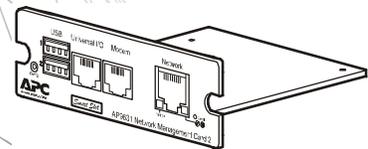


User's Guide

UPS Network Management Card 2

AP9631-IBM



Contents

Introduction	1
Product Description	1
Features	1
IPv4 Initial setup	2
IPv6 Initial setup	2
Network management features	2
Internal Management Features	3
Overview	3
Access priority for logging on	3
Types of user accounts	3
How to Recover from a Lost Password	4
Front Panel (AP9631)	5
Features	5
LED Descriptions	5
Status LED	5
Link-RX/TX (10/100) LED	7
Watchdog Features	7
Overview	7
Network interface watchdog mechanism	7
Resetting the network timer	7
Command Line Interface (CLI)	8
How To Log On	8
Overview	8
Remote access to the command line interface	8
Local access to the command line interface	9
Main Screen	9
Sample main screen	9
Information and status fields	9

How to Use the Command Line Interface	11
Overview	11
How to enter commands	11
Command syntax	11
Syntax examples	12
Command Response Codes	12
Command Descriptions	13
?	13
about	13
alarmcount	13
boot	13
cd	14
cfgshutdn	14
cfgpower	15
console	15
date	16
delete	16
detstatus	17
dir	17
dns	17
eventlog	18
exit	18
format	18
ftp	19
help	19
netstat	19
ntp	19
ping	20
portspeed	20
prompt	20
quit	20
radius	21
reboot	21
resetToDef	22
snmp, snmpv3	22
system	22
tcpip	22
tcpip6	23
uio	23
ups	24
upswupdate	26
user	27
web	27
xferINI	28
xferStatus	28

Web Interface 29

Introduction 29

Overview 29

Supported Web browsers 29

How to Log On 29

Overview 29

URL address formats 30

Home Page 31

Overview 31

Quick status icons 31

Recent Device Events 31

How to Use the Tabs, Menus, and Links 32

Tabs 32

Menus 32

Quick links 32

Monitor and Configure the UPS 33

Overview Page 33

Operating state 33

Quick Status 33

Recent UPS Events 34

Detailed Status/ Status Page 34

measurements option 34

outlet groups option 35

energy usage option 35

Control Page 36

UPS option 36

outlet groups option 38

Configuration Pages	40
What are Outlet Groups?	40
The outlet groups option (including automatic load-shedding) ..	40
The power settings option	42
The shutdown option	42
The general option	43
The self-test schedule option	44
The firmware update option	44
The PowerChute clients option	44
The sync control option	44
The parallel units option (Smart-UPS VT UPS devices)	47
 Diagnostics Page	 48
 Scheduling Page (for Shutdowns)	 49
For both the UPS and outlet group options	49
For the UPS option only	49
 About Page	 50

Environmental Monitoring 51

Overview Page	51
Temperature and Humidity Page	51
Brief status	51
Detailed status and configuration	51
Input Contacts Page	53
Brief status	53
Detailed status and configuration	53
Output Relay Page	54
About Page	54
Configuring the Control Policy	55
Configuring an output to respond to an event	55
Configuring the UPS or output to respond to an input alarm	55

Logs 56

Use the Event and Data Logs	56
Event log	56
Data log	57
How to use FTP or SCP to retrieve log files	59

Administration: Security	62
Local Users	62
Setting user access	62
Remote Users	62
Authentication	62
RADIUS	63
Configuring the RADIUS Server.....	64
Summary of the configuration procedure	64
Configuring a RADIUS server on UNIX® with shadow passwords	64
Supported RADIUS servers	64
Inactivity Timeout	65

Administration: Network Features	66
TCP/IP and Communication Settings	66
TCP/IP settings	66
DHCP response options	66
Ping Response.....	68
Port Speed	68
DNS.....	69
Web.....	70
Console	72
SNMP	73
SNMPv1	73
SNMPv3	74
FTP Server	75

Administration: Notification	76
Event Actions.....	76
Types of notification	76
Configuring event actions	76

Active, Automatic, Direct Notification	78
E-mail notification	78
SNMP traps	79
SNMP Trap Test	80
Remote Monitoring Service	80
Syslog	81

Administration: General Options 83

Identification	83
Set the Date and Time	83
Mode	83
Daylight saving	84
Format	84
Use an .ini File	84
Event Log, Temperature Units, Language, and Logon Page	85
Color-code event log text	85
Change the default temperature scale	85
Specify the UI language	85
Specify a default logon page	85
Reset the Network Management Card 2	86
Configure Links	86
About the Network Management Card 2	87

Device IP Configuration Wizard 88

Capabilities, Requirements, and Installation	88
How to use the Wizard to configure TCP/IP settings	88
System requirements	88
Installation	88
Use the Wizard	89
Launch the Wizard	89
Configure the basic TCP/IP settings remotely	89
Configure or reconfigure the TCP/IP settings locally	90

How to Export Configuration Settings..... 91

Retrieving and Exporting the .ini File91

- Summary of the procedure 91
- Contents of the .ini file 91
- Detailed procedures 91

The Upload Event and Error Messages.....93

- The event and its error messages 93
- Messages in config.ini 93
- Errors generated by overridden values 94

Related Topics.....94

File Transfers 95

How to Upgrade Firmware95

- Benefits of upgrading firmware 95
- Firmware files (Network Management Card 2) 95
- Obtain the latest firmware version 95

Firmware File Transfer Methods96

- Use FTP or SCP to upgrade one Network Management Card 2 .. 96
- How to upgrade multiple Network Management Cards 97
- Using the NMC2 Firmware Upgrade Utility for multiple upgrades 98
- Use XMODEM to upgrade one NMC 98
- Use a USB drive to transfer the files (AP9631 only) 99

Verifying Upgrades and Updates.....100

- Verify the success or failure of the transfer 100
- Last Transfer Result codes 100
- Verify the version numbers of installed firmware 100

