Web/SNMP Management SmartSlot Card

AP9606

User's Guide

Thank You!

Thank you for selecting the APC Web/SNMP Management SmartSlot Card. It has been designed for many years of reliable, maintenance-free service. APC is dedicated to the development of high-performance electrical power conversion and control products. We hope that you will find this product a valuable, convenient addition to your system.

Please read this manual! It provides important configuration and operating instructions that will help you get the most from your Management Card. For detailed information on installation and set-up, see the *Web/SNMP Management SmartSlot Card Installation and Quick Start Manual* provided in printed format, and in PDF format on the Web/SNMP Management Card *utility* CD (.*doc**Insguide.pdf*).

Contents

Continued on next page

Contents

Continued on next page

Contents

Continued on next page

Contents

Continued on next page

Contents

Introduction

Product Description

Functionality

American Power Conversion's Web/SNMP Management SmartSlot Card (APC part number AP9606) is a web-based UPS Management product that uses multiple, open standards such as Telnet, HTTP, and SNMP to provide full management of UPS systems. Through the Web/SNMP Management SmartSlot Card, which is referred to as the Management Card in this guide, you can monitor and configure your APC UPS systems to shut down and reboot your computer systems.

The Management Card can be installed into the following APC devices:

- UPS systems with card slots: Smart-UPS®, Matrix-UPS®, Symmetra® *Power Array*™, and Silcon™ DP300E series UPS (with the use of a SmartSlot Expansion Triple Chassis)
- SmartSlot Expansion Chassis (AP9600)
- SmartSlot Expansion Triple Chassis (AP9604, AP9604R, or AP9604SR)

Note: In addition to connecting the UPS to an Ethernet network, the Management Card is used to manage MasterSwitch II and MasterSwitch *plus* power distribution units, and the standalone Environmental Monitoring Unit. In order to provide such a range of support to specific devices, the Management Card uses different firmware application layers to control each device. For more information on how a Management Card is used with the MasterSwitch devices and the Environmental Monitoring Unit, see the documentation for those products.

Continued on next page

Introduction

Product Description *continued*

Management Card versions

The Management Card (v3.0.0) has firmware that provides an APC operating system (AOS) layer (*aos300.bin*), and one of three available application layers. Which application firmware a Management Card uses depends on the UPS it supports.

- Symmetra *Power Array* (*sy300.bin*)
- Smart-UPS and Matrix-UPS (*sumx300.bin*)
- Silcon DP300E series UPS (*dp3e300.bin*)

Note: For information about how to download firmware, or for information about how to use the APC Management Card Wizard to configure multiple Management Cards, see the *Management Card Addendum*, provided in PDF format on the APC Web/SNMP Management Card *utility* CD (.*doc**Addendum.pdf*). For information about the MasterSwitch devices, see their product documentation.

Initial set-up

You must define three TCP/IP settings for the Management Card before it can operate on the network.

- IP address of the Management Card
- Subnet mask
- IP address of the default gateway

For instructions about how to configure the TCP/IP settings, see the *Web/SNMP Management SmartSlot Card Installation and Quick Start Manual*, provided in printed form, and in PDF on the APC Web/SNMP Management Card *utility* CD (.*doc**Insguide.pdf*).

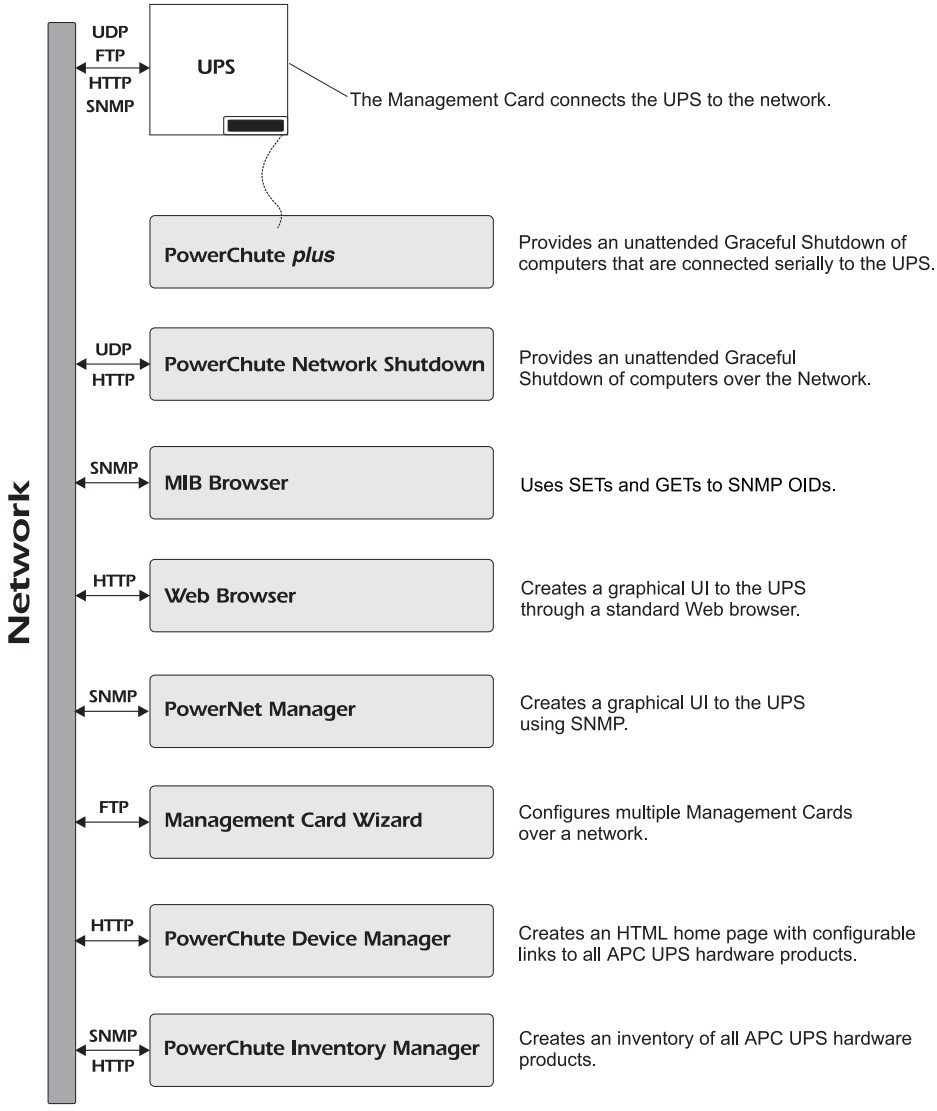
Continued on next page

Introduction

Product Description *continued*

Network management features

The figure below identifies and describes the network management applications that can work with a UPS that connects to the network through a Management Card.



Introduction

Internal Management Features

Overview

The Management Card has two internal interfaces, the Control Console and the Web interface, which provide menus with options that allow you to manage the UPS, an Environmental Monitoring SmartSlot Card, and the Management Card. The Management Card's SNMP interface allows you to use an SNMP browser with the APC MIB (PowerNet MIB) to manage the UPS and an Environmental Monitoring SmartSlot Card.

For more information about the Management Card's internal user interfaces, see **Control Console on page 14** and **Web Interface on page 20**; for more information about how to use the APC MIB with an SNMP browser, see the *PowerNet MIB Reference Guide* which is provided on the APC Web/SNMP Management Card *utility* CD (.*doc**Mibguide.pdf*)

Login control

Only one user at a time can log into the Management Card to use its internal user interface features. The priority for access, from highest to lowest, is as follows:

- Local access to the Control Console from a computer with a direct serial connection to the Management Card
- Telnet access to the Control Console from a remote computer
- Web access

Note: For information about how SNMP access to the Management Card is controlled, see **SNMP on page 29**.

Types of user accounts

The Management Card has two levels of access (Administrator and Device Manager), both of which are protected by **Password** and **User Name** requirements.

- An Administrator can use all of the management menus available in the Control Console and the Web interface. The Administrator's default **Password** and **User Name** are both **apc**.
- A Device Manager can access only the **Log** option in the **Events** menu and use the **UPS** and **Environment** menus. The Device Manager's default **Password** is **device**, and the default **User Name** is **apc**.

Note: The Management Card also uses a **User Name** and **Password** to protect FTP access to the Management Card, as described in **FTP Client on page 28**.

For information about how to set Administrator and Device Manager **Password** and **User Name** settings, see **User Manager on page 31**.

Introduction

Front Panel

Features

The front panel has the following features:

- Reset button
- 10Base-T network cable connector
- Link-RX/TX LED
- Status LED

Reset Button. Allows you to reset the Management Card while power is on.

10Base-T Port. Used to connect the Management Card to the Ethernet network.

Link-RX/TX LED. Indicates the network status.

Condition	Description
Off	The device which connects the Management Card to the network is turned off or it is not operating correctly.
Flashing	The Management Card is receiving data packets from the network.

Status LED. Indicates the status of the Management Card.

Condition	Description
Off	The Management Card has no power.
Solid Green	The Management Card has valid network settings.
Flashing Green	The Management Card does not have valid TCP/IP settings.[1]
Solid Red	A hardware failure has been detected in the Management Card. Contact APC Technical Support as described in **APC Worldwide Technical Support on page 74**.
Flashing Red	The Management Card is making BOOTP requests. If you do not use a BOOTP server, you need to configure the Management Card's TCP/IP settings.[1]

1 For information about how to configure the three TCP/IP settings that the Management Card needs to operate on the network, see the *Web/SNMP Management SmartSlot Card Installation and Quick Start Manual* provided in printed format, and in PDF format on the APC Web/SNMP Management Card *utility* CD (.*doc**Insguide.pdf*).

Introduction

Watchdog Features

Overview

The Management Card is designed to recover from unanticipated inputs. Through the use of internal, system-wide watchdog mechanisms, the Management Card can detect most internal problems and reboot itself to recover.

Network interface watchdog mechanism

The Management Card implements numerous internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For Example, if within a seven-minute period the Management Card does not receive any network traffic (either direct, such as SNMP, or broadcast, such as an Address Resolution Protocol [ARP] request) it assumes that there is a problem with its network interface and reboots itself.

The role of the Default Gateway in resetting the network timer

Most networks will have some level of broadcast traffic which will be received by the Management Card and reset the seven-minute timer to zero. But since it is not desirable for the Management Card to reboot just because the network is quiet, the Management Card will attempt to contact the Default Gateway once every five minutes. If the gateway is present, it will respond to the Management Card and the seven-minute timer will be reset to zero.

If your application does not require a gateway or does not have one, specify the IP address of a computer on the same subnet which is running on the network most of the time. This will have the same effect as configuring a gateway.

Control Console

Introduction

Overview

The Control Console provides a set of menus that you can use to manage the Management Card, its UPS, and an Environmental Monitoring SmartSlot Card, from a local computer or over the network.

Menu structure

The Control Console menus list options by number and name. To use an option, type the option's number and press ENTER, then follow any on-screen instructions.

Menus that allow you to change a setting have an **Accept Changes** option which you must use to save the changes you made.

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

Do This	Action
Type ? ENTER	Accesses brief menu option descriptions (if the menu has help available).
Press ENTER	Refreshes the menu.
Press ESC	Returns to the previous menu.
Press CTRL-C	Returns to the main (Control Console) menu.
Press CTRL-D	Toggles between the UPS and Environmental Monitoring SmartSlot Card menus.
Press CTRL-L	Accesses the event log. **Note:** For information about the event log, see **Events Menu on page 50**.

Control Console

How to Log In

Overview

You can use either a local (serial) connection, or a remote (Telnet) connection with a computer on the Management Card's subnet to access the Control Console. Use case-sensitive **User Name** and **Password** entries to log in (by default, **apc** and **apc**, for an Administrator, or **device** and **apc**, for a Device Manager). For information about the screen that appears when you log into the Control Console, see **Main Screen on page 17**.

Local (serial) access

You can use a computer that connects to the Management Card through the serial port at the UPS or chassis to access the Control Console.

1. Select a serial port at the computer to be used for a terminal-emulation connection with the Management Card.
2. Disable any service that currently uses the selected serial port, such as PowerChute® *plus* or UNIX® Respond.
3. Disconnect any cable from the selected serial port and connect the smart-signaling cable (940-0024) that came with the Management Card to the selected serial port and to the serial port on the UPS or chassis.

   Note: If the computer uses smart-signaling PowerChute *plus*, omit step 3: A smart-signaling cable (APC part number 940-0024 or 940-1524) is already installed.
4. Run a terminal program, such as HyperTerminal.
5. Configure the serial port for 2400 bps, 8 data bits, no parity, 1 stop bit, and no flow control, then save the changes.
6. Press ENTER to display the **User Name** prompt (you may need to press ENTER two or three times).
7. Enter your **User Name** and **Password**.

