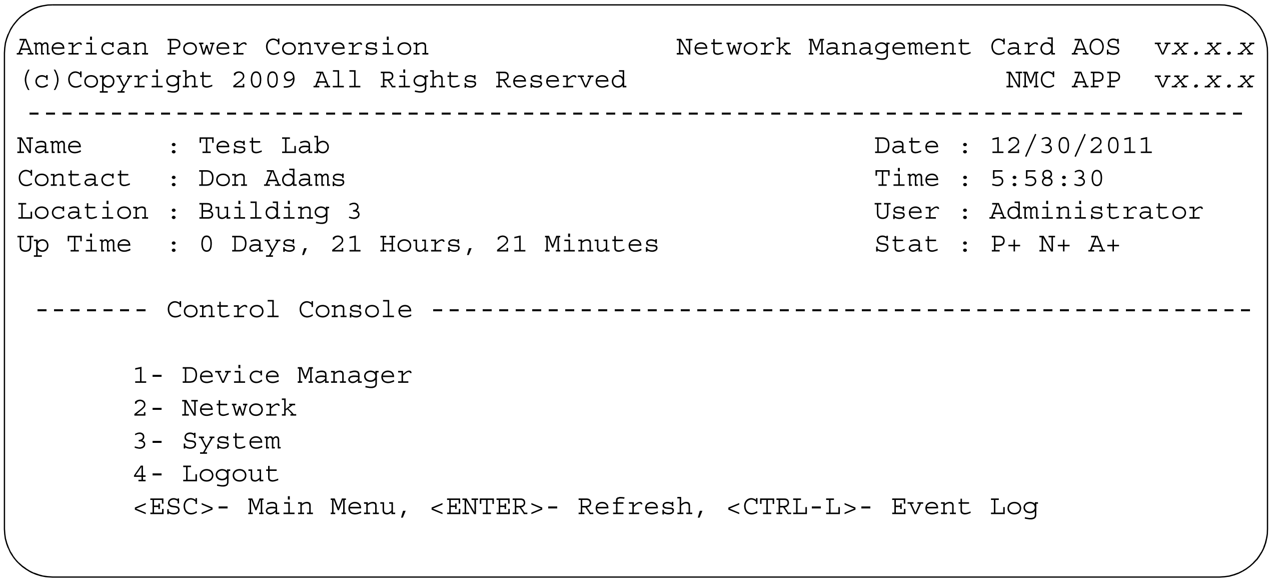
For local access, use a computer that connects to the Modular PDU through the serial port, to access the control console:

1. Select a serial port at the computer and disable any service that uses the port.
2. Connect the provided serial cable from the selected port on the computer to the configuration port at the NMC.
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, and at the prompts, enter your user name and password.

Main Screen

Sample main screen

The following is an example of the screen that displays when you log on to the control console at the NMC.



```
American Power Conversion             Network Management Card AOS  vx.x.x
(c)Copyright 2009 All Rights Reserved                     NMC APP  vx.x.x
 --------------------------------------------------------------------------
Name     : Test Lab                                   Date : 12/30/2011
Contact  : Don Adams                                  Time : 5:58:30
Location : Building 3                                 User : Administrator
Up Time  : 0 Days, 21 Hours, 21 Minutes               Stat : P+ N+ A+

 ------- 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.

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

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

```
Name: Test Lab

Contact: Don Adams

Location: Building 3
```

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

```
Up Time: 0 Days 21 Hours 21 Minutes
```

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

```
Date : 12/30/2011
Time : 5:58:30
```

- The **User** field reports 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.

- The **Stat** field reports the Modular 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 NMC failed to connect to the network.
N!	Another device is using the IP address of this NMC.
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 the APC support staff at **www.apc.com/support** even if you can still access the NMC.

- The status field displays the status of the PDU in which the NMC is installed. Under normal operation, this field displays **Communication Established**.

Control Console Menus

Overview

The control console provides options to monitor and configure the Modular PDU.

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 using a menu, you can also do the following:

- Type ? and press ENTER for menu option descriptions if help exists for the menu.