Adding and Changing Language Packs101

Troubleshooting 102

Network Management Card Access Problems102

SNMP Issues103

Synchronization Problems103

Appendix A: List of Supported Commands	104
Appendix B: Getting Help and Technical Assistance	106
Before You Call	106
Using the Documentation	106
Getting Help and Information from the World Wide Web	106
Software Service and Support	107
Hardware Service and Support	107
IBM Taiwan Product Service	107
Appendix C: Notices	108
Edition Notice	108
Network M 89 anagement Card User's Guide	108
Trademarks	109
Important Notes	109

Introduction

Product Description

Features

The two American Power Conversion UPS Network Management Cards (NMC) mentioned below are Web-based, IPv6 Ready products that manage supported devices using multiple open standards such as:



- Hypertext Transfer Protocol (HTTP)
- Simple Network Management Protocol versions 1 and 3 (SNMPv1, SNMPv3)
- File Transfer Protocol (FTP)
- Telnet
- Secure SHell (SSH)
- Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)
- Secure Copy (SCP)

The **AP9631** Network Management Card 2:

- Provides UPS control and self-test scheduling features
- Provides data and event logs
- Provides support for the PowerChute[®] Network Shutdown utility
- Supports using a Dynamic Host Configuration Protocol (DHCP) or BOOTstrap Protocol (BOOTP) server to provide the network (TCP/IP) values of the NMC
- Supports using the Remote Monitoring Service (RMS)
- Enables you to configure notification through event logging (by the NMC and Syslog), e-mail, and SNMP traps. You can configure notification for single events or groups of events, based on the severity level or category of events
- Provides the ability to export a user configuration (.ini) file from a configured card to one or more unconfigured cards without converting the file to a binary file
- Provides a selection of security protocols for authentication and encryption
- Communicates with InfraStruxure[®] Central or InfraStruxure Manager
- Provides two USB ports
- Supports two universal input/output ports, to which you can connect:
 - Temperature (AP9335T) or temperature/humidity sensors (AP9335TH)
 - Relay input/output connectors that support two input contacts and one output relay (using AP9810 Dry Contact I/O Accessory)

Devices in which you can install the Network Management Card 2. The NMC can be installed in the following devices:

- Any Smart-UPS[®] model that has an internal expansion slot, or any Symmetra[®] UPS except the Symmetra PX 250 or Symmetra PX 500 UPS
- MGE[®] Galaxy[®] 300, 3500, or 7000
- Expansion Chassis (AP9600)
- Triple Expansion Chassis (AP9604)

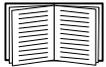
IPv4 Initial setup

You must define two TCP/IP settings for the NMC before it can operate on the network:

- IP address of the NMC
- IP address of the default gateway (only needed if you are going off segment)



Caution: Do not use the loopback address (127.0.0.1) as the default gateway. Doing so disables the card. You must then log on using a serial connection and reset the TCP/IP settings to their defaults.



To configure the TCP/IP settings, see the Network Management Card *Installation Manual*, available on the Network Management Card *Utility* CD and in printed form.

For detailed information on how to use a DHCP server to configure the TCP/IP settings at an NMC, see “TCP/IP and Communication Settings” on page 66.

IPv6 Initial setup

IPv6 network configuration provides flexibility to accommodate the user's requirements. To configure the TCP/IP settings for IPv6, see the Network Management Card *Installation Manual*, available as a PDF file on the Network Management Card *Utility* CD and on the APC website, www.apc.com.

Network management features

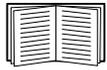
These applications and utilities work with a UPS that connects to the network through an NMC.

- PowerChute Network Shutdown — Provide unattended remote graceful shutdown of computers that are connected to UPS devices
- PowerNet[®] Management Information Base (MIB) with a standard MIB browser — Perform SNMP SETs and GETs and use SNMP traps
- InfraStruxure Central — Provide enterprise-level power management and management of agents, UPS devices, and environmental monitors.
- Device IP Configuration Wizard — Configure the basic settings of one or more NMCs over the network
- Security Wizard — Create components needed for high security for the NMC when you are using Secure Sockets Layer (SSL) and related protocols and encryption routines

Internal Management Features

Overview

Use the Web interface or the command line interface to view the status of the UPS and manage the UPS and the NMC. You can also use SNMP to monitor the status of the UPS.



For more information about the internal user interfaces, see “Web Interface” on page 29 and “Command Line Interface (CLI)” on page 8. See “SNMP” on page 73 for information about how SNMP access to the NMC is controlled.

Access priority for logging on

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

- Local access to the command line interface from a computer with a direct serial connection to the Management Card
- Telnet or SSH access to the command line interface from a remote computer
- Web access, either directly or through InfraStruXure Central



Note: SNMP has **Write +** and **Write** access. Write + has top access and enables logging on when another user is already logged on. Write access is equivalent to Web access.

Types of user accounts

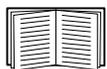
The NMC has three levels of access — Administrator, Device User, and Read-Only User — which are protected by user name and password requirements.

- An Administrator can use all of the menus in the Web interface and all of the commands in the command line interface. The default user name and password are both **apc**.
- A Device User can access only the following:
 - In the Web interface, recent events on the **Home** tab; the menus on the **UPS** tab; and the menus of the **Logs** tab including the event and data logs, accessible under the **Events** and **Data** headings. (The event and data logs display no button for this user to clear the log).
 - In the command line interface, the equivalent features and options.

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

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

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



To set **User Name** and **Password** values for the three account types, see “Setting user access” on page 62.

How to Recover from a Lost Password

You can use a local computer that connects to the Management Card through the serial port to access the command line interface.