   Note: If you cannot remember your **User Name** or **Password**, see **How to Recover from a Lost Password on page 16**.

Remote (Telnet) access

You can use Telnet to log into the Control Console from any computer on the same subnet as the Management Card.

1. At a command prompt, type `telnet` and the Management Card's System IP address, and then press ENTER. For example:
   `telnet 159.215.12.114`
2. Enter your **User Name** and **Password**.

Control Console

How to Recover from a Lost Password

Overview

If the **User Name** or **Password** becomes unknown, you can use a local computer to restore access to a Management Card that uses the APC AOS module, version 3.0 (or later). The latest AOS version is available at the APC web site (www.apcc.com).

Recovery procedure

To recover from a lost **Password** or **User Name**, do the following:

1. Select a serial port at the computer to be used for a terminal-emulation connection with the Management Card.
2. Disable any service that currently uses the selected serial port, such as PowerChute *plus* or UNIX Respond.
3. Disconnect any cable from the selected serial port and connect the smart-signaling cable (940-0024) that came with the Management Card to the selected serial port and to the serial port on the UPS or chassis.

   Note: If the computer uses smart-signaling PowerChute *plus*, omit **Step 3**: A smart-signaling cable (940-0024 or 940-1524) is already installed.
4. Run a terminal program (such as HyperTerminal).
5. Configure the serial port for 2400 bps, 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.
6. Press ENTER to display the **User Name** prompt (you may need to press ENTER two or three times).
7. Press the reset button on the Management Card.
8. Press ENTER to redisplay the **User Name** prompt.
9. Use **apc** for both the **User Name** and **Password** to log in.

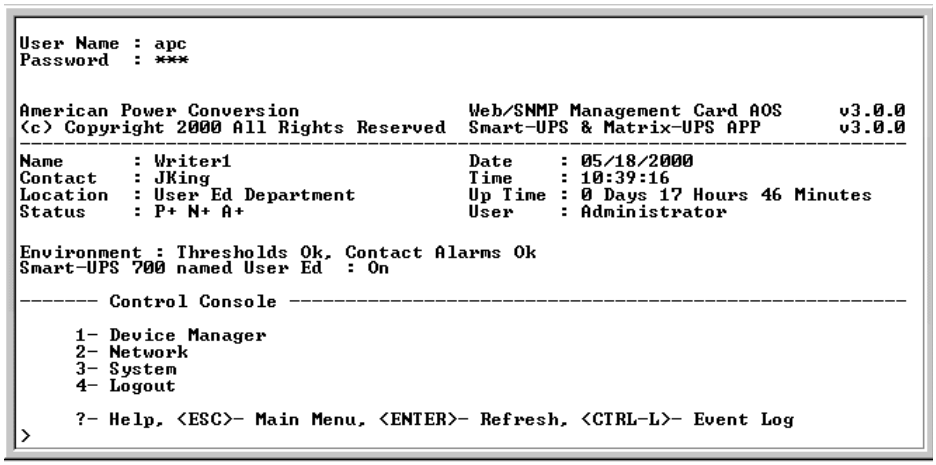
   Note: If you take longer than 30 seconds to log in, you will need to repeat **Step 6** through **Step 8**.
10. Select **System** from the **Control Console** menu.
11. Select **User Manager** from the **System** menu.
12. Select **Administrator** from the **User Manager** menu, and follow the on-screen instructions to change the **User Name** and **Password** settings to the new values.
13. Press CTRL-C to exit to the **Control Console** menu.
14. Log out to save the changes.
15. If necessary, reconnect any cable disconnected from the computer's serial port in **Step 3**.
16. Restart any service disabled in **Step 2**.

Control Console

Main Screen

Example main screen

The following is an example of the screen that appears when you log into the Control Console.



Status and identification information

In addition to a menu (described in **Control Console Menu on page 19**), the main screen provides the following information:

- Two fields identify the APC operating system (AOS) and application (APP) firmware versions. A Management Card can use Smart-UPS/Matrix-UPS, Symmetra *Power Array*, or Silcon DP300E versions of the APP firmware. The example above shows that this Management Card uses the application firmware for the Smart-UPS/Matrix-UPS.

  ```
  Web/SNMP Management Card AOS    v3.0.0
  Smart-UPS & Matrix-UPS APP      v3.0.0
  ```

- Three fields identify the system **Name**, **Contact**, and **Location** values.

  ```
  Name                            : Writer1
  Contact                         : JKing
  Location                        : User Ed Department
  ```

  Note: For information about how to set the **Name**, **Contact**, and **Location** values, see **System Menu on page 30**.

Continued on next page

Control Console

Main Screen *continued*

Status and identification information, *continued*

- Two fields identify when you logged in, by **Date** and **Time**.

  ```
  Date      : 05/10/2000
  Time      : 10:39:16
  ```

  Note: For information about how to change the **Date** and **Time** values, see **System Menu on page 30**.

- A **User** field identifies whether you logged in as an **Administrator** or **Device Manager**.

  ```
  User      : Administrator
  ```

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

  ```
  Up Time   : 0 days 17 hours 46 Minutes
  ```

- A **Status** field reports the Management Card status.

  ```
  Status    : P+ N+ A+
  ```

  The possible status symbols and there meanings are identified and described in the following table:

P+	Indicates that the APC operating system (AOS) is functioning properly.
N+	Indicates that the network is functioning properly.
A+	Indicates that the network is functioning properly.
A-	Indicates that the application has a bad checksum
A?	Indicates that the application is initializing.
A!	Indicates that the application is not compatible with the AOS.

  Note: If you can access the Control Console, the AOS and network will report that the status is operating properly (`P+` and `N+`).

- A **UPS model and name** field reports the status of the UPS.

  ```
  Smart-UPS 700 named User Ed: On
  ```

  Note: For more information about the UPS status, see **UPS Status Options on page 35**.

- An **Environment** field reports the status of the Environmental Monitoring SmartSlot Card.

  ```
  Environment: Thresholds Ok, Contact Alarms Ok
  ```

  Note: For more information about the Environmental Monitoring SmartSlot Card status, see **Environment Menu Options on page 49**.

Control Console

Control Console Menu

Overview

The Control Console menu has four options, three of which provide access to the Control Console's management features:

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

Note: When you log in as Device Manager, you can access only the event log and the Device Manager menus.

Device Manager option

This option accesses the Device Manager menu. You use this menu's options to select the device to manage:

```
1- Environment
2- Smart-UPS 700
```

Note: The first **Environment** option is only present when an Environmental Monitoring SmartSlot Card is present.

For information about the menus used to manage a UPS and Environmental Monitoring SmartSlot Card, see **Device Manager Menus on page 34**.

Network option

To do any of the following tasks, see **Network Menu on page 26**:

- Configure the Management Card's TCP/IP settings.
- Use the Ping utility.
- Define settings that affect the use of TFTP, FTP, Telnet, the Web interface, SNMP, and Email.

System option

To do any of the following tasks, see **System Menu on page 30**:

- Control Administrator and Device Manager access.
- Define the system **Name**, **Contact**, and **Location** values.
- Set the **Date** and **Time** used by the Management Card.
- Use file transfer protocols.
- Reboot the Management Card.
- Reset the Control Console settings to default settings.
- Access system information about the Management Card.

Web Interface

Introduction

Overview

Unless the Web interface is disabled by the Web menu's **Access** option, you can use a supported Web browser to manage a UPS, an Environmental Monitoring SmartSlot Card, and the Management Card.

Web menu options

Two Web menu options affect access to the Web interface.

- **Access**: Enables or disables the Web interface.
- **Port:** Defines the Web-server port (**80**, by default) used for the Web interface.

For more information about the Access and Port options, see **FTP Server, Telnet, and Web on page 28**.

Supported Web browsers

You can use Microsoft® Internet Explorer (IE) 3.0.2 (or later), or Netscape® Navigator 3.0 (or later).

Some Web interface features (data verification, APC Interactive Assistant, and MD5 authentication) require that you enable the following for your Web browser:

- JavaScript
- Java
- Cookies

Note: For more information, see **MD5 authentication (Web interface) on page 68**.

The Management Card 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 Management Card.
- Configure the proxy server not to proxy the specific IP address of the Management Card.

Web Interface

How to Log In

Overview

You can use a Management Card's DNS name or System IP address for the URL address of the Web interface. Use your case-sensitive **User Name** and **Password** settings to log in (by default, **apc** and **apc**, for an Administrator, or **device** and **apc**, for a Device Manager).

For information about the Web page that appears when you log into the Web interface, see **Status Summary Page on page 22**.

URL address formats

Type the Management Card's DNS name or IP address in the Web browser's URL address field and press ENTER. Except as noted below, http:// is automatically added by the browser.

- For a DNS name of `Web1`, the entry would look like this:

  `http://Web1`

  Note: The Management Card must have a DNS name before it can use E-mail for event notifications. For more information, see **Email on page 56**.
- For a System IP address of 159.215.12.114, when the Management Card uses the default port (80) at the Web server, the entry would look like this:

  `http://159.215.12.114`
- For a System IP address of 159.215.12.114, when the Management Card uses a non-default port (5000, in this example) at the Web server, the entry would look like this:

  `http://159.215.12.114:5000`

  Note: For Internet Explorer, you must type in `http://` as part of the address when any port other than 80 is used.

Error pages. Error pages can appear when you attempt to log into the Management Card's Web interface.

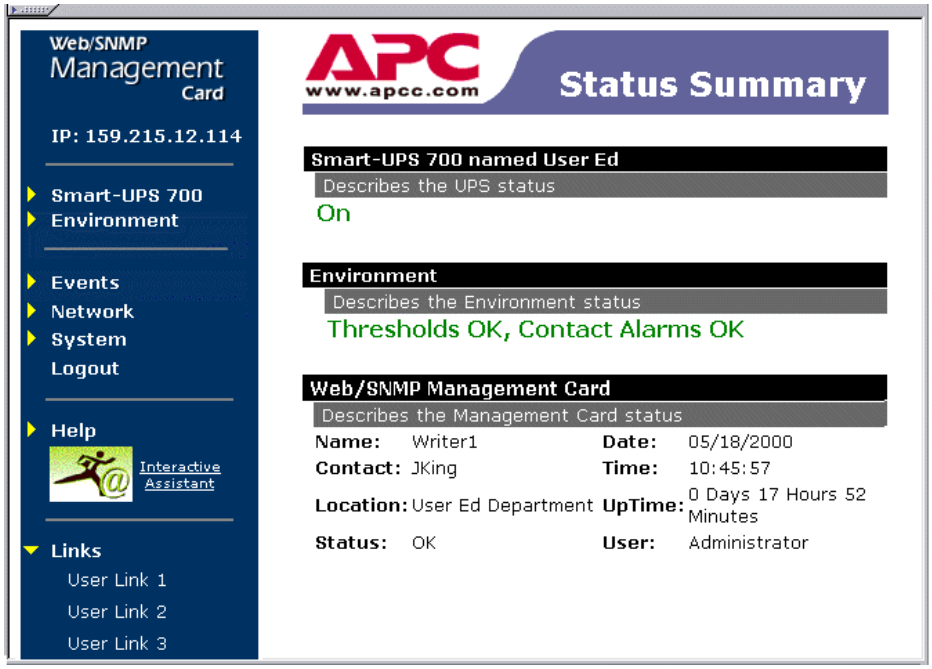
Error Page	Description
"You are not authorized to view this page" (Internet Explorer)	Someone is logged into the Web interface or Control Console.
"No Response" (Netscape)	Access may be disabled, or the Management Card may use a non-default Web-server port, and you did not include the correct port number in the address.[1]
"This page cannot be displayed" (Internet Explorer)	Access may be disabled, or the the Management Card may use a non-default Web-server port, and you did not include the correct port number in the address, or you did not type http:// as part of the address. **Note:** For more information about non-default Web-server ports, see **FTP Server, Telnet, and Web on page 28**.

Web Interface

Status Summary Page

Example Web page

The following is an example of the “Status Summary” page that appears when you log into the Web interface.



Status and identification information

In addition to the menu frame elements described in **Menu Frame on page 23**, the “Status Summary” page provides the following information:

- A **UPS model and name** section reports the UPS status.
- An **Environment** section reports the status of the Environmental Monitoring SmartSlot Card.
- **Date** and **Time** fields identify when you logged in.
- A **User** field identifies whether you logged in as an **Administrator** or **Device Manager**.
- An **Up Time** field reports how long the Management Card has been running since it was last turned on or reset.
- A **Status** field reports the status of the Management Card.

  Note: If the Status field does not report **Ok**, contact APC Technical Support as described in **APC Worldwide Technical Support on page 74**.