- 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+D to toggle between menus
- Press CTRL+L to access the event log

Control console structure

For menus not specific to the NMC but shared among APC network-enabled devices, names and locations of options differ from those of the Web interface. The menu structure in the control console is retained from earlier firmware versions for compatibility with scripts and programs that rely on that structure.

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 (equivalent to Device User in the Web interface), you can access only the **Device Manager** menus and the **Logout** menu.

Device Manager menu

An Administrator or Device User can use the options of the **Device Manager** menu to view parameters and display detailed status.

Network menu

To perform these tasks, use the options of the **Network** menu:

- Configure the TCP/IP settings of the NMC or, if the NMC obtains its TCP/IP settings from a server, configure the settings for the type of server (DHCP or BOOTP).
- Use the Ping utility.
- Define settings that affect FTP, Telnet and SSH, the Web interface and SSL, SNMP, e-mail, DNS, and Syslog.

System menu

Use the options of the **System** menu to perform these tasks:

- Control **Administrator** and **Device Manager** access. (**Read Only User** access is managed through the Web interface only.)
- Define the **Name**, **Contact**, and **Location** values for the system.
- Set the date and time used by the NMC.
- Through the **Tools** option:
  - Restart the NMC interface.
  - 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 Modular PDU. The current NMC then uses the values in that .ini file to configure its own settings.
- Access system information about the NMC.

Logout

Select the logout option to log out of the control console.

Web Interface

Introduction

Supported Web browsers

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

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

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

Log On

Overview

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

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

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

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

URL address formats

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

Common browser error messages at log-on.

Error Message	Browser	Cause of the Error
"You are not authorized to view this page" or "Someone is currently logged in..."	Internet Explorer, Firefox	Someone else is logged on.
"This page cannot be displayed."	Internet Explorer	Web access is disabled, or the URL was not correct
"Unable to connect."	Firefox	

Home Page

Overview

View active alarm conditions and the most recent events recorded in the event log.

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

Icon	Description
✗	**Critical**: A critical alarm exists, which requires immediate action.
⚠	**Warning**: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
✓	**No Alarms Present:** The Modular PDU is operating normally.

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

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

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

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

Tabs, Menus, and Links

Tabs

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

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

Menus

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

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

Top menu bar. The **Administration** tab has a selection of menu options on the top menu bar. Select one of the menu options to display its left navigation menu.

Quick Links

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

- **Link 1**: The home page of the APC Web site
- **Link 2**: Demonstrations of APC Web-enabled products.
- **Link 3**: Information on APC Remote Monitoring Services.

Managing Power Distribution

View Modular PDU Information

Power distribution alarm status

Path: Power Distribution > Overview

If an alarm exists, a status icon and accompanying text display at the top of the page.

View output measurements

Path: Power Distribution > System Output > measurements

Click **measurement**s to see detailed information about power leaving the PDU:

- Voltage: The phase-to-phase output voltage of a 3-wire connection, or the phase-to-neutral output voltage for a 4-wire connection.
- Current: The load supported by each phase, in RMS current (Irms).
- Power: The active power, in kW, provided for each phase and for the total of the three phases.
- Frequency: The frequency, in Hz, of the output.

View alarm configuration

Path: Power Distribution > System Output > alarm config

Select and check the boxes under **Output Voltage Thresholds**,or **Load Alarm Thresholds** to define the acceptable ranges.

- Maximum
- High
- Low
- Minimum

Select the Maximum Deviation for **Frequency Thresholds** or select Disabled.

When you have finished making your selections, click **Apply** to save your settings. Click **Cancel** to leave the page without saving your changes.

View Module status

Distribution Module Status can be shown **Populated Only** or by **All Locations**. The Status, Rating, Position, Load Name, Current, and Power are shown on each page.