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the provided serial cable (part number 940-0299) to the selected port at the computer and to the configuration port at the Management Card.
3. Run a terminal program (such as HyperTerminal[®]) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
 - The serial port is not in use by another application.
 - The terminal settings are correct as specified in step 3.
 - The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
6. Press ENTER, repeatedly if necessary, to display the **User Name** prompt again, then use the default, **apc**, for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must repeat step 5 and log on again.)
7. At the command line interface, use the following commands to change the **User Name** and **Password** settings, both of which are now **apc**:

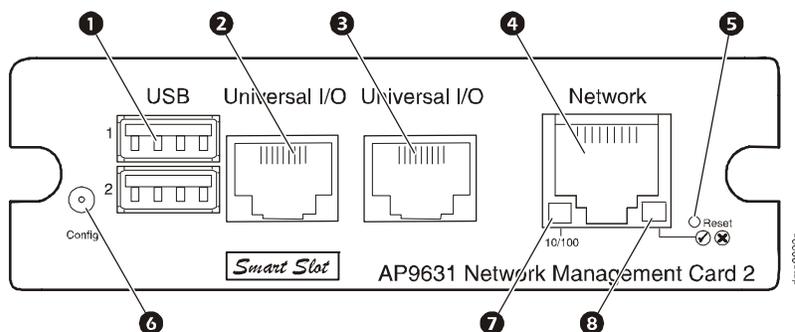
```
user -an yourAdministratorName  
  
user -ap yourAdministratorPassword
```

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

```
user -an Admin
```

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

Front Panel (AP9631)



Features

	Item	Description
①	USB ports	Reserved for future use.
② ③	Sensor ports	Connect temperature sensors, temperature/humidity sensors, or relay input/output connectors that support two input contacts and one output relay.
④	10/100 Base-T connector	Connects the NMC to the Ethernet network.
⑤	Reset button	Resets the NMC while power remains on.
⑥	Serial configuration port	Connects the NMC to a local computer to configure initial network settings or access the command line interface.
⑦	Link-RX/TX (10/100) LED	See “Link-RX/TX (10/100) LED” on page 7.
⑧	Status LED	See “Status LED” on page 5.

LED Descriptions

Status LED

This LED indicates the status of the NMC.

Condition	Description
Off	One of the following situations exists: <ul style="list-style-type: none"> The NMC is not receiving input power. The NMC is not operating properly. It may need to be repaired or replaced. Contact APC Customer Support. See “Appendix B: Getting Help and Technical Assistance” on page 106.
Solid green	The NMC has valid TCP/IP settings.
<ol style="list-style-type: none"> If you do not use a BOOTP or DHCP server, see the Network Management Card <i>Installation Manual</i> provided in printed format and on the Network Management Card <i>Utility CD</i> in PDF to configure the TCP/IP settings of the NMC. To use a DHCP server, see “TCP/IP and Communication Settings” on page 66. 	

Condition	Description
Solid orange	A hardware failure has been detected in the NMC. Contact APC Customer Support. See “Appendix B: Getting Help and Technical Assistance” on page 106.
Flashing green	The NMC does not have valid TCP/IP settings. ¹
Flashing orange	The NMC is making BOOTP requests. ¹
Alternately flashing green and orange	If the LED is flashing slowly, the NMC is making DHCP ² requests. ¹ If the LED is flashing rapidly, the NMC is starting up.
<p>1. If you do not use a BOOTP or DHCP server, see the Network Management Card <i>Installation Manual</i> provided in printed format and on the Network Management Card <i>Utility</i> CD in PDF to configure the TCP/IP settings of the NMC.</p> <p>2. To use a DHCP server, see “TCP/IP and Communication Settings” on page 66.</p>	

Link-RX/TX (10/100) LED

This LED indicates the network status of the NMC.

Condition	Description
Off	One or more of the following situations exist: <ul style="list-style-type: none">• The NMC is not receiving input power.• The cable that connects the NMC to the network is disconnected or defective.• The device that connects the NMC to the network is turned off or not operating correctly.• The NMC itself is not operating properly. It may need to be repaired or replaced. Contact APC Customer Support. See “Appendix B: Getting Help and Technical Assistance” on page 106.
Solid green	The NMC is connected to a network operating at 10 Megabits per second (Mbps).
Solid orange	The NMC is connected to a network operating at 100 Mbps.
Flashing green	The NMC is receiving or transmitting data packets at 10 Mbps.
Flashing orange	The NMC is receiving or transmitting data packets at 100 Mbps.

Watchdog Features

Overview

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

Network interface watchdog mechanism

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

Resetting the network timer

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

Command Line Interface (CLI)

How To Log On

Overview

To access the command line interface, you can use either a local, serial connection, or a remote connection (Telnet or SSH) with a computer on the same network as the Network Management Card (NMC).

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



If you cannot remember your user name or password, see “How to Recover from a Lost Password” on page 4.

Remote access to the command line interface

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

To enable or disable these access methods, use the Web interface. On the **Administration** tab, select **Network** on the top menu bar, and then the **access** option under **Console** on the left navigation menu.

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

To use Telnet to access the command line interface:

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

If the NMC uses a non-default port number (from 5000 to 32768), you must include a colon or a space, depending on your Telnet client, between the IP address (or DNS name) and the port number. (These are commands for general usage: some clients don't allow you to specify the port as an argument and some types of Linux might want extra commands).

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

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

Local access to the command line interface

For local access, use a computer that connects to the Network Management Card through the serial port to access the command line interface:

1. Select a serial port at the computer and disable any service that uses the port.
2. Connect the provided serial cable (part number 940-0299) from the selected port on the computer to the configuration port at the NMC.
3. Run a terminal program (e.g., HyperTerminal), and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER. At the prompts, enter your user name and password.

Main Screen

Sample main screen

Following is an example of the screen displayed when you log on to the command line interface at the Network Management Card (NMC).

```
American Power Conversion          Network Management Card AOS  vx.x.x
(c)Copyright 2010 All Rights Reserved Symmetra APP                vx.x.x
-----
Name      : Test Lab                      Date : 10/30/2010
Contact   : Don Adams                    Time  : 5:58:30
Location  : Building 3                   User  : Administrator
Up Time   : 0 Days, 21 Hours, 21 Minutes Stat  : P+ N+ A+

APC>
```

Information and status fields

Main screen information fields.