For information about how to set the Name, Contact, and Location values, or to modify the Date and Time settings, see **System Menu on page 30**; for information about UPS status, see **UPS Status Options on page 35**; for information about the Environmental Monitoring SmartSlot Card status, see **Environment Menu Options on page 49**.

Web Interface

Menu Frame

Overview

When you log into the Web interface as an Administrator, the navigation bar (left frame) includes the following elements:

- The Management Card's IP address
- An **Events** menu
- A **UPS** menu which uses the UPS model for its name (Smart-UPS 700, in the example on **page 22**)
- An **Environment** menu
- A **Network** menu
- A **System** menu
- A **Logout** option
- A **Help** menu
- Logo and text links to **Interactive Assistant**
- Three user-definable **User Links**

Note: The **Environment** menu appears only when an Environmental Monitoring SmartSlot Card is used; the **Network** and **System** menus appear only when you log in as an Administrator.

Events menu

This menu's options allow you to do the following:

- Access the event log.
- Configure the actions that will occur, based on an event's severity level.
- Configure the SNMP Trap Receiver settings for sending event-based traps.
- Define who will receive Email notifications of events.

For information about how to use this menu, see **Events Menu on page 50**.

UPS and Environment menus

For information about how to use the **UPS** and **Environment** menus to manage a UPS or an Environmental Monitoring SmartSlot Card, see **Device Manager Menus on page 34**.

Continued on next page

Web Interface

Menu Frame continued

Network menu

This menu's options allow you to do the following:

- Configure new TCP/IP settings for the Management Card.
- Define settings that affect the use of TFTP, FTP, Telnet, SNMP, and Email.

Note: For information about how the **Network** menu's Web options affect access to the Web interface, see **Web menu options on page 20**.

For information about how to use this menu, see **Network Menu on page 26**.

System menu

This menu's options allow you to do the following:

- Control Administrator and Device Manager access.
- Define the System Name, Contact, and Location values.
- Set the Date and Time used by the Management Card.
- Use file transfer protocols.
- Reboot the Management Card
- Reset the Control Console settings to default settings.

Note: For information about how to configure the Menu Frame's user links, as well as the links used by the APC logo and the Interactive Assistance logo and text, see **User-definable links on page 25**.

For information about how to use this menu, see **System Menu on page 30**.

Help menu

When you click **Help**, the **Contents** option is automatically selected, and the online help appears in your browser. Use the question mark (**?**) that appears in a Web page to link to the online help for that page.

The **Help** menu has two other links:

- **Interactive Assistant** links to the APC Interactive Assistant Web page. For more information, see **Interactive Assistant on this page**.
- **About System** displays information about the Management Card. For more information, see **About System on page 33**.

Continued on next page

Web Interface

Menu Frame continued

Interactive Assistant

APC Interactive Assistant brings APC customer service to the Web. When you select **Interactive Assistant**, the Management Card transmits information about itself, and its UPS, to the APC Interactive Assistant server. The server informs you if the UPS has a bad battery. The “Interactive Assistant” Web page provides links to more information about the Management Card and the UPS, as well as links to relevant pages at the APC Web site.

User-definable links

The **Link** menu has three link options. By default, these links are labeled **User Link 1** through **User Link 3**, and all three link to APC’s home page.

Use the following procedure to redefine these links so that they point to other UPS devices or to the MasterSwitch devices and servers that are being powered by the UPS.

- Click on **Links** in the **System** menu.
- Define the new names.
- Define the new URL addresses that you want the links to access.
- Click **Apply** to save your changes.

Note: This “Links” page also has fields you can use to modify the URL address used by the APC logo and by the Interactive Assistant logo and text links.

Network Menu

Introduction

Overview

The **Network** menu provides access to the options you use to configure the Management Card's network settings.

Note: Only an Administrator has access to the **System** menu.

Menu options

For information about the settings available for the **Network** menu options, see the following descriptions:

- **TCP/IP on page 27**
- **DNS on page 27**
- **Ping utility on page 27**

  Note: The **Ping** utility option is available only in the Control Console.
- **TFTP Client on page 28**
- **FTP Client on page 28**
- **FTP Server, Telnet, and Web on page 28**
- **SNMP on page 29**
- **Email on page 56**

Network Menu

Option Settings

TCP/IP

This option allows you to enable or disable BOOTP, and when BOOTP is disabled, define the three TCP/IP settings that the Management Card needs to operate on the network.

- The Management Card's System IP address
- The subnet mask value
- The IP address of the Default Gateway

Note: For information about the watchdog role the Default Gateway plays, see **The role of the Default Gateway in resetting the network timer on page 13**; for information about how to configure the initial TCP/IP settings when you install the Management Card, see the *Web/SNMP Management SmartSlot Card Installation and Quick Start Manual*, provided in printed form and on the APC Web/SNMP Management Card *utility* CD (*.\doc\insguide.pdf*).

When **BOOTP** is enabled (by default), you can affect only the **BOOTP** setting: A BOOTP server provides the Management Card with its TCP/IP settings whenever the Management Card is turned on, reset, or rebooted.

Note: For information about how to use BOOTP, see the *Management Card Addendum*, provided in PDF format on the APC Web/SNMP Management Card *utility* CD (*./doc/adendum.pdf*).

DNS

Use this option (which is combined with TCP/IP, described above, in the Web interface) to define the IP address of the Domain Name Server (DNS). You must define the DNS address to use the Management Card's Email feature.

Note: For information about how to use the Email feature, see **Email on page 56**.

Ping utility

This option (which is available only in the Control Console) allows you to use Ping, a network utility, to test the Management Card's network connection.

By default, the Default Gateway IP address (see **TCP/IP** above) is used. However, you can use the IP address of any device known to be running on the network.

Continued on next page

Network Menu

Option Settings *continued*

TFTP Client

Use this option to define the IP address of the TFTP server used to download configuration files (**0.0.0.0**, by default).

Note: For information about how to use TFTP to download configuration files, see the *Management Card Addendum* on the APC Web/SNMP Management Card *utility* CD **(***./doc/addendum.pdf***)**.

FTP Client

Use this option to define the IP address of the FTP server used to download configuration files (**0.0.0.0**, by default), as well as the case-sensitive **User Name** and **Password** settings (**apc** is the default for both) used to protect FTP access.

Note: For information about how to use FTP to download configuration files, see the *Management Card Addendum* on the APC Web/SNMP Management Card *utility* CD (*./doc/addendum.pdf*); for information about how to use FTP to access a text-version of the Management Card's event log, see **FTP on page 52**.

FTP Server, Telnet, and Web

Each of these options has a setting which enables (by default) or disables Access, and a **Port** setting that identifies the TCP/IP port used for communications with the Management Card. The default **Port** settings are **21** (FTP), **23** (Telnet), and **80** (Web interface).

You change a **Port** setting to any port number between **5000** and **65535** to enhance the protection provided by **User Name** and **Password** settings. However, if you do, you must use a colon (:) to add the non-default **Port** number to the IP address used. The selected port number must be unique. The following examples show what the FTP, Telnet, and Web interface commands could look like when the **Port** numbers for all three interfaces have been changed from their default settings at a Management Card with a System IP address of 159.215.12.114:

```
ftp 159.215.12.114:5000
telnet 159.215.12.114:59401
http://159.215.12.114:65002
```

Continued on next page

Network Menu

Option Settings *continued*

SNMP

An **Access** option (the **Settings** option in the Control Console) enables (by default) or disables SNMP. When SNMP is enabled, the **Access Control** settings allow you to control how each of the four available SNMP channels is used.

Note: For information about how to define up to four NMSs which will server as trap receivers, see **Trap receivers on page 55**; for more information about how to use SNMP to manage a UPS or an Environmental Monitoring SmartSlot Card, see the *PowerNet MIB Reference Guide* on the APC Web/SNMP Management Card *utility* CD (.*doc**mibguide.pdf*).

Setting	Definition	
Community Name	This setting defines the password (maximum of 15 characters) which an NMS that is defined by the **NMS IP** setting below uses to access the channel.	
NMS IP	Limits access to the NMS or NMSs specified by the format used for the IP address. For example: • **159.215.12.1** allows only the NMS with that specific IP address to have access. • **159.215.12.255** allows access for any NMS on the 159.215.12 segment. • **159.215.255.255** allows access for any NMS on the 159.215 segment. • **159.255.255.255** allows access for any NMS on the 159 segment. • **0.0.0.0** or **255.255.255.255** allows access for any NMS.	
Access Type	Selects how the NMS defined by the **NMS IP** setting can use the channel, when that NMS uses the correct **Community Name**.	
	Read	The NMS can use GETs at any time, but it can never use SETs.
	Write	The NMS can use GETs at any time, and can use SETs when no one is logged into either the Control Console or Web interface.
	Write+	The NMS can use GETs and SETs at any time.
	Disabled	The NMS cannot use GETs or SETs.

System Menu

Introduction

Overview

The **System** menu provides access to the options that you use to do the following tasks:

- Configure system identification, date and time settings, and Administrator and Device Manager access.
- Download configuration files.
- Reset or reboot the Management Card.
- Define the URL links available in the Web interface
- Access hardware and firmware information about the Management Card.

Note: Only an Administrator has access to the **System** menu.

Menu options

Two differences exist in the **System** menu as it appears in the Control Console and the Web interface:

- The **About System** option in the Control Console's **System** menu is located in the **Help** menu in the Web interface.
- The Web interface has a **Links** option you can use to configure its URL links.

For information about the settings available for the **System** menu options, see the following descriptions:

- **User Manager on page 31**
- **Identification on page 31**
- **Date & Time on page 32**
- **File Transfer on page 32**
- **Tools on page 32**
- **Links on page 33**
- **About System on page 33**

System Menu

Option Settings

User Manager

Use this option to define the access values shared by the Control Console and the Web interface, and the authentication used to access the Web interface.

Setting	Definition
Auto Logout	Defines (in minutes) how long someone logged into the Control Console or Web interface can be inactive before that user is automatically logged out (**3** minutes by default).
Authentication	The **Basic** setting (default) causes the Web Interface to use standard HTTP 1.1 login (base64-encoded passwords); **MD5** causes the Web Interface to use an MD5-based authentication login. **Note:** Cookies must be enabled at a browser before it can be used with MD5 authentication.
Administrator and **Device Manager User**	
User Name	Defines the case-sensitive name (maximum of 10 characters) used to log in (**apc**, by default, for **Administrator**, and **device**, by default, for **Device Manager User**).
Password	Defines the case-sensitive password (maximum of 10 characters) always used to log into the Control Console, but only used to log into the Web interface when **Basic** is selected for the **Authentication** setting (**apc** is the default for both **Password** settings).
Authentication Phrase	Defines the case-sensitive, 15-to-32 character phrase used to log into the Web interface when **MD5** is the **Authentication** setting (**admin user phrase**, is the default for **Administrator**; **device user phrase** is the default for Device Manager User).

Identification

Use this option to define the System **Name**, **Location**, and **Contact** values used by the Management Card's SNMP agent. The option's settings provide the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifications (OIDs).

For more information about the MIB-II OIDs, see the *PowerNet MIB Reference Guide* provided on the APC Web/SNMP Management Card *utility* CD (*./doc/mibguide.pdf*).

Continued on next page

System Menu

Option Settings *continued*

Date & Time

Use this option to change the **Date** (MM/DD/YYYY format) or **Time** (HH:MM:SS format) used by the Management Card.

File Transfer

The Web interface identifies the IP addresses for the remote TFTP and FTP servers, as well as the case-sensitive **User Name** and **Password** settings used for FTP (**apc**, is the default for both). To use TFTP and FTP for file transfers, do the following:

1. Define the file name in the **Filename** field, and click **Apply**.
2. Select **TFTP** or **FTP** from the **Initiate File Transfer Via** menu, and click **Apply**.

The Control Console allows you to use TFTP, FTP, and XMODEM.

1. Use the **Settings** option to define the file name.
2. Select **TFTP**, **FTP**, or **XMODEM** from the menu and follow the on-screen instructions.

For information about how to define the **TFTP** and **FTP** settings, see **Network Menu on page 26**; for more information about file transfers, see the *Management Card Addendum* provided on the APC Web/SNMP Management Card *utility* CD (*.\doc\Addendum.pdf*).

Tools

Use this option's drop-down menu to reboot the Management Card or to reset some or all of its configuration settings to their original, default values.

Menu Option	Definition
Reboot Card	Restarts the Management Card.
Reset Card to Defaults	Resets all configuration settings including the TCP/IP settings, and enables BOOTP. **Note:** The Management Card will not be able to operate on the network until its TCP/IP settings are redefined.
Reset Card to Defaults Except TCP/IP	Resets all configuration settings except the TCP/IP and BOOTP settings.

Continued on next page

System Menu

Option Settings *continued*

Links

Use this option, which is only available in the Web interface, to configure the three User Links, the URL address used by the APC logo, and the URL address used by the various Interactive Assistant links.