Quick status icons. Color-coded icons show the status of the Modules:

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

Mass Configuration. All modules can be configured at the same time by clicking on **Mass Configuration** at the bottom right of either the **Populated Only** or by **All Locations** pages. Alarm generation and current threshold settings are selected on this page. Click on Apply to All Modules at the bottom of the page to enable the selections.

View Manufacturing information

Path: Power Distribution > Manufacturing Info > modules

View the status of the modules. The first selectable heading under **Manufacturing Info** is **modules**. All of the modules are listed in the page with Status, Model Number, Serial Number, Manufacturing Date and the number of Output Cables for each module. A status icon and accompanying text display next to the Status of the Module.

Path: Power Distribution > metering system

View the status of the metering system. The next selectable heading under **Manufacturing Info** is **metering system**. The metering system information for the modules is shown on the page. The Model Number, Serial Number, Manufacture Date and Firmware Revision number are all identified.

Path: Power Distribution > electrical config

View the status of the electrical configuration. The last selectable heading under Manufacturing Info is electrical config. Nominal Voltage and Maximum Panel Current are identified.

Configure Contacts and Relays

View and configure input contact settings

Path: Environment > Input Contacts

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

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

Configure output relays

Path: Environment > Output Relays

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

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

Monitor and Map Alarms

View active alarms

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

To view a complete event log, see “Logs” on page 14.

Configure the alarm relay map

Path: Environment > Alarm Relay Map

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

- system output
- power distribution
- environment: Contact 1–4 Alarms

Select **Apply** to save your settings and **Cancel** to leave the page without saving.

Logs

Use the Event and Data Logs

Event log

Path: Logs > Events > *options*

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

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

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

- By default, view the event log as a page of the Web interface.
- To see the listed events on one page, click **Launch Log in New Window** from the event log page to display a full-screen view of the log.
  Note: In your browser's options, JavaScript® must be enabled for you to use the **Launch Log in New Window** button. You can also use FTP or SCP to view the event log. See “Using FTP or SCP to retrieve log files” on page 17.

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

- **Filter the log by date or time:** To display the entire event log, or to change the number of days or weeks for which the log displays the most recent events, select **Last**. Select a time range from the drop-down menu, then click **Apply**. The filter configuration is saved until the Modular PDU restarts.
  To display events logged during a specific time range, select **From**. Specify the beginning and ending times (using the 24-hour clock format) and dates for which to display events, then click **Apply**. The filter configuration is saved until the Modular PDU restarts.
- **Filter the log by event**: To specify the events that display in the log, click **Filter Log**. Clear the check box of an event category or alarm severity level to remove it from view. Text at the upper right corner of the event log page indicates that a filter is active.
  As Administrator, click **Save As Default** to save this filter as the default log view for all users. If you do not click **Save As Default**, the filter is active until you clear it or until the Modular PDU restarts.
- To remove an active filter, click **Filter Log**, then **Clear Filter (Show All)**.
  Note: Events are processed through the filter using **OR** logic.
  - Events that are not selected from the **Filter By Severity** list never display in the filtered event log, even if the event occurs in a selected category from the **Filter by Category** list.
  - Events that are not selected from the **Filter by Category** list never display in the filtered event log, even if devices in the category enter an alarm state selected from the **Filter by Severity** list..

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

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

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

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

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

Data log

Path: Logs > Data > *options*

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

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

- By default, view the data log as a page of the Web interface.
- To see the listed data on one page, click **Launch Log in New Window** from the data log page to display a full-screen view of the log.
  Note: In your browser's options, JavaScript® must be enabled for you to use the **Launch Log in New Window** button. You can also use FTP or SCP to view the event log. See "Using FTP or SCP to retrieve log files" on page 17.

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

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

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

To view the entire data log, export the log and then view it using a spreadsheet application. To export the log, see "Using FTP or SCP to retrieve log files" on page 17.