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

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

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

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

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

Up Time: 0 Days 21 Hours 21 Minutes

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

Date : 10/30/2009

Time : 5:58:30

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

User : Administrator

Main screen status fields.

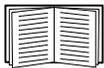
- The **Stat** field reports the NMC status. The middle status varies according to whether you are running IPv4, IPv6, or both, as indicated in the second table below.

Stat : P+ N+ A+

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

IPv4 only	IPv6 only	IPv4 and IPv6*	Description
N+	N6+	N4+ N6+	The network is functioning properly.
N?	N6?	N4? N6?	A BOOTP request cycle is in progress.
N-	N6-	N4- N6-	The NMC failed to connect to the network.
N!	N6!	N4! N6!	Another device is using the IP address of the NMC.
* The N4 and N6 values can be different from one another: you could, for example, have N4- N6+.			

A+	The application is functioning properly.
A-	The application has a bad checksum.
A?	The application is initializing.
A!	The application is not compatible with the AOS.



If P+ is not displayed, contact APC Customer Support. See “Appendix B: Getting Help and Technical Assistance” on page 106.

How to Use the Command Line Interface

Overview

The command line interface provides options to configure the network settings and manage the UPS and its Network Management Card (NMC).

How to enter commands

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

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

- Type `?` and press `ENTER` to view a list of available commands, based on your account type.
To obtain information about the purpose and syntax of a specified command, type the command, a space, and `?` or the word `help`. For example, to view `RADIUS` configuration options, type:
`radius ?`
or
`radius help`
- Press the `UP` arrow key to view the command that was entered most recently in the session. Use the `UP` and `DOWN` arrow keys to scroll through a list of up to ten previous commands.
- Type at least one letter of a command and press the `TAB` key to scroll through a list of valid commands that match the text you typed in the command line.
- Type `ups -st` to view the status of the UPS.
- Type `exit` or `quit` to close the connection to the command line interface.

Command syntax

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

Syntax examples

A command that supports multiple options:

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

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

1. Type the `user` command, one option, and the argument XYZ:

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

```
user -an XYZ
```

A command that accepts mutually exclusive arguments for an option:

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

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

```
alarmcount -p critical
```

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

Command Response Codes

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

The CLI reports all command operations with the following format:

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

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

Command Descriptions



Note: The availability of the commands and options below can vary between UPS devices.

?

Access: Administrator, Device User

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

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

about

Access: Administrator, Device User

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

alarmcount

Access: Administrator, Device User

Description:

Option	Arguments	Description
-p	all	View the number of active alarms reported by the NMC. Information about the alarms is provided in the event log.
	warning	View the number of active warning alarms.
	critical	View the number of active critical alarms.

Example: To view all active warning alarms, type:
`alarmcount -p warning`

boot

Access: Administrator only

Description: Define how the NMC will obtain its network settings, including the IP address, subnet mask, and default gateway. Then configure the BOOTP or DHCP server settings.

Option	Argument	Description
-b <boot mode>	dhcp bootp manual	Define how the TCP/IP settings will be configured when the NMC turns on, resets, or restarts. See “TCP/IP and Communication Settings” on page 66 for information about each boot mode setting.
-c	enable disable	dhcp boot modes only. Enable or disable the requirement that the DHCP server provide the APC cookie.

Option	Argument	Description
<p>The default values for these three settings generally do not need to be changed:</p> <ul style="list-style-type: none"> -v <vendor class>: APC -i <client id>: The MAC address of the NMC, which uniquely identifies it on the network -u <user class>: The name of the application firmware module 		

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

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

cd

Access: Administrator, Device User

Description: Navigate to a folder in the directory structure of the NMC.

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

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

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

`cd ..`

cfgshutdn

Access: Administrator only, Device User

Description: Configure the shutdown parameters: this enables you to show and configure UPS Shutdown Delay, UPS Return Delay, UPS Low Battery Duration, UPS Sleep Time, and UPS Min Return Runtime.



Note: These options are not available with all UPS devices.

Option	Argument	Description
-all		Show all applicable shutdown parameters for this UPS.
-sd	000 090 180 270 360 450 540 630	Set the shutdown delay in seconds.
-lo	02 05 08 11 14 17 20 23	Set the low battery duration in minutes.
-rd	000 060 120 180 240 300 360 420	Set the UPS return delay in seconds, that is, the delay time before the UPS turns on again.
-rrt	0–3600	Set the minimum return runtime in seconds, that is, the battery runtime to support the load must reach this value before the UPS turns on again.

Option	Argument	Description
-sl	0.0–359.9	Set the sleep time, in hours. The argument can have any number between 0.0 and 359.9.
-rsc	00 15 30 45 60 75 90	Set the minimum battery charge, as a percentage of the total capacity.

cfgpower

Access: Administrator only, Device User

Description: Configure the power parameters: this enables you to show and configure transfer points, sensitivity and output voltage.



Note: These options are not available with all UPS devices.

Option	Argument These values can vary with different devices.	Description
-all		Show all applicable power parameters for this UPS.
-l	97–106	Set the low transfer point, in VAC.
-h	127–136	Set the high transfer point, in VAC.
-ov	100 120 110	Set the outlet voltage, in VAC.
-s	Normal Reduced Low	Set the sensitivity, using one of the three arguments.
-bu	127 130 133 136 139 142 145 148	Set the bypass upper voltage in VAC; when the voltage rises above this value, the device goes into bypass.
-bl	086 088 090 092 094 096 098 100	Set the bypass lower voltage in VAC; when the voltage drops below this value, the device goes into bypass.

console

Access: Administrator only

Description: Define whether users can access the command line interface using Telnet, which is enabled by default, or Secure SHell (SSH), which provides protection by transmitting user names, passwords, and data in encrypted form. You can change the Telnet or SSH port setting for additional security. Alternately, disable network access to the command line interface.

Option	Argument	Description
-S	disable telnet ssh	Configure access to the command line interface, or use the <code>disable</code> command to prevent access. Enabling SSH enables SCP and disables Telnet.
-pt	<telnet port n>	Define the Telnet port used to communicate with the NMC (23 by default).