Setting	Definition
User Links	
Name	Defines the link name (up to 3) that appears on the menu frame.
URL	Defines the URL address used by each link (*http://www.apcc.com* is the default for all three user links).
APC Links	
URL for **APC Home Page**	Defines the link used by the APC logo that appears at the top of each Web page. By default, the APC logo accesses APC's home page (*http://www.apcc.com*).
URL for **APC Interactive Assistant**	Defines the link used by the Interactive Assistant logo and text links. By default, the Interactive Assistant links access the "APC Interactive Assistant" Web page.

About System

This option displays hardware, factory, application module, and APC OS information for the Management Card. It includes information such as the Management Card's serial number, hardware revision, and the date and time when the application and APC OS modules were loaded.

Note: **About System** is a **Help** menu option in the Web interface.

Device Manager Menus

Introduction

Overview

Two **Device Manager** menus appear in the Control Console and Web interface.

- A **UPS** menu, which uses the UPS model for its name, provides the options that you use to manage the UPS. For more information about this menu, see **UPS menu options** below.
- An **Environment** menu, which appears only when an Environmental Monitoring SmartSlot Card is present, provides options that you use to manage the Environmental Monitoring SmartSlot Card. For more information about this menu, see **Environment Menu Options on page 49**.

UPS menu options

The **UPS** menu options, and the information provided by those options, vary by UPS model.

The **UPS** menu in the Web interface includes a ***PowerChute*** option which allows you to use APC's PowerChute network shutdown utility. For more information about this ***PowerChute*** option, which is not available in the Control Console, see **UPS PowerChute network shutdown Option on page 48**.

For information about the **UPS** menu options available in the Control Console and Web Interface, see the following descriptions:

- **UPS Status Options on page 35**
- **UPS Diagnostics Options on page 40**
- **UPS Control Options on page 41**
- **UPS Configuration Options on page 43**
- **Module Status Option (Symmetra Power Array) on page 47**

  Note: A Silcon DP300E series UPS has no diagnostics options.

Device Manager Menus

UPS Status Options

Overview

The **Status** options provide access to the information described in the following sections:

- **Detailed UPS status on this page**
- **Input voltage on page 36**
- **Output voltage on page 37**
- **Fault tolerance (Symmetra Power Array) on page 38**
- **Battery on page 39**

Note: No description is provided for the self-explanatory **About UPS** status fields.

The **UPS** menu for a Symmetra *Power Array* also has the diagnostics and status options which are described in **Module Status Option (Symmetra Power Array) on page 47**.

Detailed UPS status

In the Web interface, UPS status information is displayed at the top of the page that appears when the **UPS** menu's **Status** option is selected. This UPS status includes information about what caused the most recent transfer to battery power at the UPS, as well as the internal temperature of the UPS.

Note: The detailed UPS status also appears on the Web interface's "Control" and "Diagnostics" Web pages.

In the Control Console, the following information is displayed above the **UPS** menu options:

- Reason for the last transfer to battery
- UPS internal temperature
- The voltage values described in **Input voltage on page 36**, **Output voltage on page 37**, and **Battery on page 39**.

The options **Detailed Status** (Smart-UPS or Matrix-UPS) and **Detailed UPS Information** (Symmetra *Power Array* or Silcon DP300E) provide access to the expanded UPS operational status and other status information. In addition, the Control Console's **UPS** menu for a Symmetra *Power Array* has a **Faults & Alarms** option which describes any faults or alarms reported as part of the UPS status.

Note: A Silcon DP300E series UPS reports a non-specific fault for about 50 different conditions, including transfer to Bypass mode. When a specific fault is reported, access the UPS Keyboard at the Silcon DP300E series UPS for details.

For information about the UPS events that can be reported as part of the UPS status, see **Management Card and Device Events on page 61**.

Continued on next page

UPS Status Options *continued*

Input voltage

All UPS models report the input voltage and frequency. A Silcon DP300E series UPS, which identifies the input voltage values for all three phases, also reports the current (amperage) provided by the input voltage.

Note: In the Control Console, use the **Detailed UPS Information** option to access the **Minimum** and **Maximum Input Voltage** status for a Symmetra *Power Array* or Silcon DP300E series UPS.

Status Field	Definition
Input Voltage	The AC voltage (VAC) being input to the UPS.
Input Frequency	The input voltage's frequency, in Hertz (Hz). **Note:** In the Control Console for Smart-UPS or Matrix-UPS, the **Operating Frequency** field reports the frequency value shared by the input and output voltages.
Maximum Line Voltage	The highest AC voltage input to the UPS during the previous minute of operation.
Minimum Line Voltage	The lowest AC voltage input to the UPS during the previous minute of operation.
Input Current (Silcon DP300E series UPS only)	How much current is being supplied by the input voltage.

Continued on next page

Output voltage

The output voltage status information displayed depends on the UPS model.

Smart-UPS/Matrix-UPS. Four status fields report on the output from a Smart-UPS or Matrix-UPS.

Note: In the Control Console, the output voltage fields for a Smart-UPS or Matrix-UPS are all displayed above the **UPS** menu.

Status Field	Definition
Output Voltage	How much AC voltage the UPS is providing to its attached equipment.
Output Frequency	The frequency used by the output voltage. **Note:** In the Control Console, an **Operating Frequency** field reports the frequency value that is shared by the input and output voltages.
Load Power	The load placed on the UPS by its attached equipment.
Load Current (Matrix-UPS only)	The current being supplied by the output voltage.

Symmetra *Power Array*. Five status fields report the Symmetra *Power Array* output values.

Note: In the Control Console, only the **Output Voltage** and **Output Watts** (as a single **Load Power** field) is reported in the status displayed above the **UPS** menu. Use the **Detailed UPS Information** option to access the other status fields for the output voltage.

Status Field	Definition
Output Voltage	How much AC voltage the UPS is providing to its attached equipment.
Output Frequency	The frequency used by the output voltage.
Output Current	The current supplied by the output voltage.
Output Watts	The load placed on each of the Power Modules by the attached equipment, expressed in Watts.
Output VA	The load placed on each of the Power Modules by the attached equipment, expressed as a percentage of the kVA available from the UPS.

Continued on next page

Output voltage, continued

Silcon DP300E. Five status fields report the output values for a Silcon DP300E series UPS.

Note: In the Control Console, use the **Detailed UPS Information** option to access the **Peak Output Current** status.

Status Field	Definition
Output Voltage	How much AC voltage the UPS is providing to its attached equipment for each phase.
Output Current	How much current the output voltage is providing for each phase.
Output Power	The load placed on each phase by the attached equipment, in total kVA.
Output Power Percentage	The load placed on each phase by the attached equipment, expressed as a percentage of the of the kVA available from the UPS.
Peak Output Current	The highest current output by each phase.

Fault tolerance (Symmetra Power Array)

Two status fields report the Symmetra *Power Array* fault tolerance.

Note: In the Control Console, you use the **Detailed UPS Information** option to access the fault tolerance status.

Status Field	Definition
Redundancy	The number of power modules which can fail or be removed without causing the Symmetra *Power Array* to generate a Minimum Redundancy Lost event.
Present KVA Capacity	The maximum load that the Symmetra *Power Array* can support.

Continued on next page

Device Manager Menus

UPS Status Options *continued*

Battery

The following table uses footnotes to indicate which fields are shared by which UPS models. Only one battery-related status field (**Runtime Remaining**) is shared by all UPS models.

Note: In the Control Console, use the **Detailed UPS Information** option to access the **Number of External Batteries**, **Number of Bad Batteries**, and **Actual Battery Bus Voltage** status for a Symmetra *Power Array*. All other fields, for all UPS models, are displayed above the **UPS** Menu.

Status Field	Definition
Battery Capacity[1]	The percentage of full UPS battery capacity that is available to support the attached equipment.
Runtime Remaining	How long the UPS can use battery power to support its attached equipment.
Nominal Battery Voltage[3]	The basic voltage range that the battery needs to supply when the UPS uses its battery for output power. **Note:** This field only appears in the Web interface.
Battery Voltage[2] or **Actual Battery Bus Voltage**[3]	The available DC power.
Battery Current[4]	The current which is being output from the battery.
Number of External Batteries[1]	The number of external batteries the UPS has.
Number of Bad Batteries[1]	The number of the external batteries that may need replacing. **Note:** This field appears only when the UPS has at least one external battery.
Self-Test Result[1]	The result of the last self-test.
Self-Test Date[1]	The date of the last self-test.
Calibration Result[1]	The result of the last runtime calibration.
Calibration Date[1]	The date of the last runtime calibration.

[1] Smart-UPS, Matrix-UPS, or Symmetra *Power Array*
[2] Smart-UPS or Matrix-UPS
[3] Symmetra *Power Array* or Silcon DP300E
[4] Silcon DP300E only

Device Manager Menus

UPS Diagnostics Options

Overview

There are two types of diagnostics options you can use with a Smart-UPS, Matrix-UPS, or Symmetra *Power Array* (a Silcon DP300E has no diagnostic options):

- Options which cause a specified test to occur immediately.
- A scheduling option which controls when a UPS self-test occurs.

How these options are accessed depends on whether you use the Web interface or Control Console.

Diagnostics

The following table describes the available diagnostics options.

Note: In the Control Console, the diagnostics options are in the Control menu.

Test	Definition
Self-Test	Causes the UPS to perform a self-test.
Simulate Power Failure	Causes the UPS to test its ability to go on battery.
Start/Stop Runtime Calibration	Initiates (or cancels) a runtime calibration, a process which determines how much runtime the UPS has available when its battery is at 100% capacity. **Note:** You can perform a runtime calibration only when the battery is at 100% capacity.
Test UPS Alarm (Smart-UPS and Matrix-UPS)	Causes a Matrix-UPS to generate an alarm tone, and a Smart-UPS to generate an alarm tone and flash its front panel lights.

Scheduled UPS self-tests

A scheduling option allows you to control when a UPS self-test occurs. The available selections are **Never**, **UPS Startup**, **Every 7 Days**, or **Every 14 Days**.

In the Web interface, this option is located on the same page as the diagnostic test options.

In the Control Console, the location of this option depends on the type of UPS:

- Symmetra *Power Array* has a **Scheduled Tests** option in the **UPS** menu.
- Smart-UPS or Matrix-UPS has a **Self-Test Schedule** option which is accessed as follows:
  a. Select **Configuration** from the **UPS** menu.
  b. Select **General** from the **Configuration** menu.

Device Manager Menus

UPS Control Options

Silcon DP300E series UPS

Three control actions are available for a Silcon DP300E series UPS.

Note: Only the **Reset UPS to Defaults** option is available by default.

Action	Definition
Turn UPS Off	Turns the UPS off after the expiration of the **Shutdown Delay** described in the table in **Shutdown parameters on page 45**.
Turn UPS Off Gracefully	Causes the UPS to turn off after PowerChute *plus* has time to shut down the server's operating system safely.
Reset UPS To Defaults	Resets all UPS parameters to their default settings.

To enable the turn-off options, do the following:

1. Access the Control Console from a local computer which has a direct, serial-cable connection with the Management Card, as described in **Local (serial) access on page 15**.

   Note: You cannot use the Web interface or Telnet access to the Control Console to enable the turn-off options.
2. Select the **Device Manage**r option from the **Control Console** menu.
3. Select the Silcon DP300E option.
4. Select the **Control** option.
5. Enable the turn-off options.
6. Use CTRL-C to return to the **Control Console** menu.
7. Log out to have the change take effect.

You can use the Web interface or Telnet to disable the turn-off options, but you must use local access to the Control Console to enable them again.

Continued on next page

Device Manager Menus

UPS Control Options *continued*

Smart-UPS, Matrix-UPS, and Symmetra Power Array

The Smart-UPS, Matrix-UPS, and Symmetra *Power Array* **Control** options are identical, with one exception: Symmetra *Power Array* and Matrix-UPS use a bypass mode; Smart-UPS does not.

Note: For information about the **Sleep Time** setting which appears in the Web interface's "Control" and "Configuration" pages, see the table in **Shutdown parameters on page 45**.

With one exception, control actions are accessed through the **Control** menu in the Web interface and the Control Console. The **Reset UPS To Defaults** is a **Configuration** menu option in the Control Console.

Note: Use the **Control** menu in the Control Console to access the diagnostic tests which are accessed through the **Diagnostics** option in the Web interface. For descriptions of the **Self-Test**, **Simulate Power Failure**, **Start/Stop Runtime Calibration**, and **Test UPS Alarm** options, see **UPS Diagnostics Options on page 40**.