To delete the data log:

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

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

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

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

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

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

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

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

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

Using FTP or SCP to retrieve log files

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

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

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

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

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

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

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

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

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

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

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

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

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

   ```
   ftp>open ip_address port_number
   ```

   To set a non-default port value to enhance security for the FTP Server, see "FTP Server" on page 33. You can specify any port from 5001 to 32768.

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

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

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

   or

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

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

   ```
   ftp>del event.txt
   or
   ftp>del data.txt
   ```

   You will not be asked to confirm the deletion.

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

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

Administration: Security

Local Users

Setting user access

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

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

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

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

Remote Users

Authentication

Path: Administration > Security > Remote Users > Authentication Method

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

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

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

- When a user accesses the Modular PDU that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user’s permission level.
- RADIUS user names used with the Modular PDU are limited to 32 characters.

Select one of the following:

- **Local Authentication Only**: RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Authentication**: RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used.
- **RADIUS Only**: RADIUS is enabled. Local authentication is disabled.
  Note: If **RADIUS Only** is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, you must use a serial connection to the command line interface and change the **Access** setting to **Local Authentication Only** or **RADIUS, then Local Authentication** to regain access.

RADIUS

Path: Administration > Security > Remote Users > RADIUS

Use this option to do the following:

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

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

Configure the RADIUS Server

Summary of the configuration procedure

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

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

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

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

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

Configure a RADIUS server on UNIX® with shadow passwords

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

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

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

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

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

Supported RADIUS servers

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

Inactivity Timeout

Path: Administration > Security > Auto Log Off

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

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

Administration: Network Features

TCP/IP and Communication Settings

TCP/IP settings

Path: Administration > Network > TCP/IP

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

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

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

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

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

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

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

DHCP response options

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

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

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

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

  To disable the requirement of an APC cookie, see "DHCP" on page 23.

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

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

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

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

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

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

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

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

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

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

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

Port Speed

Path: Administration > Network > Port Speed

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

- For **Auto-negotiation** (the default), Ethernet devices negotiate to transmit at the highest possible speed, but if the supported speeds of two devices are unmatched, the slower speed is used.
- Alternatively, you can choose 10 Mbps or 100 Mbps, each with the option of half-duplex (communication in only one direction at a time) or full-duplex (communication in both directions on the same channel simultaneously).

DNS

Path: Administration > Network > DNS > *options*

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

- Select **servers** to specify the IP addresses of the primary and optional secondary DNS server. For the Modular PDU to send e-mail, at least the IP address of the primary DNS server must be defined.
  - The Modular PDU waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the Modular PDU does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the Modular PDU or on a nearby segment (but not across a wide-area network [WAN]).
  - After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for that computer.
- Select **naming** to define the host name and domain name of the Modular PDU:
  - **Host Name**: After you configure a host name here and a domain name in the **Domain Name** field, users can enter a host name in any field in the Modular PDU interface (except e-mail addresses) that accepts a domain name.
  - **Domain Name**: You need to configure the domain name here only. In all other fields in the Modular PDU interface (except e-mail addresses) that accept domain names, the Modular PDU adds this domain name when only a host name is entered.
    - To override all instances of the expansion of a specified host name by the addition of the domain name, set the domain name field to its default, `somedomain.com`, or to `0.0.0.0`.
    - To override the expansion of a specific host name entry (for example, when defining a trap receiver) include a trailing period. The Modular PDU recognizes a host name with a trailing period (such as *`mySnmpServer.`*) as if it were a fully qualified domain name and does not append the domain name.
- Select **Test** to send a DNS query that tests the setup of your DNS servers:
  - As **Query Type**, select the method to use for the DNS query:
    - **by Host**: the URL name of the server
    - **by FQDN**: the fully qualified domain name
    - **by IP**: the IP address of the server
    - **by MX**: the Mail Exchange used by the server

– As **Query Question**, identify the value to be used for the selected query type:

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

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

Web

Path: Administration > Network > Web > *options*

Option	**Description**

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

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

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

Console

Path: Administration > Network > Console > *options*

Option	Description

access	Choose one of the following for access by Telnet or Secure SHell (SSH):
	• **Disable**: Disables all access to the command line interface.