Option	Argument	Description
-ps	<SSH port n>	Define the SSH port used to communicate with the NMC (22 by default).
-b	2400 9600 19200 38400	Configure the speed of the serial port connection (9600 bps by default).

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

```
console -S ssh
```

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

```
console -pt 5000
```

date

Access: Administrator only

Definition: Configure the date used by the NMC.



To configure an NTP server to define the date and time for the NMC, see “Set the Date and Time” on page 83.

Option	Argument	Description
-d	<“datestring”>	Set the current date. Use the date format specified by the <code>date -f</code> command.
-t	<00:00:00>	Configure the current time, in hours, minutes, and seconds. Use the 24-hour clock format.
-f	mm/dd/yy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd	Select the numerical format in which to display all dates in this user interface. Each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.
-z	<time zone offset>	Set the difference with GMT in order to specify your time zone. This enables you to synchronize with other people in different time zones.

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

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

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

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

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

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

delete

Access: Administrator only

Description: Delete a file in the file system. (To delete the event log, see “eventlog,” beginning on page 18).

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

Example: To delete a file:

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

detstatus

Access: Administrator, Device User

Description: View the detailed status of the UPS. See also the -st option in “ups” on page 24.

Option	Arguments	Description
-all		Show all applicable status information for this UPS.
-rt		Runtime remaining, in hours and minutes.
-ss		UPS status summary: on line, on battery, etc.
-soc		UPS battery charge, as a percentage of the total capacity.
-om		Output measurements: voltage, frequency, watts percentage, VA percentage, current.
-im		Input measurements: voltage and frequency.
-bat		Battery voltage
-tmp		Internal temperature of the UPS
-dg		Diagnostic test results: self-test result and date, calibration result and date.

dir

Access: Administrator, Device User

Description: View the files and folders stored on the NMC.

dns

Access: Administrator

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

Parameter	Argument	Description
-OM	enable disable	Override the manual DNS.
-p	<primary DNS server>	Set the primary DNS server.
-s	<secondary DNS server>	Set the secondary DNS server.
-d	<domain name>	Set the domain name.
-n	<domain name IPv6>	Set the domain name IPv6.
-h	<host name>	Set the host name.

eventlog

Access: Administrator, Device User

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

Key	Description
ESC	Close the event log and return to the command line interface.
ENTER	Update the log display. Use this command to view events that were recorded after you last retrieved and displayed the log.
SPACEBAR	View the next page of the event log.
B	View the preceding page of the event log. This command is not available at the main page of the event log.
D	Delete the event log. Follow the prompts to confirm or deny the deletion. Deleted events cannot be retrieved.

exit

Access: Administrator, Device User

Description: Exit from the command line interface session.

format

Access: Administrator only

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



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

ftp

Access: Administrator only

Description: Enable or disable access to the FTP server. Optionally, change the port setting to the number of any unused port from 5001 to 32768 for added security.

Option	Argument	Definition
-p	<port number>	Define the TCP/IP port that the FTP server uses to communicate with the NMC (21 by default). The FTP server uses both the specified port and the port one number lower than the specified port.
-S	enable disable	Configure access to the FTP server.

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

```
ftp -p 5001
```

help

Access: Administrator, Device User

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

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

```
help
```

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

```
alarmcount help
```

netstat

Access: Administrator, Device User

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

ntp

Access: Administrator, Device User

Description: View and configure the network time protocol parameters.

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

Example 1: To enable the override of manual setting, type:

```
ntp -OM enable
```

Example 2: To specify the primary NTP server, type:

```
ntp -p 150.250.6.10
```

ping

Access: Administrator, Device User

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

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

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

```
ping 150.250.6.10
```

portspeed

Access: Administrator

Description:

Option	Arguments	Description
-s	auto 10H 10F 100H 100F	Define the communication speed of the Ethernet port. The <code>auto</code> command enables the Ethernet devices to negotiate to transmit at the highest possible speed. See “Port Speed” on page 68 for more information about the port speed settings.

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

```
portspeed -s 100H
```

prompt

Access: Administrator, Device User

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

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

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

```
prompt -s long
```

quit

Access: Administrator, Device User

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

radius

Access: Administrator only

Description: View the existing RADIUS settings, enable or disable RADIUS authentication, and configure basic authentication parameters for up to two RADIUS servers.



For a summary of RADIUS server configuration and a list of supported RADIUS servers, see “Configuring the RADIUS Server” on page 64.

Additional authentication parameters for RADIUS servers are available at the Web interface of the NMC. See “RADIUS” on page 63 for more information.

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

Option	Argument	Description
-a	local radiusLocal radius	Configure RADIUS authentication: local — RADIUS is disabled. Local authentication is enabled. radiusLocal — RADIUS, then Local Authentication. RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used. radius — RADIUS is enabled. Local authentication is disabled.
-p1 -p2	<server IP>	The server name or IP address of the primary or secondary RADIUS server. NOTE: RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.
-s1 -s2	<server secret>	The shared secret between the primary or secondary RADIUS server and the NMC.
-t1 -t2	<server timeout>	The time in seconds that the NMC waits for a response from the primary or secondary RADIUS server.

Example 1:

To view the existing RADIUS settings for the NMC, type `radius` and press ENTER.

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

```
radius -a radiusLocal
```

Example 3: To configure a 10-second timeout for a secondary RADIUS server, type:

```
radius -t2 10
```

reboot

Access: Administrator

Description: Restart the interface of the NMC.

resetToDef

Access: Administrator only

Description: Reset all parameters to their default.

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

Example: To reset all of the configuration changes *except* the TCP/IP settings for the NMC, type:
`resetToDef -p keepip`

snmp, snmpv3

Access: Administrator only

Description: Enable or disable SNMP 1 or SNMP 3.

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

Example: To enable SNMP version 1, type:
`snmp -S enable`

system

Access: Administrator only

Description: View and set the system name, the contact, the location and view up time as well as the date and time, the logged-on user, and the high-level system status P, N, A (see “Main screen status fields”).