Action	Definition
Turn UPS On	Turns the UPS on.
Turn UPS Off	Turns the UPS off after the **Shutdown Delay** described in the table in **Shutdown parameters on page 45**.
Turn UPS Off Gracefully[1]	Causes the UPS to turn off after PowerChute *plus* has time to shut down the server's operating system safely.
Reboot UPS	Reboots the attached equipment by immediately causing the UPS to turn off and then back on again.
Reboot UPS Gracefully[1]	Reboots the attached equipment by causing the UPS to turn off and then back on again, after PowerChute *plus* has time to safely shut down the server's operating system.
Put UPS To Sleep	Turns the UPS immediately off for the period of time defined by the **Sleep Time** setting described in the table in **Shutdown parameters on page 45**.
Put UPS To Sleep Gracefully[1]	Turns the UPS off for the period of time defined by the **Sleep Time** setting described in the table in **Shutdown parameters on page 45**, after PowerChute *plus* has time to safely shut down the server's operating system.
Put UPS In/Take UPS Off Bypass	Controls the use of bypass mode, which allows some maintenance to be performed at a Matrix-UPS or Symmetra *Power Array* model without turning off the UPS.
Reset UPS To Defaults	Resets all UPS parameters to their default settings.

[1] For information about the **Low-Battery Shutdown** parameter that defines how much time PowerChute *plus* has available to shut down the server safely, see the table in **Shutdown parameters on page 45**.

Device Manager Menus

UPS Configuration Options

Overview

The **UPS** menu's **Configuration** option provides access to the configurable parameters described in the following sections:

- **Utility line settings on this page**
- **Alarm thresholds (Symmetra Power Array) on page 44**
- **Shutdown parameters on page 45**
- **General settings on page 46**
- **Battery on page 39**

Utility line settings

The **Utility Line** settings and their values differ by UPS model.

Note: No **Utility Line** settings are available for a Silcon DP300E series UPS.

Smart-UPS/Matrix-UPS. The following table describes the Smart-UPS and Matrix-UPS **Utility Line** settings.

Setting	Definition
Output Voltage	The nominal AC voltage level for the UPS output.
High Transfer Voltage	The upper limit of acceptable input voltage. When the input reaches this value, the UPS switches to battery operation (Matrix-UPS) or starts using its SmartBoost feature (Smart-UPS).
Low Transfer Voltage (Smart-UPS)	The lower limit of acceptable input voltage. When the input reaches this value, a Smart-UPS starts using its SmartTrim feature, or switches to battery operation, if it does not have SmartTrim. **Note:** For Matrix-UPS, this setting appears in the Control Console's **Line Transfer** menu, but the value cannot be changed.
Vout Reporting (Matrix-UPS)	How Matrix-UPS scales its output voltage readings.
Sensitivity	How sensitive the UPS is to distortions in the input voltage. **Note:** Matrix-UPS always uses an **Automatic** setting.

Continued on next page

UPS Configuration Options *continued*

Utility line settings, *continued*

Symmetra *Power Array*. The following table describes the Symmetra *Power Array* **Utility Line** settings.

Setting	Definition
Output Voltage	The nominal AC voltage level for the UPS output.
Vout Reporting	How the UPS scales its output voltage readings.
Output Frequency Range	The nominal value for the frequency used by the output voltage.
If UPS fails, and frequency or voltage is out of range	How the UPS will respond if the stated condition occurs.

Alarm thresholds (Symmetra Power Array)

The following table describes the Symmetra *Power Array* **Alarm Thresholds** settings.

Threshold	Definition
Alarm if Redundancy Under	The minimum redundancy level that can be present without causing an alarm.
Alarm if Load Over	The maximum load that the attached equipment can place on the UPS without causing an alarm.
Alarm If Runtime Under	The minimum runtime that can be available without causing an alarm.

Continued on next page

Device Manager Menus

UPS Configuration Options *continued*

Shutdown parameters

Symmetra *Power Array*, Smart-UPS, and Matrix-UPS use all five **Shutdown Parameter** settings. A Silcon DP300E series UPS uses only **Low-Battery Duration** and **Shutdown Delay**.

Note: In the Control Console, use the **Configuration** menu's **Battery** option to access the **Return Battery Capacity** setting.

Setting	Definition
Return Battery Capacity	The minimum battery capacity that must be present before the UPS turns on after a shutdown that was caused by a power failure. **Note:** The UPS must also wait the time defined by the **Return Delay** setting before it can turn on.
Low-Battery Duration	How long the UPS can continue to run on battery once a low-battery condition occurs. **Note:** This setting also defines how much time PowerChute *plus* has to safely shut down its server in response to the menu options **Turn UPS Off Gracefully**, **Reboot Gracefully**, and **Put UPS To Sleep Gracefully Control**.
Shutdown Delay	How long the UPS will wait before it shuts down in response to a turn-off command.
Return Delay	How long a UPS must wait before it turns on after a shutdown that was caused by a power failure. **Note:** The UPS must also have the capacity specified by the **Return Battery Capacity** setting before it can turn on.
Sleep Time	How long the UPS will sleep (keep its outlets turned off) when you use either one of the **Control** menu's sleep options (**Put UPS To Sleep** or **Put UPS To Sleep Gracefully**). **Note:** This setting also appears in the "Control" page.

Continued on next page

Device Manager Menus

UPS Configuration Options *continued*

General settings

The available **General Settings** differ by UPS model.

Four **General Settings** are available for Smart-UPS. The first two settings (**UPS Name** and **Last Battery Replacement**) are available for all UPS models. The third setting (**Audible Alarm)** is also available for Matrix-UPS.

Note: In the Control Console, use the **Configuration** menu's **Battery** option to access the **Last Battery Replacement** and **External Batteries** settings.

Setting	Definition
UPS Name (all models)	The name used by the UPS.
Last Battery Replacement (all models)	The date when the UPS battery was last replaced. **Note:** Use a mm/dd/yy format.
Audible Alarm (Smart-UPS and Matrix-UPS only)	When the UPS will generate an alarm in response to going on battery.
External Batteries (Smart-UPS only)	How many external battery packs are connected to a Smart-UPS XL model. **Note:** Matrix-UPS can automatically sense and report the number of connected battery packs; Smart-UPS XL cannot.

Device Manager Menus

Module Status Option (Symmetra Power Array)

Menu options

A **Module Status** option in the Web interface and a **Module Diagnostics & Information** option in the Control Console provide access to status, hardware, and diagnostics information about the Symmetra *Power Array* modules.

Note: For each module, the **Module Diagnostics & Information** option in the Control Console also provides raw data that is used by APC engineers and technical support to troubleshoot hardware problems.

Module status

With the exception of the fields which report the operational status for a module, the information reported for the following modules is self-explanatory.

- The Intelligence Module
- The Redundant Intelligence Module
- The Power Modules
- The Battery in the Main Frame
- Any External Battery Frames

For information about the module-related, Symmetra *Power Array* status events, see **Management Card and Device Events on page 61**.

Device Manager Menus

UPS PowerChute network shutdown Option

Overview

A ***PowerChute*** option in the Web interface's **UPS** menu allows you to use the APC PowerChute network shutdown utility to shut down servers on your network that are using any client-version of PowerChute network shutdown.

For more information about PowerChute network shutdown, see the following documents provided in the *.\pcns* directory on the APC Web/SNMP Management Card *utility* CD:

- *PowerChute network shutdown Installation Guide* (*Install.htm*)
- *PowerChute network shutdown Release Notes* (*Relnotes.htm*)
- *PowerChute Network Shutdown with more than 50 Computers on One UPS* (*50.pdf*)

Parameters

The following table describes the PowerChute network shutdown parameters.

Parameter	Definition
Event Notification Port	Identifies the port on which the PowerChute network shutdown clients will listen for asynchronous events. This value is not configurable.
Shutdown Behavior	Defines how the UPS will be turned off after the PowerChute network shutdown clients finish shutting down their computer systems.
Add Client IP	Allows you to add up to 50 PowerChute network shutdown clients to the list of **Configured Client IP Addresses**. A PowerChute network shutdown client is also added to the list automatically when that client is installed on your network. **Note:** For information about how you can shut down more than 50 PowerChute network shutdown clients that connect to a single UPS, see *PowerChute Network Shutdown with more than 50 Computers on One UPS* (*50.pdf*) in the *.\pcns* directory on the APC Web/SNMP Management Card *utility* CD
Configured Client IP Addresses	Allows you to view the list of PowerChute network shutdown clients, and remove PowerChute network shutdown clients from the list. A PowerChute network shutdown client is also removed from the list automatically when that client is uninstalled.

Device Manager Menus

Environment Menu Options

Overview

The **Status** option (Web interface) and the **Threshold and Contact Details** option (Control Console) provide access to the status information about the probes and contacts. The **Status** option in the Web interface also accesses the firmware information for the Environmental Monitoring SmartSlot Card. In the Control Console, the firmware information is accessed through the **About Environmental Monitor** option.

The **Configuration** option in the Web interface provides access to all of the configuration settings for the probes and contacts. In the Control Console, individual options (**Trap Thresholds Probe 1**, **Trap Thresholds Probe 2**, and **Contact Settings**) are used.

Probe status

These fields report on the status for each probe.

Note: For information about the threshold values cited in the table, see **Probe settings** below.

Status Field	Definition
Temperature	The temperature sensed by the probe.
High or **Low Temperature Violation**	Whether the current temperature violates the probe's temperature threshold settings: **Yes**, **No**, or **Disabled**.
Humidity	The relative humidity sensed by the probe.
High or **Low Humidity Violation**	Whether the current humidity violates the probe's humidity threshold settings: **Yes**, **No**, or **Disabled**.

Contact status

Reports the name of each contact alarm, and whether the contact's alarm condition exists: **Yes**, **No**, or **Disabled**. For information about the contact alarm settings, see **Contact settings** below.

Probe settings

Use the **Setting** fields to define the temperature or humidity values for the thresholds, and the **Trap** fields to **Enable** or **Disable** each threshold.

Contact settings

Use the **Name** fields to define the name for the contact alarms, and the **Trap** fields to **Enable** or **Disable** each alarm.

Events Menu

Introduction

Overview

The **Events** menu provides access to the options that you use to do the following tasks:

- Access the event log.
- Define the actions to be taken when an event occurs, based on the severity level of that event.
  - Event logging
  - SNMP trap notification
  - Email notification

  Note: You can use only the Web interface to define which events will use which actions. You can also use an *evntlist.htm* page to affect individual events, as described in **How to Configure Individual Events on page 59**.
- Define up to four SNMP trap receivers, by NMS-specific IP address, for event notifications by SNMP traps.
- Define up to four recipients for event notifications by Email.

Menu options

In the Web interface, all of the events options are accessed through the **Events** menu.

In the Control Console, you access the available events-related options, as follows:

- Use the **Email** option in the **Network** menu to define the SMTP server and Email recipients.
- Use the **SNMP** option in the **Network** menu to define the SNMP trap receivers.
- Use CTRL-L to access the event log from any menu.

For information about the settings available for the **Events** menu options, and for a more detailed description of the Email feature, see the following descriptions:

- **Event Log on page 51**
- **Event Actions (Web Interface only) on page 53**
- **Event Recipients on page 55**
- **Email on page 56**

Events Menu

Event Log

Overview

The Management Card supports event logging for all UPS application firmware modules (*sumx300.bin*, *sy300.bin*, and *dp3e300.bin*.) This allows you to record and view UPS, Environmental Monitoring SmartSlot Card, and Management Card events.

You can use any of the following to view the event log:

- Web interface
- Control Console
- FTP

Logged events

By default, any event which causes an SNMP trap is logged, except for SNMP authentication failures. Additionally, the Management Card logs its abnormal internal system events. However, you can use the **Actions** option in the Web interface's **Events** menu to disable the logging of events based on their assigned severity level, as described in **Event Actions (Web Interface only) on page 53**.

Note: Some system (Management Card) events do not have a severity level. Even if you disable the event log for all severity levels, these no-severity events will still be logged.

For a list of the UPS, Environmental Monitoring SmartSlot Card, and Management Card events, see **Management Card and Device Events on page 61**.

Note: The event log will log a graceful shutdown of the UPS, even when that shutdown was not initiated by the Management Card. A graceful shutdown from SP=1 typically indicates that PowerChute *plus* or PowerNet Manager performed the shutdown. A graceful shutdown from SP=0 typically indicates that a management peripheral, such as PowerView or the Out-of-Band Management SmartSlot Card, initiated the shutdown.

Web interface

The **Log** option in the **Events** menu accesses the event log, which displays up to the last 300 recorded events, in reverse chronological order. A **Delete Log** button allows you to clear all events from the log.

Control Console

You can access the Management Card's Control Console from a local computer (direct serial-cable connection) or over the network (using Telnet). In the Control Console, press CTRL-L to display the event log. The most recent events are displayed first. Use the SPACE BAR to view up to the last 300 recorded events. While viewing the log, type d and press ENTER to clear all events from the log.