	• **Enable Telnet** (the default): Telnet transmits user names, passwords, and data without encryption.
	• **Enable SSH v1 and v2**: Do not enable both versions 1 and 2 of SSH unless you require both. (They use extensive processing power.)
	• **Enable SSH v1 only**: SSH version 1 encrypts user names, passwords, and data for transmission. There is little or no delay as you log on.
	• **Enable SSH v2 only**: SSH version 2 transmits user names, passwords, and data in encrypted form with more protection than version 1 from attempts to intercept, forge, or alter data during transmission. There is a noticeable delay as you log on.
	
	Configure the ports to be used by these protocols:
	• **Telnet Port**: The Telnet port used to communicate with the Modular PDU (23 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) or a space, as required by your Telnet client program, to specify the non-default port. For example, for port 5000 and an IP address of 152.214.12.114, your Telnet client requires one of the these commands:
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• **SSH Port**: The SSH port used to communicate with the Modular PDU (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port.

ssh encryption	Enable or disable encryption algorithms (block ciphers) compatible with SSH version 1 or version 2 clients: If your SSH v1 client cannot use **Blowfish**, you must also enable **DES**. Your SSH v2 client selects the enabled algorithm that provides the highest security. If the client cannot use the default algorithms (**3DES** or **Blowfish**), enable an AES algorithm that it can use (**AES 128** or **AES 256**)

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

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

SNMP

SNMPv1

Path: Administration > Network > SNMPv1 > *options*

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

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

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

Option	Description
access	**Enable SNMPv1 Access:** Enables SNMP version 1 as a method of communication with this device.
access control	You can configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four available SNMPv1 communities, but you can edit these settings to apply more than one entry to any community to grant access by several specific IP addresses, host names, or IP address masks. To edit the access control settings for a community, click its community name. • If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network. • If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device. **Community Name:** The name that a Network Management System (NMS) must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are `public`, `private`, `public2`, and `private2`. **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows: • 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment. • 149.225.**255.255**: Access only by an NMS on the 149.225 segment. • 149.**255.255.255**: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. **Access Type**: The actions an NMS can perform through the community. • **Read**: GETS only, at any time • **Write**: GETS at any time, and SETS when no user is logged onto the Web interface or command line interface. • **Write+**: GETS and SETS at any time. • **Disabled**: No GETS or SETS at any time.

SNMPv3

Path: Administration > Network > SNMPv3 > *option*

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. You must have a MIB program that supports SNMPv3. The Modular PDU supports only MD5 authentication and DES encryption.

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

Option	Description
user profiles	By default, lists the settings of four user profiles, configured with the user names **apc snmp profile1** through **apc snmp profile4**, no authentication and no privacy (no encryption). To edit the following settings for a user profile, click a user name in the list. **User Name:** The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters. **Authentication Passphrase:** A phrase of 15 to 32 ASCII characters (`apc auth passphrase`, by default) that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time. **Privacy Passphrase:** A phrase of 15 to 32 ASCII characters (`apc crypt passphrase`, by default) that ensures the privacy of the data (by means of encryption) that an NMS is sending to this device or receiving from this device through SNMPv3. **Authentication Protocol:** Supports MD5 authentication. Authentication will not occur unless MD5 is selected as the authentication protocol. **Privacy Protocol:** Supports DES as the protocol for encrypting and decrypting data. Privacy of transmitted data requires that DES is selected. It cannot be selected unless an authentication protocol is selected.