Option	Argument	Description
-n	<system name>	Define the device name, the name of the person responsible for the device, and the physical location of the device. NOTE: If you define a value with more than one word, you must enclose the value in quotation marks. These values are also used by InfraStruxure Central and the NMC’s SNMP agent.
-c	<system contact>	
-l	<system location>	

Example 1: To set the device location as `Test Lab`, type:
`system -l "Test Lab"`

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

tcpip

Access: Administrator only

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

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

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

Example 2: To manually configure an IP address of 150.250.6.10 for the NMC, type:

```
tcpip -i 150.250.6.10
```

tcpip6

Access: Administrator only

Description: Enable IPv6 and view and manually configure these network settings for the NMC (NMC):

Option	Argument	Description
-S	enable disable	Enable or disable IPv6.
-man	enable disable	Enable manual addressing for the IPv6 address of the NMC.
-auto	enable disable	Enable the NMC to automatically configure the IPv6 address.
-i	<IPv6 address>	Set the IPv6 address of the NMC.
-g	<IPv6 gateway>	Set the IPv6 address of the default gateway.
-d6	router statefull stateless never	Set the DHCPv6 mode, with parameters of router controlled, statefull (for address and other information, they maintain their status), stateless (for information other than address, the status is not maintained), never.

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

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

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

uio

Access: Administrator, Device User

Description: This command is available for an AP9631 Network Management Card 2 with a connected Dry Contact I/O Accessory (AP9810).

Option	Argument	Description
-rc <UIO port #>	open close	Change the state of a connected output, and specify the UIO (universal input/ output) port number.
-st	<UIO port #> <UIO port #>, <UIO port #> <UIO port #>-<UIO port #>	View the status of the sensors connected to the Dry Contact I/O Accessory. To view the status of a specific sensor or several sensors, type their UIO port numbers.
-disc	<UIO port #> <UIO port #>, <UIO port #> <UIO port #>-<UIO port #>	Identify new input contact or output relay connections.

Example 1: To open the output, type:

```
uio -rc 2 open
```

Example 2: To view the status of the devices connected to a Dry Contact I/O Accessory that is installed in universal input/ output port 2, type:

```
uio -st 2
```

ups



Note: Some **ups** options are dependant on the UPS model. Not all configurations may support all options of the **ups** command.

Access: Administrator, Device User

Description: Control the UPS and view status information.

Option	Arguments	Description
-c	off graceoff on reboot gracereboot sleep gracesleep	Configure UPS actions. See “ Note: The Control Page is not available on the MGE Galaxy 300 and MGE Galaxy 7000 UPS.” on page 36 for detailed information.
-r	start stop	Initiate or end a runtime calibration. A calibration recalculates remaining runtime and requires the following: <ul style="list-style-type: none"> • Because a calibration temporarily depletes the UPS batteries, you can perform a calibration only if battery capacity is at 100%. • For some UPS devices, the load must be at least 7% to perform a calibration.
-s	start	Initiate a UPS self-test.
-b	enter exit	Control the use of bypass mode. This command is model-specific and may not apply to your UPS. See “ Note: The Control Page is not available on the MGE Galaxy 300 and MGE Galaxy 7000 UPS.” on page 36 for detailed information.

Option	Arguments	Description
-o#	Off DelayOff On DelayOn Reboot DelayReboot Shutdown DelayShutdown Cancel	<p>Control any of three outlet groups at a Smart-UPS XLM. Specify the outlet group with #. For information about outlet groups, see “What are Outlet Groups?” on page 40.</p> <p>When the state of the outlet group is on, the option accepts three arguments:</p> <ul style="list-style-type: none"> • Off — Turn off the group immediately. • DelayOff — Turn off the group after the number of seconds configured as Power Off Delay. • Reboot — Turn off the group immediately, then turn it on after the number of seconds configured as Reboot Duration and Power On Delay. • DelayReboot — Turn the outlet group off after the number of seconds configured as Power Off Delay, then turn it on after the number of seconds configured as Reboot Duration and Power On Delay. • Shutdown — If the UPS is online, this reboots the outlet group. If the UPS is on battery, this shuts down the group and waits for AC utility power before turning on the group again. • DelayShutdown — Shut down the outlet group after the number of seconds configured as Power Off Delay. • Cancel — Cancel your previous commands, e.g. turning off. <p>When the state of the outlet group is off, the option accepts two arguments:</p> <ul style="list-style-type: none"> • On — Turn on the group immediately. • DelayOn — Turn on the group after the number of seconds configured as Power On Delay. <p>The Power On Delay, Power Off Delay, and Reboot Duration must be configured at the Web interface. See “The outlet groups option (including automatic load-shedding)” on page 40 for more information.</p>
-os#		<p>View the status (on, off, or rebooting) of all the outlet groups. To view the status of a specific outlet group, specify its number. For example, type <code>ups -os1</code> to view the status of outlet group 1, see note below.</p> <p>Note: When you use this option on a UPS with a main outlet group: 1 identifies the main outlet group, 2 identifies Switched Outlet Group 1, 3 identifies Switched Outlet Group 2, etc.</p> <p>On a UPS with NO main outlet group: 1 identifies Switched Outlet Group 1, etc.</p>
-st		View the status of the UPS.
-a	start	Test the UPS audible alarm.

The ups command options for MGE Galaxy-specific UPS devices:



Note: These commands are only available on the MGE Galaxy 300 and MGE Galaxy 7000 UPS. Some options may only be available based on the individual UPS model.