Continued on next page

Events Menu

Event Log continued

FTP

You can use FTP to retrieve a text version (*event.txt*) of the event log.

- The *event.txt* file is Tab-delineated so that it can be easily imported into any spreadsheet application.
- It reports as many as 5000 events that occurred since the log was last deleted.
- It includes information that is not in the Web interface and Control Console event log displays.
  - The version of the *event.txt* file format (first field).
  - The **Date** and **Time** the *event.txt* file was retrieved.
  - The **Name**, **Contact**, **Location**, and IP address of the Management Card.
  - The unique **Event Code** for every type of event.

    Note: The Management Card always uses 4-digit year representation when logging and displaying event data. However, you may need to select a 4-digit date format in the spreadsheet to display all four digits.

To use FTP to retrieve the *event.txt* file, do the following:

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

   ```
   ftp 159.215.12.114
   ```

2. Log in.

   Note: Case-sensitive **User Name** and **Password** settings (**apc** is the default for both) protect FTP access. You use the **Network** menu (the **FTP option** in the Control Console or the **TFTP & FTP** option in Web interface) to change these settings.

3. Use the get command to transmit the text-version of the event log to your local drive.

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

4. You can use the delete command to clear all events from the log. You will not be asked to confirm the deletion. A new event.txt file will be created immediately to record a Deleted Log event.

   ```
   ftp>del event.txt
   250 Requested file action okay, completed.
   ftp>
   ```

5. Use the quit command to exit from FTP.

   ```
   ftp>quit
   ```

Events Menu

Event Actions (Web Interface only)

Overview

The **Actions** option is available only in the Web interface's **Events** menu. It allows you to select whether the following actions are enabled or disabled for events with a specified severity level:

- **Events Log**
- **SNMP Traps**
- **Email**

Note: You can use an *evntlist.htm* page to change the severity level assigned to a specific event. For more information, see **How to Configure Individual Events on page 59**.

For information about the event log, see **Event Log on page 51**; for information about the UPS, Environmental Monitoring SmartSlot Card, and Management Card events, including the default severity level for each event, see **Management Card and Device Events on page 61**; for information about Email notifications, see **Email on page 56**.

Severity levels

With the exception of some system (Management Card) events that do not have a severity level assigned, each event is assigned a default severity level based on the type of action that is required when the event occurs.

- Informational: Indicates an event that requires no action, such as a notification of a return from an abnormal condition.
- Warning: Indicates an event that may need to be addressed if the condition continues, but which does not require immediate attention.
- Severe: Indicates an event that requires immediate attention. Unless resolved, UPS and Management Card severe events can cause incorrect operation of the UPS or its supported equipment, or can result in the loss of UPS protection during a power failure. Environmental Monitoring SmartSlot Card severe events warn of abnormal environmental conditions or possible security violations.

Note: To use an *evntlist.htm* page to change the severity level assigned to a specific event, see **How to Configure Individual Events on page 59**.

Continued on next page

Events Menu

Event Actions (Web Interface only) *continued*

Event Log action

You can disable the recording of events in the event log. By default, all events are recorded.

Note: Even if you disable the **Event Log** action for all severity levels, system (Management Card) events which have no severity level assigned will still be logged.

SNMP Traps action

By default, the **SNMP Traps** action is enabled for all informational, warning, and severe events. However, before you can use SNMP traps for event notifications, you must identify the trap receivers (up to four), by their specific IP addresses.

For information about how to define the trap receivers, see **Event Recipients on page 55**.

Email action

By default, the **Email** action is enabled for severe events only. However, before you can use Email for event notifications, you must define the Email recipients.

For information about how to define the Email recipients, see **Email on page 56**.

Events Menu

Event Recipients

Overview

The Web interface and Control Console both have options that allow you to define the trap receivers and up to four Email addresses to be used when an event occurs that has the SNMP traps or Email enabled, as described in **Event Actions (Web Interface only) on page 53**.

Trap receivers

The **Trap Receiver** settings allow you to define up to four specific NMSs to which traps will be sent.

Note: In the Control Console, access these settings through the **SNMP** option in the **Network** menu.

Item	Definition
Community Name	The password (maximum of 15 characters) used when traps are sent to the NMS identified by the **Receiver NMS IP** setting.
Receiver NMS IP	The IP address of the NMS to which traps will be sent. If this setting is **0.0.0.0** (the default value), traps will not be sent to any NMS.
Trap Generation	Enables (by default) or disables the sending of any traps to the NMS identified the **Receiver NMS IP** setting.
Authentication Traps	Enables or disables the sending of authentication traps to the NMS identified the **Receiver NMS IP** setting.

Email options

See **Email** on the next page.

Events Menu

Email

Overview

You can use the Simple Mail Transfer Protocol (SMTP) to send Email to up to four recipients when an event occurs.

To use the Email feature, you must define the following settings:

- The IP address of the Domain Name Service (DNS) server
- The DNS name of the SMTP server and the **From Address** settings for SMTP
- The Email addresses for a maximum of four recipients

Note: You can use the Email feature to page an Email recipient who uses a text-based pager gateway. For more information, see the description of the **To Address** setting in **Email recipients on page 57**.

DNS server

The Management Card cannot send any Email messages unless the DNS server is defined. The **TCP/IP & DNS** (Web interface) or **DNS** (Control Console) option in the **Network** menu accesses the setting that you use to identify the Domain Name Service (DNS) server by its IP address.

If the Management Card does not receive a response from the DNS server within five seconds, Email cannot be sent. Therefore, use a DNS server that is on the same segment as the Management Card, or on a nearby segment (but not across a WAN).

Once you define the DNS server's IP address, verify that DNS is working correctly by entering the DNS name of a computer on your network to obtain the IP address for that DNS name.

SMTP settings

The **Email** option in the **Network** menu accesses the following settings:

Setting	Description
SMTP Server	The DNS name of the SMTP server.
From Address	The contents of the **From** field in the Email messages sent by the Management Card. **Note:** The SMTP server's configuration may require that you use a valid user account on the server for this setting. See the server's documentation for more information.

Continued on next page

Events Menu

Email continued

Email recipients

The **Recipients** option in the Web interface's **Events** menu, or the **Email** option in the Control Console's **Network** Menu, accesses the settings you use to identify up to four Email recipients.

Note: In the Web interface, once you configure the settings for an Email recipient, you can use an **Email Test** option to send an Email message to that recipient. The **Email Test** option is located directly below the **Email Recipients** settings.

Setting	Description
To Address	Defines the user and domain names of the recipient. To use Email for paging, use the Email address for that recipient's pager gateway account (for example, **myacct100@skytel.com**). The pager gateway will generate the page. **Note:** Email can only send text messages. Therefore, the recipient's pager must be able to use text-based messaging.
Send via	Selects whether Email will be routed through the Management Card's SMTP server (**Local SMTP Server** option) or sent directly to the recipient's SMTP server (**Recipient's SMTP Server** option). When the recipient uses the Management Card's SMTP server, this setting has no effect. **Note:** The recommended selection is the **Local SMTP Server** option. See **Optimal Email Configuration Issues on page 58**.
Email Generation	Enables (by default) or disables the sending of Email to the defined recipient.

Continued on next page

Events Menu

Email continued

Email recipients, *continued*

Optimal Email Configuration Issues. APC recommends that you select the **Local SMTP Server** option for the **Send via** setting for the following reasons:

- If the SMTP server does not respond to the Management Card within 20 seconds, the Email will not be sent. Therefore, it is best to specify a local SMTP server rather than one across the Internet, especially if the remote SMTP server is handling large amounts of traffic.

  Note: The Management Card has limited resources to queue and transmit Email. Therefore, the Management Card has relatively low time-out values.

- The local SMTP server will queue the Email and attempt to send it several times to the remote SMTP server. When you select the **Recipient's SNMP Server** option, the Management Card will try to send the Email only once.

When you select the **Local SNMP Server** option, you must do one of the following:

- Enable forwarding at that server so that the server can route Email to external SMTP servers. Typically, SMTP servers are not configured to forward Email. Consult with your SMTP-server administrator before changing the configuration of your SMTP server to allow forwarding.
- Set up a special Email account for the Management Card. This account would then forward the Email to an external Email account.

Events Menu

How to Configure Individual Events

Overview

The **Actions** option in the Web interface's **Events** menu allows you to configure the actions to be taken by events based on the severity level assigned to each event. An event list (*evntlist.htm)* page allows you to configure the actions to be taken for an individual event.

Note: The I2C Configuration Utility on the APC Web/SNMP Management Card *utility* CD allows you to perform the same configuration described in this section by editing a text-formatted configuration (INI) file. You then convert that file to a binary-formatted configuration (CFG) file which you can send to multiple Management Cards over the network using the Web/SNMP Management Card Wizard. For more information on the I2C utility, see the *Management Card Addendum*, which is also available on the APC Web/SNMP Management Card *utility* CD (.*doc\Addendum.pdf*).

Event list access

To access the event list, you must add */evntlist.htm* to the Management Card's URL address value (IP address or DNS name). You cannot access the event list directly from the Web interface menus.

- For an IP address of 159.215.12.114, and the default TCP port of 80, the URL would be as follows:

  http://159.215.12.114/evntlist.htm
- For an IP address of 159.215.12.114, and a TCP port other than 80 (in this example, 5000), the URL would be as follows:

  http://159.215.12.114:5000/evntlist.htm
- For a DNS name of writers, the URL would be as follows:

  http://writers/evntlist.htm

Event list format

The *evntlist.htm* page uses the following columns to identify each event:

- **Code: The** event's unique Event Code.
- **Description**: The text used for the event.
- **Severity**: The event's default severity level.
- **Configuration**: The hexadecimal code that defines the actions that will occur for the event, and provides a link to the event mask you can use to configure that event.

Continued on next page

Events Menu

How to Configure Individual Events *continued*

Event mask

Use the codes identified in the following table to configure an event. For example, to configure the UPS on battery event, as follows:

- To configure it as a severe event, change the 1st character to 3.
- To log the event, and send traps to trap receivers 1 and 2, change the 2nd character to B.
- To disable traps to receivers 3 and 4, and disable Email recipients 1 and 2, change the 3rd character to 0.
- To send Email only to Email recipient 3, change the 4th character to 8.

Note: The result would be a code of 3B0800.

Character	Event Mask Code Format
1st (Left-Most)	Defines the severity code for the event. 0 (0000): No severity 1 (0001): Informational 2 (0010): Warning 3 (0011): Severe
2nd	Defines whether the event is logged, and whether SNMP traps are sent to trap receivers 1 and 2. 0 (0000): Disable logging and SNMP traps 1 (0001): Disable logging, send traps to receiver 2 2 (0010): Disable logging, send traps to receiver 1 3 (0011): Disable logging, send traps to both receivers 8 (1000): Enable logging, disable SNMP traps 9 (1001): Enable logging, send traps to receiver 2 A (1010): Enable logging, send traps to receiver 1 B (1011): Enable logging, send traps to both receivers
3rd	Controls the sending of SNMP traps to trap receivers 3 and 4, and Email notifications to Email recipients 1 and 2. 0 (0000): Disable traps and Email 1 (0001): Disable traps, send Email to recipient 2 2 (0010): Disable traps, send Email to recipient 1 3 (0011): Disable traps, send Email to both recipients 4 (0100): Send traps to receiver 3, disable Email 5 (0101): Send traps to receiver 3, Email to recipient 2 6 (0110): Send traps to receiver 3, Email to recipient 1 7 (0111): Send traps to receiver 3, Email to both recipients 8 (1000): Send traps to receiver 4, disable Email 9 (1001): Send traps to receiver 4, Email to recipient 2 A (1010): Send traps to receiver 4, Email to recipient 1 B (1011): Send traps to receiver 4, Email to both recipients C (1100): Send traps to both receivers, disable Email D (1101): Send traps to both receivers, Email to recipient 2 E (1110): Send traps to both receivers, Email to recipient 1 F (1111): Send traps to both receivers, Email to both recipients
4th	Defines whether the event sends Email notifications to Email recipients 3 and 4. 0 (0000): Disable Email 4 (0100): Send Email to recipient 4 8 (1000): Send Email to recipient 3 C (1100): Send Email to both recipients
5th and 6th	Reserved for future use. Always map as 00.

Events Menu

Management Card and Device Events

Overview

The Management Card, UPS, and Environmental Monitoring SmartSlot Card all generate event codes in response to specific conditions. Each event has a unique code and is classified as having no severity level, or with a default severity level that indicates the seriousness of the event.

Note: For information about severity levels and how they define the actions associated with an event, see **Event Actions (Web Interface only) on page 53**.

Management Card events

The following table identifies the Management Card events (labeled as System events in the table's descriptions).