access control	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. Edit the 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. • Leave the default access control entry unchanged for a user profile and all NMSs that use that profile have access to this device. • Multiple access entries for one user profile, means there can be no access control entry for one or more of the other user profiles. If no access control entry is listed for a user profile, NMSs using that profile have no 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 access control. **User Name:** Select the user profile to which access control will apply. The choices are the four user names you configured in the **user profiles** option. **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 allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows: • 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment. • 149.225.**255**.**255**: Access only by an NMS on the 149.225 segment. • 149.**255**.**255**.**255**: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

FTP Server

Path: Administration > Network > FTP Server

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

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

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

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

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

Administration: Notification and Logging

Event Actions

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

Types of notification

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

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

For another method of indirect notification, see “SNMP” on page 30. SNMP enables an NMS to perform informational queries. For SNMPv1, configuring the most restrictive SNMP access type, READ, enables informational queries without the risk of allowing remote configuration changes.

You can also log system performance data to use for device monitoring. See “Data log” on page 15 for information on how to configure and use this data logging option.

Configure event actions

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

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

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

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.
2. In the list of events, review the marked columns to see whether the action you want is already configured. (By default, logging is configured for all events.)
3. To view or change the current configuration, such as recipients to be notified by e-mail, or Network Management Systems (NMSs) to be notified by traps, click on the event name.

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

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

- "Identifying Syslog Servers" on page 39
- "E-mail recipients" on page 37
- "Trap Receivers" on page 38

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

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

   b. Select whether to leave the newly configured event action enabled for this group of events or to disable the action.

Active, Automatic, Direct Notification

E-mail notification

Overview of setup. Use the Simple Mail Transfer Protocol (SMTP) to send e-mail to up to four recipients when an event occurs.

To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and, optionally, the secondary Domain Name System (DNS) servers. (See “DNS” on page 26.)
- The IP address or DNS name for **SMTP Server** and **From Address**.
- The e-mail addresses for a maximum of four recipients. (See “E-mail recipients” on page 37.)

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

SMTP.

Path: Administration > Notification > E-mail > server

Setting	Description
Local SMTP Server	The IP address or DNS name of the local SMTP server. **NOTE:** This definition is required only when **SMTP Server** is set to **Local**. See “E-mail recipients” on page 37.
From Address	The contents of the **From** field in e-mail messages sent by the Modular PDU: • In the format *user@* [*IP_address*] (if an IP address is specified as **Local SMTP Server**) • In the format *user@domain* (if DNS is configured and the DNS name is specified as **Local SMTP Server**) in the e-mail messages. **NOTE:** The local SMTP server may require that you use a valid user account on the server for this setting. See the server’s documentation.

E-mail recipients.

Path: Administration > Notification > E-mail > recipients

Identify up to four e-mail recipients.

Setting	Description
To Address	The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page. To bypass the DNS lookup of the mail server's IP address, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly. **NOTE:** The recipient's pager must be able to use text-based messaging.
SMTP Server	Select one of the following methods for routing e-mail: • **Local**: Through the Modular PDU's SMTP server. This setting (recommended) ensures that the e-mail is sent before the Modular PDU's 20-second time-out, and, if necessary, is retried several times. Also do one of the following: • Enable forwarding at the Modular PDU's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Check with the administrator of your SMTP server before changing its configuration to allow forwarding. • Set up a special e-mail account for the Modular PDU to forward e-mail to an external mail account. • **Recipient**: Directly to the recipient's SMTP server. With this setting, the Modular PDU tries to send the e-mail only once. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent. When the recipient uses the Modular PDU's SMTP server, this setting has no effect.
E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.
Format	The long format contains Name, Location, Contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.

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

SNMP traps

Trap Receivers.

Path: Administration > Notification > SNMP Traps > trap receivers

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

- To open the page for configuring a new trap receiver, click **Add Trap Receiver**.
- To modify or delete a trap receiver, first click its IP address or host name to access its settings. (If you delete a trap receiver, all notification settings configured under Event Actions for the deleted trap receiver are set to their default values.)
- To specify the trap type for a trap receiver, select the SNMPv1 radio button.

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.