Option	Argument	Description
-input	<phase#> all	Display the input measurements for the chosen phase of the UPS. Typing “all” displays the information for all phases of the UPS.
	voltage current frequency all	Specify the input measurement for the ups command. Example: ups -input 2 frequency Displays the frequency for phase 2 of the UPS.
-bypass	<phase#> all	Display the input measurements for the chosen phase of the bypass main. Typing “all” displays all phases of the bypass main.
	voltage current frequency all	Specify the input measurement for the ups command. Example: ups -bypass 2 current Displays the current for phase 2 of the bypass main.
-output	<phase#> all	Display the output measurements for the chosen phase of the UPS. Typing “all” displays the information for all phases of the UPS.
	voltage current load power perclload pf frequency all	Specify the output measurement for the ups command. Example: ups -output 2 perclload Displays the percentage of load for phase 2 of the UPS.
-batt		Display the battery status of the UPS
-about		Displays information about the UPS.
-al	<c w>	Display all existing alarms. Specifying “c” or “w” limits the display to either Critical (c) or Warning (w) alarms.

Example 1: To initiate a runtime calibration, type:

```
ups -r start
```

Example 2: To immediately turn off outlet group 2 at a Smart-UPS XLM, type:

```
ups -o2 off
```

upswupdate



Note. This command might not be available for all UPS devices.

Access. Administrator, Device User.

Description: Initiate an update of the UPS firmware. The firmware update file must have been previously sent using FTP to the NMC and stored in the /upsw/ directory.

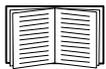
Option	Argument	Description
-apply		Start the firmware update.

Option	Argument	Description
-status		Check the status of a firmware update that is already initiated.
-lastresult		View the result of the last attempted firmware update.
-fileinfo		View information about the firmware update file present on your NMC, including its name, whether it is compatible with the UPS, and its version.

user

Access: Administrator only

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



For information on the permissions granted to each account type (Administrator, Device User, and Read-Only User), see “Types of user accounts” on page 3.

Option	Argument	Description
-an -dn -rn	<admin name> <device name> <read-only name>	Set the case-sensitive user name for each account type. The maximum length is 10 characters.
-ap -dp -rp	<admin password> <device password> <read-only password>	Set the case-sensitive password for each account type. The maximum length is 32 characters. Null/ blank passwords are not allowed.
-t	<minutes>	Set the time that the system waits before logging off an inactive user. Three minutes is the default, with a maximum of ten.

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

```
user -an XYZ
```

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

```
user -t 10
```

web

Access: Administrator

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

For additional security, you can change the port setting for HTTP and HTTPS to any unused port from 5000 – 32768. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114:

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

Option	Argument	Definition
-S	disable http https	Configure access to the Web interface. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate.

Option	Argument	Definition
-ph	<http port #>	Specify the TCP/IP port used by HTTP to communicate with the NMC (80 by default).
-ps	<https port #>	Specify the TCP/IP port used by HTTPS to communicate with the NMC (443 by default).

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

```
web -S disable
```

xferINI

Access: Administrator only. This command only works through serial CLI.

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

- If there are any system or network changes, the command line interface restarts, and you must log on again.
- If you selected a baud rate for the file transfer that is not the same as the default baud rate for the NMC, you must reset the baud rate to the default to re-establish communication with the NMC.

xferStatus

Access: Administrator only

Description: View the result of the last file transfer.



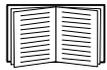
See “Verifying Upgrades and Updates” on page 100 for descriptions of the transfer result codes.

Web Interface

Introduction

Overview

The Web interface provides options to manage the UPS and the UPS Network Management Card 2 (NMC) and to view the status of the UPS.



See “Web” on page 70 for information on how to select, enable, and disable the protocols that control access to the Web interface and to define the Web-server ports for the protocols.

Supported Web browsers

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

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

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

How to Log On

Overview

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

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

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

You can set your user interface language as you log on by choosing a language from the **Language** drop-down box. See “Adding and Changing Language Packs” on page 101.



Note: When HTTPS is enabled, the NMC generates its own certificate. This certificate negotiates encryption methods with your web browser. Refer to the Security Guide on the CD or on the APC website for more details.



For information about the Web page displayed when you log on, see “Home Page” on page 31.

URL address formats

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

Common browser error messages at log-on.

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

URL format examples.

- For a DNS name of Web1:
 - `http://Web1` if HTTP is your access mode
 - `https://Web1` if HTTPS (HTTP with SSL) is your access mode
- For a System IP address of 139.225.6.133 and the default Web server port (80):
 - `http://139.225.6.133` if HTTP is your access mode
 - `https://139.225.6.133` if HTTPS (HTTP with SSL) is your access mode
- For a System IP address of 139.225.6.133 and a non-default Web server port (5000):
 - `http://139.225.6.133:5000` if HTTP is your access mode
 - `https://139.225.6.133:5000` if HTTPS (HTTP with SSL) is your access mode.
- For a System IPv6 address of 2001:db8:1::2c0:b7ff:fe00:1100 and a non-default Web server port (5000):
 - `http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` if HTTP is your access mode

Home Page

Overview

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

Quick status icons

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

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

At the upper right corner of every page, the Web interface displays the same icons currently displayed on the **Home** page to report UPS Status:

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

To return to the **Home** page to view its summary of UPS status, including the active alarms, click a quick status icon on any page of the interface.

Recent Device Events

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

How to Use the Tabs, Menus, and Links

Tabs

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

- **UPS:** Display UPS status, issue UPS control commands, configure the UPS parameters, run diagnostic tests, configure and schedule shutdowns, and view information about the UPS and the NMC.
- **Environment:** View the status of each temperature sensor, temperature and humidity sensor, input contact, or output relay connected to the NMC. View active environmental alarms and recent environmental events. Configure thresholds and other parameters related to environmental monitoring.



Note: For the UPS, the **Environment** tab displays only when a temperature sensor, temperature and humidity sensor, input contact, or output relay is present.

- **Logs:** View and configure event and data logs.
- **Administration:** Configure security, network connection, notification, and general settings.

Menus

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

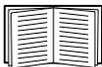
- If a heading has indented option names below it, the heading itself is not a navigational link. Click an option to display or configure parameters.
- If a heading has no indented option names, the heading itself is a navigational link. Click the heading to display or configure parameters.

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

Quick links

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

- **Link 1:** the Knowledge Base page of the APC Web site
- **Link 2:** the Product Information page of the APC Web site
- **Link 3:** the downloads page of the APC Web site

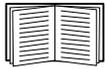


To reconfigure the links, see “Configure Links” on page 86.