Note: The Management Card has events that are classified as having no severity level. You cannot configure any action to occur for such events.

Code	Severity	Description
0x0001	Severe	System: Coldstart. (The Management Card was turned on.)
0x0002	Severe	System: Warmstart. (The Management Card was reset while it was turned on.)
0x0003	Warning	System: SNMP configuration change.
0x0004	Informational	System: Detected an unauthorized user attempting to access the SNMP interface.
0x0005	Warning	System: Detected an unauthorized user attempting to access the Control Console interface.
0x0006	Warning	System: Detected an unauthorized user attempting to access the Web interface.
0x0008	Warning	System: Password changed.
0x000C	No severity	System: File transfer started. (FTP)
0x000D	No severity	System: File transfer started. (TFTP)
0x000F	No severity	System: File transfer failed.
0x0014	No severity	System: Control Console User logged in.
0x0015	No severity	System: Web User logged in.
0x0016	No severity	System: FTP User logged in.
0x0018	No severity	System: Reset to Defaults.
0x0019	No severity	System: Initializing data.

Continued on next page

Events Menu

Management Card and Device Events *continued*

UPS events

The following table identifies all of the UPS events. However, not all of the events are generated by all UPS models.

Code	Severity	Description
0x0101	Informational	UPS: Communications established.
0x0102	Severe	UPS: Communications lost.
0x0103	Severe	UPS: Sensed a load greater than 100 percent of rated capacity.
0x0104	Informational	UPS: Overload condition cleared.
0x0105	Informational	UPS: Passed internal self-test.
0x0106	Severe	UPS: Failed internal diagnostic self-test.
0x0107	Severe	UPS: Batteries discharged.
0x0108	Informational	UPS: Battery discharge condition cleared.
0x0109	Warning	UPS: Switched to battery backup power; utility power failure.
0x010A	Informational	UPS: Returned from battery backup power; utility power restored.
0x010B	Warning	UPS: Enabled SmartBoost; low incoming line voltage.
0x010C	Informational	UPS: Returned from SmartBoost.
0x010D	Warning	UPS: Enabled SmartTrim; high incoming line voltage.
0x010E	Informational	UPS: Returned from SmartTrim.
0x010F	Severe	UPS: Battery power is low and will soon be exhausted.
0x0110	Informational	UPS: Returned from a Low-Battery condition.
0x0113	Informational	UPS: Turned on.
0x0114	Warning	UPS: Turned off.
0x0115	Warning	UPS: Entered sleep mode.
0x0116	Informational	UPS: Returned from sleep mode.
0x0117	Warning	UPS: Started reboot sequence.
0x0119	Severe	UPS: Batteries need immediate replacement.
0x011A	Informational	UPS: Bad battery condition cleared.
0x011B	Severe	UPS: In bypass due to an internal fault.
0x011C	Warning	UPS: In bypass due to user command via software or panel.
0x011D	Warning	UPS: In bypass initiated by user. (The bypass switch at the UPS was used.)
0x011E	Informational	UPS: Returned from bypass.
0x011F	Severe	UPS: Base module bypass power supply failure.

Continued on next page

Events Menu

Management Card and Device Events *continued*

UPS events, *continued*

Code	Severity	Description
0x0120	Severe	UPS: Base module fan failure.
0x0121	Informational	UPS: External battery pack communications established.
0x0122	Severe	UPS: External battery pack communications lost.
0x0123	Informational	UPS: Battery calibration test initiated.
0x0124	Informational	UPS: Battery calibration complete.
0x0125	Informational	UPS: Graceful shutdown initiated.
0x0126	Warning	UPS: SmartBoost or SmartTrim relay failure.
0x0127	Informational	UPS: SmartBoost or SmartTrim relay failure cleared.
0x0128	Warning	UPS: Bad output voltage condition.
0x0129	Informational	UPS: Bad output voltage condition cleared.
0x012A	Warning	UPS: Battery charger failure.
0x012B	Informational	UPS: Battery charger failure cleared.
0x012C	Warning	UPS: Internal battery temperature threshold violation.
0x012D	Informational	UPS: Internal battery temperature threshold violation cleared.
0x012F	Warning	UPS: No batteries installed.
0x0130	Informational	UPS: No batteries installed cleared.
0x0201	Severe	UPS: Power Module failure.
0x0202	Informational	UPS: Power Module failure cleared.
0x0203	Severe	UPS: Intelligence Module failure.
0x0204	Informational	UPS: Intelligence Module failure cleared.
0x0205	Severe	UPS: Redundant Intelligence Module failure.
0x0206	Informational	UPS: Redundant Intelligence Module failure cleared.
0x0207	Severe	UPS: Battery failure.
0x0208	Informational	UPS: Battery failure cleared.
0x0209	Severe	UPS: Load(kVA) alarm threshold violation.
0x020A	Informational	UPS: Load(kVA) alarm threshold violation cleared.
0x020B	Severe	UPS: Redundancy lost.
0x020C	Informational	UPS: Redundancy returned.
0x020D	Severe	UPS: Redundancy below alarm threshold.
0x020E	Informational	UPS: Redundancy below alarm threshold cleared.

Continued on next page

Events Menu

Management Card and Device Events *continued*

UPS events, *continued*

Code	Severity	Description
0x020F	Severe	UPS: bypass not in range; either frequency or voltage.
0x0210	Informational	UPS: bypass not in range cleared; either frequency or voltage.
0x0211	Severe	UPS: Bypass contactor stuck in bypass position.
0x0212	Informational	UPS: Bypass contactor stuck in bypass position cleared.
0x0213	Severe	UPS: Bypass contactor stuck in on-line position.
0x0214	Informational	UPS: Bypass contactor stuck in on-line position cleared.
0x0215	Severe	UPS: In bypass due to an internal fault.
0x0216	Informational	UPS: In bypass due to an internal fault cleared.
0x0217	Severe	UPS: In bypass due to an overload.
0x0218	Informational	UPS: In bypass due to an overload cleared.
0x0219	Severe	UPS: In maintenance bypass.
0x021A	Informational	UPS: In maintenance bypass cleared.
0x021B	Severe	UPS: Input circuit breaker tripped open.
0x021C	Informational	UPS: Input circuit breaker tripped open cleared.
0x021D	Severe	UPS: System level fan failure.
0x021E	Informational	UPS: System level fan failure cleared.
0x021F	Severe	UPS: Redundant Intelligence Module in control.
0x0220	Informational	UPS: Redundant Intelligence Module in control cleared.
0x0221	Severe	UPS: IIC inter-module communications failure.
0x0222	Informational	UPS: IIC inter-module communications failure cleared.
0x0223	Severe	UPS: No working Power Modules.
0x0224	Informational	UPS: No working Power Modules cleared.
0x0225	Severe	UPS: Load shutdown from bypass; input frequency or voltage outside limits.
0x0226	Informational	UPS: Load shutdown from bypass cleared; input frequency or voltage outside limits.
0x0227	Severe	UPS: Runtime below alarm threshold.
0x0228	Informational	UPS: Runtime below alarm threshold cleared.
0x0229	Severe	UPS: Extended Run Frame fault.
0x022A	Informational	UPS: Extended Run Frame fault cleared.
0x022B	Severe	UPS: Output voltage out of range.

Continued on next page

Events Menu

Management Card and Device Events *continued*

UPS events, *continued*

Code	Severity	Description
0x022C	Informational	UPS: Output voltage out of range cleared.
0x022D	Severe	UPS: Not synchronized fault.
0x022E	Informational	UPS: Not synchronized fault cleared.
0x022F	Severe	UPS: No batteries installed.
0x0230	Informational	UPS: No batteries installed cleared.
0x0231	Severe	UPS: Battery voltage high.
0x0232	Informational	UPS: Battery voltage high cleared.
0x0233	Severe	UPS: Non-specific fault; Access UPS keyboard for details.
0x0234	Informational	UPS: Non-specific fault cleared.
0x0235	Severe	UPS: Site wiring fault.
0x0236	Informational	UPS: Site wiring fault cleared.
0x0237	Severe	UPS: Backfeed protection relay open.
0x0238	Informational	UPS: Backfeed protection relay open cleared.
0x0239	Severe	UPS: Bit 28 of the abnormal condition register set.
0x023A	Informational	UPS: Bit 28 of the abnormal condition register cleared.
0x023B	Severe	UPS: Bit 29 of the abnormal condition register set.
0x023C	Informational	UPS: Bit 29 of the abnormal condition register cleared.
0x023D	Severe	UPS: Bit 30 of the abnormal condition register set.
0x023E	Informational	UPS: Bit 30 of the abnormal condition register cleared.
0x023F	Severe	UPS: Bit 31 of the abnormal condition register set.
0x0240	Informational	UPS: Bit 31 of the abnormal condition register cleared.
0x0241	Informational	UPS: Number of batteries increased.
0x0242	Informational	UPS: Number of batteries decreased.
0x0243	Informational	UPS: Number of Power Modules increased.
0x0244	Informational	UPS: Number of Power Modules decreased.
0x0245	Informational	UPS: Intelligence Module inserted.
0x0246	Informational	UPS: Intelligence Module removed.
0x0247	Informational	UPS: Redundant Intelligence Module inserted.
0x0248	Informational	UPS: Redundant Intelligence Module removed.
0x0249	Informational	UPS: Number of Extended Run Frames increased.
0x024A	Informational	UPS: Number of Extended Run Frames decreased.

Continued on next page

Events Menu

Management Card and Device Events *continued*

Environmental Monitoring SmartSlot Card events

The following table identifies the Environmental Monitoring SmartSlot Card events.

Code	Severity	Description
0x0301	Severe	Environment: Contact fault. (Contact 1)
0x0302	Informational	Environment: Contact fault cleared. (Contact 1)
0x0303	Severe	Environment: Contact fault. (Contact 2)
0x0304	Informational	Environment: Contact fault cleared. (Contact 2)
0x0305	Severe	Environment: Contact fault. (Contact 3)
0x0306	Informational	Environment: Contact fault cleared. (Contact 3)
0x0307	Severe	Environment: Contact fault. (Contact 4)
0x0308	Informational	Environment: Contact fault cleared. (Contact 4)
0x0309	Severe	Environment: Temperature threshold violation on probe 1. (Low)
0x030A	Informational	Environment: Temperature threshold violation on probe 1 cleared. (Low)
0x030B	Severe	Environment: Temperature threshold violation on probe 1. (High)
0x030C	Informational	Environment: Temperature threshold violation on probe 1 cleared. (High)
0x030D	Severe	Environment: Humidity threshold violation on probe 1. (Low)
0x030E	Informational	Environment: Humidity threshold violation on probe 1 cleared. (Low)
0x030F	Severe	Environment: Humidity threshold violation on probe 1. (High)
0x0310	Informational	Environment: Humidity threshold violation on probe 1 cleared. (High)
0x0311	Severe	Environment: Temperature threshold violation on probe 2. (Low)
0x0312	Informational	Environment: Temperature threshold violation on probe 2 cleared. (Low)
0x0313	Severe	Environment: Temperature threshold violation on probe 2. (High)
0x0314	Informational	Environment: Temperature threshold violation on probe 2 cleared. (High)
0x0315	Severe	Environment: Humidity threshold violation on probe 2. (Low)
0x0316	Informational	Environment: Humidity threshold violation on probe 2 cleared. (Low)
0x0317	Severe	Environment: Humidity threshold violation on probe 2. (High)
0x0318	Informational	Environment: Humidity threshold violation on probe 2 cleared. (High)
0x0319	Informational	Environment: Communications established.
0x031A	Severe	Environment: Communications lost.

Security

Security Features

Planning and implementing security features

As a network device that passes information across the network, the Management Card is subject to the same exposure as other devices on the network.

Use the information in this section to plan and implement the security features appropriate for your environment.

Port assignments

If a Telnet, FTP, or Web server uses a non-standard port, a user must specify the port when using the client interface, such as a Web browser. The non-standard port address becomes an extra “password,” hiding the server to provide an additional level of security. The TCP ports for which the Telnet, FTP, and Web servers listen are initially set at the standard “well known ports” for the protocols.To hide the interfaces, use any port numbers from 5000 to 65535.

For examples of what the commands would look like when the default port numbers are changed, see **FTP Server, Telnet, and Web on page 28**.

User names, passwords and community names

All user names, passwords, and community names for SNMP are transferred over the network as plain text. A user who is capable of monitoring the network traffic can determine the user names and passwords required to log into the Management Card’s Control Console or Web interface as an Administrator or Device Manager. This security limitation of the protocols affects any device using Telnet, a Web server, or an SNMP version 1 agent.

Security

Authentication

Authentication versus encryption

The Management Card controls access by providing basic authentication through user names, passwords, and IP addresses, but provides no type of encryption. These basic security features are sufficient for most environments, in which sensitive data is not being transferred. To ensure that data and communication between the Management Card and the client interfaces, such as Telnet and the Web browser, cannot be captured, you can provide a greater level of security by enabling MD5 authentication (described below) for the Web interface.