SNMP Trap Test

Path: Administration > Notification > SNMP Traps > test

Last Test Result. The result of the most recent SNMP trap test. A successful SNMP trap test verifies only that a trap was sent; it does not verify that the trap was received by the selected trap receiver. A trap test succeeds if all of the following are true:

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

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

Syslog

Path: Logs > Syslog > *options*

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

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

Identifying Syslog Servers.

Path: Logs > Syslog > servers

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

Syslog Settings.

Path: Logs > Syslog > settings

Setting	Definition
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the Modular PDU's Syslog messages (**User**, by default). **NOTE: User** best defines the Syslog messages sent by the Modular PDU. **Do not** change this selection unless advised to do so by the Syslog network or system administrator.
Severity Mapping	Maps each severity level of Modular PDU or Environment events to available Syslog priorities. You should not need to change the mappings. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the four **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info**

Syslog Test and Format example.

Path: Logs > Syslog > test

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

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

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

Queries (SNMP GETs)

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

Administration: General Options

Identification

Path: Administration > General > Identification

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

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

Set the Date and Time

Method

Path: Administration > General > Date & Time > mode

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

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

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

Daylight saving

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

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

When customizing Daylight Saving Time (DST):

- If the local DST always starts or ends on the fourth occurrence of a specific weekday of a month (e.g, the fourth Sunday), choose **Fourth/Last**. If a fifth Sunday occurs in that month in a subsequent year, the time setting still changes on the fourth Sunday.
- If the local DST always starts or ends on the last occurrence of a specific weekday of a month, whether it is the fourth or the fifth occurrence, choose **Fifth/Last**.

Format

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

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

Use an .ini File

Path: Administration > General > User Config File

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

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

To retrieve and customize the file of a configured Modular PDU, see “Export Configuration Settings” on page 47.

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

Temperature Units

Path: Administration > General > Unit Preference

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

Reset the Interface

Path: Administration > General > Reset/Reboot

Action	Definition
Reboot Management Interface	Restarts the interface of the Modular PDU.
Reset All[1]	Select **Exclude TCP/IP** to reset all values except TCP/IP; clear **Exclude TCP/IP** to reset all configuration values.
Reset Only[1]	**TCP/IP settings**: Set TCP/IP Configuration to **DHCP & BOOTP**, its default setting, requiring that the Modular PDU receive its TCP/IP settings from a DHCP or BOOTP server. See ""TCP/IP and Communication Settings" on page 23".
	Event configuration: Reset all changes to event configuration, by event and by group, to their default settings.
1. Resetting may take up to a minute.	

Configuring Links

Path: Administration > General > Quick Links

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

By default, these links access the following Web pages:

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

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

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

About the Modular PDU

Path: Administration > General > About

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

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

Management Uptime is the length 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 Modular PDUs. You can use the Wizard in either of the following ways:

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

System requirements

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

Installation

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

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

To install the Wizard from a downloaded executable file:

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

Use the Wizard

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

Launch the Wizard

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

Configure the basic TCP/IP settings remotely

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

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

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

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

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

Configure or reconfigure the TCP/IP settings locally

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

Export Configuration Settings

Retrieve and Export the .ini File

Summary of the procedure

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

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

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

Contents of the .ini file

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

- *section headings* and *keywords* (only those supported for the device from which you retrieve the file)*:* Section headings are category names enclosed in brackets ([ ]). Keywords, under each section heading, are labels describing specific Modular PDU settings. Each keyword is followed by an equals sign and a value (either the default or a configured value).
- The `override` keyword: With its default value, this keyword prevents the exporting of one or more keywords and their device-specific values, e.g., in the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the Modular PDU) blocks the exporting of values for the `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.

Detailed procedures

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

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

   ```
   ftp> open ip_address
   ```

   b. Log on using the Administrator user name and password.

   c. Retrieve the config.ini file containing the Modular PDU's settings:

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

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

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

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

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   - Enclose in quotation marks any values that contain leading or trailing spaces or are already enclosed in quotation marks.