MD5 authentication (Web interface)

The Web interface option for MD5 authentication enables a higher level of access security than the basic HTTP authentication scheme. The MD5 scheme is similar to CHAP and PAP remote access protocols. Enabling MD5 implements the following security features:

- The Web server requests a user name and a password phrase (distinct from the password). The user name and password phrase are not transmitted over the network, as they are in basic authentication. Instead, a Java login applet combines the user name, password phrase, and a unique session challenge number to calculate an MD5 hash number. Only the hash number is returned to the server to verify that the user has the correct login information; MD5 authentication does not reveal the login information.
- In addition to the login authentication, each form post for configuration or control operations is authenticated with a unique challenge and hash response.
- After the authentication login, subsequent page access is restricted by IP addresses and a hidden session cookie. (You must have cookies enabled in your browser.) Pages are transmitted in their plain-text form, with no encryption.

If you use MD5 authentication, which is available only for the Web interface, disable the less secure interfaces, including Telnet, FTP, and SNMP. For SNMP, you can disable write-only access so that read access and trap facilities are still available. For additional information on MD5 authentication, see RFC document #1321 at the Web site of the Internet Engineering Task Force. For CHAP, see RFC document #1994.

Firewalls

Although MD5 authentication provides a much higher level of security than the plain-text access methods, complete protection from security breaches is almost impossible to achieve. Well-configured firewalls are an essential element in an overall security scheme.

Continued on next page

Security

Authentication *continued*

Summary of access methods

The following table describes each interface and its access methods.

Interface	Security Access	Notes
Serial Control Console	Access is by user name and password.	Always enabled.
Telnet Control Console	These methods are available: • User name and password • Selectable server port • Server Enable/Disable	The user name and password are transmitted as plain text.
SNMP	These methods are available: • Community Name • NMS IP filters • Agent Enable/Disable • Four access communities with read/write/disable capability	The NMS IP filters allow access from designated IP addresses. • 159.215.12.1 allows only the NMS with that IP address to have access. • 159.215.12.255 allows access for any NMS on the 159.215.12 segment. • 159.215.255.255 allows access for any NMS on the 159.215 segment. • 159.255.255.255 allows access for any NMS on the 159 segment. • 0.0.0.0 or 255.255.255.255 allows access for any NMS.
FTP Server	These methods are available: • User name and password • Selectable server port • Server Enable/Disable	Only the Administrator account has access.
Web Server	These methods are available: • User name and password • Selectable server port • Server Enable/Disable • MD5 Authentication option	In basic HTTP authentication mode, the user name and password are transmitted base-64 encoded (with no encryption). MD5 authentication mode uses a user name and password phrase.

Troubleshooting

Management Card

Management Card-access problems

The following table describes problems that are related to network or other access to the Management Card. For problems not described in this table or in the table in **SNMP issues on page 71**, see the troubleshooting flowcharts on the APC Web/SNMP Management Card *utility* CD (.*trouble*\). If you still cannot resolve the problem, see **If Problems Persist on page 73**.

Problem	Solution
Unable to ping the Management Card	Is the Management Card's Status LED green, indicating it is running its SNMP agent on the network? If yes, try to ping another node on the same network segment as the Management Card. If that fails, it is not a Management Card problem. If the Status LED is not green, or if the ping test succeeds, perform the following checks: • Verify that the Management Card is properly seated in the UPS or expansion chassis. • Verify all network connections. • Verify IP addresses of the Management Card and the NMS, and make sure both are on the same network or subnetwork. • Verify the default gateway (or router) IP address if the NMS is on a different physical network (or subnetwork) from the Management Card. • Verify the number of subnet bits for the Management Card's subnet mask.
PowerChute *plus* constantly or frequently reports "Unable to Communicate with UPS"	See **How to Correct Communication Lost Problems on page 72**.
The terminal program reports that it cannot allocate the comm port when you try to configure the Management Card	You must shut down PowerChute *plus* before you can use a terminal to configure the Management Card.
Cannot access the Web interface	1. Verify that HTTP access is enabled. 2. Verify that you can ping the adapter. 3. Verify that you are using either Internet Explorer 3.0 or above, or Netscape 3.0 or above.

Continued on next page

Troubleshooting

Management Card *continued*

SNMP issues

The following table describes known SNMP problems.

Problem	Solution
Unable to perform a GET	1. Verify the read (GET) community name. 2. Use the Control Console or Web interface to ensure that the NMS has access. See **SNMP on page 29**.
Unable to perform a SET	1. Verify the read/write (SET) community name. 2. Use the Control Console or Web interface to ensure that the NMS has write (SET) access. See **SNMP on page 29**.
Unable to receive traps at the NMS	Query the PowerNet MIB mconfigTrapReceiverTable OIDs to verify that the NMS IP address is listed correctly, and that the community name defined for the NMS matches the community name in the table. If necessary, use SETs to the OIDs, or use the Control Console or Web interface to correct the trap receiver definition problem. See **SNMP on page 29**.
Traps received at an NMS are not identified	See your NMS documentation to verify that the traps are properly integrated in the alarm/trap database.

Troubleshooting

How to Correct Communication Lost Problems

Overview

PowerChute *plus* may constantly or frequently report an Unable to Communicate with UPS condition when PowerChute *plus* and the Management Card have been installed together on a UPS.

Constant Unable to Communicate problem

1. Ensure that the cable between the computer and the UPS (or the expansion chassis) is securely connected at both ends.
2. Ensure that the UPS (or the expansion chassis) serial port is connected to the same computer port used to connect the computer to the UPS when PowerChute *plus* was installed.
3. If **Step 1** or **Step 2** did not correct the problem, reset the Management Card.
4. If the problem persists, disconnect (or remove) the Management Card and restart PowerChute *plus*.
   - If the problem still persists, see your PowerChute *plus* documentation to remove and then reinstall PowerChute *plus*.
   - If problem clears, reinstall the Management Card.
5. If the problem still continues or returns, see **APC Worldwide Technical Support on page 74** for information about how to contact APC for technical support.

Intermittent Unable to Communicate problem

To eliminate an interrupt request (IRQ) conflict, the most likely cause of the problem, disconnect (or remove) the Management Card from the UPS and restart PowerChute *plus*. If the problem persists, see your PowerChute *plus* documentation to remove and then reinstall PowerChute *plus*. If the problem still persists, see **APC Worldwide Technical Support on page 74** for information about how to contact APC for technical support

If problem cleared, do the following.

1. Stop PowerChute *plus*.
2. Use an ASCII text editor to edit the `[ups]` section of the PowerChute *plus* initialization file *(pwrchute.ini* or *powerchute.ini*, depending on the PowerChute *plus* operating system):
   - Add the `TimeoutFactor=40` parameter to the file.
   - Change the `UpsPollInterval` value to `=6` (default value is 4).
3. Reconnect (or reinstall) the Management Card and restart PowerChute *plus*. If the problem returns, see **APC Worldwide Technical Support on page 74** for information about how to contact APC for technical support.

Troubleshooting

If Problems Persist

If you could not resolve the problem using the information in the previous tables, or by using the troubleshooting flowcharts on the APC Web/SNMP Management Card *utility* CD (.*trouble*\), do the following:

1. Contact Technical Support at a phone number or address listed under **APC Worldwide Technical Support** on the next page, and be ready to provide the serial number and date of purchase of the Management Card.
2. Be prepared to provide a description of the problem so that the technician can attempt to solve the problem over the phone.
3. If phone consultation cannot solve the problem, the technician will give you a Return Material Authorization (RMA) number. If the Management Card is under warranty, repair or replacement is free of charge. If the warranty has expired, there will be a charge for repair or replacement.
4. If you are asked to return the Management Card, pack the unit carefully. Damage sustained in transit is not covered by the warranty.
   - Enclose a letter in the package with your name, address, RMA number, a copy of the sales receipt, your daytime phone number, and a check as payment (if applicable).
   - Mark the RMA number clearly on the outside of the shipping carton. The factory will not accept any materials without this marking.
5. Return the Management Card by insured, prepaid carrier to the address provided by the technician.

Troubleshooting

APC Worldwide Technical Support

APC provides technical support, for this or any other APC product, at no charge. This support is available by telephone, e-mail, or through the APC web pages.

You can contact APC Technical Support in any of the following ways:

- Use an APC web page.
  - *http://www.apcc.com* (Corporate Headquarters)
    Connect by links to APC web pages for specific countries and regions, each of which provides technical support information.
  - *http://www.apcc.com/support/*
    Submit technical support requests.
- Contact the APC representative or other distributor from whom you purchased your UPS or APC software application for information on how to obtain local technical support.
- Contact a local or regional APC Technical Support Center by telephone or e-mail.
  - For e-mail addresses and local, country-specific, technical support telephone numbers worldwide, go to *http://www.apcc.com/support/contact*.
  - For e-mail addresses and technical support telephone numbers of major APC regional technical support centers, use the following list:

APC Headquarters (U.S. & Canada)	1-800 800-4272 (toll free)
Latin America	+401-789-5735 (United States) apctchla@apcc.com
Europe, Middle East, Africa	+353 91 702020 (Ireland) apceurtech@apcc.com
Japan	03 5434 2021 jsupport@apcc.com

Product Information

Warranty Information

Limited warranty

American Power Conversion (APC) warrants the Web/SNMP Management SmartSlot Card to be free from defects in materials and workmanship for a period of two years from the date of purchase. Its obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. This warranty does not apply to equipment which has been damaged by accident, negligence, or misapplication or has been altered or modified in any way. This warranty applies only to the original purchaser.

Obtaining service

To obtain service under warranty you must obtain a returned material authorization (RMA) number from APC or a designated APC service center. Products must be returned to APC or an APC service center with transportation charges prepaid and must be accompanied by a brief description of the problem encountered and proof of date and place of purchase. For further information on obtaining service, see **If Problems Persist on page 73**.

Warranty limitations

Except as provided herein, American Power Conversion makes no warranties, express or implied, including warranties of merchantability and fitness for a particular purpose. Some jurisdictions do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser.

Except as provided above, in no event will APC be liable for direct, indirect, special, incidental, or consequential damages arising out of the use of this product, even if advised of the possibility of such damage.

Specifically, APC is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise. This warranty gives you specific legal rights and you may also have other rights which vary from state to state.

Product Information

Life-Support Policy

General policy

As a general policy, American Power Conversion (APC) does not recommend the use of any of its products in life-support applications where failure or malfunction of the APC product can be reasonably expected to cause failure of the life-support device or to significantly affect its safety or effectiveness. APC does not recommend the use of any of its products in direct patient care. APC will not knowingly sell its products for use in such applications unless it receives in writing assurances satisfactory to APC that (a) the risks of injury or damage have been minimized, (b) the customer assumes all such risks, and (c) the liability of American Power Conversion is adequately protected under the circumstances.

Examples of life-support devices

The term *life-support device* includes but is not limited to neonatal oxygen analyzers, nerve stimulators (whether used for anesthesia, pain relief, or other purposes), autotransfusion devices, blood pumps, defibrillators, arrhythmia detectors and alarms, pacemakers, hemodialysis systems, peritoneal dialysis systems, neonatal ventilator incubators, ventilators (for adults or infants), anesthesia ventilators, infusion pumps, and any other devices designated as “critical” by the U.S. FDA.

Hospital-grade wiring devices and leakage current protection may be ordered as options on many APC UPS systems. APC does not claim that units with this modifications are certified or listed as hospital-grade by APC or any other organization. Therefore these units do not meet the requirements for use in direct patient care.

Product Information

Specifications

Electrical

The following table identifies the electrical specifications.

Acceptable input voltage:	18-30 VDC
Maximum total current draw:	110 mA

Physical

The following table identifies the physical specifications.

Size (H × W × D)	1.46 x 4.75 x 4.3 in (3.7 x 12.1 x 10.9 cm)
Weight	.25 lb (.11 kg)
Shipping weight:	.8 lb (.36 kg)

Environmental

The following table identifies the environmental specifications.

Elevation (above MSL): Operating Storage	 0 to 10,000 ft (0 to 3,000 m) 0 to 50,000 ft (0 to 15,000 m)
Temperature: Operating Storage	 32° to 122° F (0° to 50° C) 5° to 158° F (-15° to 70° C)
Operating and storage humidity:	0 to 95%, non-condensing

Approvals

The following table identifies the approvals.

National and International:	FCC, Part 15, Class A EN 55 022 (CISPR 22), Class A VCCI Class 1 IEC 1000-4-2, 3, 4 CE C-Tick

Index

Index

Index

Index

Index

Index

990-6043A **7/2000**