   - To export scheduled events, configure the values directly in the .ini file.
   - To export a system time with the greatest accuracy, if the receiving Modular PDUs can access a Network Time Protocol server, configure `enabled` for `NTPEnable`:

     ```
     NTPEnable=enabled
     ```

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

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

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

     ```
     ftp> open ip_address
     ```

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

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

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

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

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

The Upload Event and Error Messages

The event and its error messages

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

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

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

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

Messages in config.ini

A device associated with the Modular PDU from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the device is not present or, for another reason, is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values.

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

Errors generated by overridden values

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

See “Contents of the .ini file” on page 47 for information about which values are overridden.

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

Related Topics

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

See “APC Device IP Configuration Wizard” on page 44.

File Transfers

Upgrading Firmware

Benefits of upgrading firmware

When you upgrade the firmware on the Modular PDU:

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

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

Firmware files (Modular PDU)

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

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

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

- `apc`: Indicates that this is an APC file.
- ***`hardware-version`*****:** `hw0`*`x`* identifies the version of the hardware on which you can use this binary file.
- ***`type`*****:** Identifies whether the file is for the APC Operating System (AOS) or the application module for the Modular PDU.
- ***`version`*****:** The version number of the file.
- `bin`: Indicates that this is a binary file.

Obtain the latest firmware version

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

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

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

To extract the firmware files:

1. Run the tool.
2. At the prompts, click **Next>**, and then specify the directory location to which the files will be extracted.
3. When the **Extraction Complete** message displays, close the dialog box.

File Transfer Methods

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

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

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

Use FTP or SCP to upgrade one Modular PDU

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

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

To transfer the files:

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

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

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

   - `apc_hw03_aos_xxx.bin`
   - `apc_hw03_application_xxx.bin`

2. Open an FTP client session:

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

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

   – For Windows FTP clients, separate a non-default port number from the IP address by a space. For example:

   ```
   ftp> open 150.250.6.10 21000
   ```

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

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

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

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

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

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the Modular PDU. The following example uses *xxx* to represent the version number of the AOS module:

   ```
   scp apc_hw03_aos_xxx.bin apc@158.205.6.185:apc_hw03_aos_xxx.bin
   ```

3. Use a similar SCP command line, with the name of the application module, to transfer the second firmware module to the Modular PDU.

How to upgrade multiple Modular PDUs

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

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

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

Use XMODEM to upgrade one Modular PDU

To upgrade the firmware for one Modular PDU that is not on the network, you must extract the firmware files from the firmware upgrade tool (see “To extract the firmware files:” on page 51).

To transfer the files:

1. Obtain the individual firmware modules (the AOS module and the application module) from **www.apc.com/tools/download**.
2. Select a serial port at the local computer and disable any service that uses the port.
3. Connect the provided configuration cable to the selected port and to the serial port at the Modular PDU.
4. Run a terminal program such as HyperTerminal, and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
5. Press ENTER to display the **User Name** prompt.
6. Enter the Administrator user name and password (**apc** by default for both).
7. From the **command line interface** menu, select **System**, then **Tools**, then **File Transfer**, then **XMODEM**; and type `Yes` at the prompt to continue.
8. Select a baud rate, change the terminal program’s baud rate to match your selection, and press ENTER. A higher baud rate causes faster upgrades.
9. From the terminal program’s menu, select the binary AOS file to transfer using XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600. The Modular PDU automatically restarts.
10. Repeat step 4 through step 9 to install the application module. In step 9, use the application module file name, not the AOS module file name.
11. For information about the format used for firmware modules, see “To extract the firmware files:” on page 51.

Verifying Upgrades and Updates

Verify the success or failure of the transfer

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

Last Transfer Result codes

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

Verify the version numbers of installed firmware

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

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.