Monitor and Configure the UPS



Note: For an AP9631 UPS Network Management Card 2 (NMC) with a connected Dry Contact I/O Accessory (AP9810), the **UPS** tab displays two top menu bar options, **UPS** and **Control Policy**. Use the **UPS** option to complete the tasks described in this chapter.



For information about the **Control Policy** option, see “Configuring the Control Policy” on page 55.

Overview Page

The **Overview** page is displayed by default when you click the **UPS** tab or when you select the **UPS** tab and then **Overview** on the left navigation menu of that tab.

Operating state

Below the UPS model name and configured UPS name, icons and accompanying text indicate the operating status of the UPS:

Operating State	Icon	Description
Online		No Alarms: No alarms are present, and the UPS and NMC are operating normally.
In an alarm state (Accompanying text names the alarm condition and gives a brief description of the alarm.)		Critical: A critical alarm exists, which requires immediate action to avoid data loss or equipment damage.
		Warning: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.

Quick Status

The following information is displayed (some fields are model-specific and may not display for your UPS).

- In graphs:
 - **Load in Watts:** A graph showing the load of the attached equipment as a percentage of available Watts.



Note: On the MGE Galaxy 300 and MGE Galaxy 7000 UPS, the title of the graph is **Load**.

- **Battery Capacity:** A graph showing the percentage of the total UPS battery capacity available to support attached equipment.

- In a list:
 - **Input Voltage:** The AC voltage (VAC) being received by the UPS or, for 3-phase UPS devices, by each phase of the UPS.
 - **Output Voltage:** The AC voltage (VAC) the UPS, or each phase of a 3-phase UPS, is providing to its load.
 - **Ambient Temperature:** The temperature of the air inside the input/output (I/O) enclosure of the UPS.
 - **Runtime Remaining:** How long the UPS can use battery power to support its load.
 - **Last Battery Transfer:** The cause of the last switch to battery operation.
 - **Redundancy:** The number of power modules which can fail or be removed without causing the UPS to switch to bypass operation. For example, with n+2 redundancy, two power modules could fail or be removed without causing the UPS to enter bypass mode.

Recent UPS Events

The most recent UPS events that occurred are listed in reverse chronological order. To view the entire event log, click **More Events**.

Detailed Status/ Status Page

To display detailed UPS status, click an option under the **Detailed Status** option on the left navigation menu of the UPS tab.



Note: The Detailed Status page is not available on the MGE Galaxy 300 and MGE Galaxy 7000 UPS.

measurements option

For every UPS device, this information is displayed:

Last Battery Transfer — The cause of the last switch to battery operation

Internal Temperature — The temperature inside the UPS

Runtime Remaining — How long the UPS can use battery power to support its load



To view detailed information about status items specific to the UPS device associated with the NMC, see the online help.

The types of model-specific information displayed include the following values, some of which are reported by phase for 3-phase UPS models:

- **Voltage, Current, and Frequency information**, such as input and output voltage, input and output current, input frequency, input voltage in bypass mode, and minimum and maximum input voltage during the last minute.
- **UPS Load information**, such as the load placed on the UPS in kVA or as a percentage of available kVA or Watts.
- **Fault Tolerance information**, such as redundant power available.
- **Battery information**, such as available battery capacity, percentage of full battery capacity, battery output current, rated voltage capacity of batteries, amp-hour rating of battery cabinets, number of batteries installed, and number of faulty batteries.

Output Efficiency tells you the percentage of the input power going directly out to the load. The remaining percentage is used by the UPS. **Output Energy Usage** is the actual energy used by the load starting from when the UPS was last reset to the default values.

- **Status of internal and external components**, such as intelligence and power modules, circuit breaker box, external switch gear, and transformer.

outlet groups option

This screen page is not available for all UPS devices.

The Outlet Group Status screen shows you the names and present statuses of any switched outlet groups on your UPS.

energy usage option

This screen page is not available for all UPS devices.

Energy usage enables you to monitor the energy consumption of equipment attached to your UPS. In addition it gives you energy-related data like your carbon dioxide emissions and your energy costs.

Energy Usage: Your estimated electricity consumed thus far in kilowatts per hour (kWh). For example, a UPS powering a 350 W light bulb for 1000 hours consumes 350 kWh of energy.

Total Cost: Your estimated electricity cost of energy used, in your local currency. For example, a light bulb consuming 350 kWh of energy over 1000 hours with a price of \$0.10 per kWh costs \$35 over that period of time.

CO₂ Emissions: Your estimated total emission of carbon dioxide (CO₂) in kilograms or pounds used thus far.

Total cost and CO₂ emissions vary greatly by energy source and distribution network. Obtain a rough estimate by choosing your country from the drop-down **Location** list and clicking the **Change** button. To input your own values, click on the **Change Custom Settings** link.

(Alternatively, choose **Custom** from the drop-down list, and click **Change** to input your own values).

Control Page

For UPS control actions, select **UPS** or **outlet groups** under Control.



Note: The Control Page is not available on the MGE Galaxy 300 and MGE Galaxy 7000 UPS.

UPS option

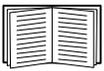
This option applies both to individual UPS devices and to Synchronized Control Groups. For background information on Synchronized Control Groups, see “The sync control option” on page 44

Actions (for a single UPS and Synchronized Control Groups). Use the actions described in the following table for single UPS devices and for Synchronized Control Groups, within these guidelines:

- The actions **Put UPS in Bypass** and **Take UPS Off Bypass** are supported:
 - Only for single UPS devices, not for Synchronized Control Groups
 - Only for Symmetra UPS and some Smart-UPS devices
- All actions *except* **Put UPS In Bypass** and **Take UPS Off Bypass** are supported:
 - For Smart-UPS devices, including those in Synchronized Control Groups
 - For single UPS devices, including single Symmetra devices



Note: When you select **Initiate PowerChute Network Shutdown** in the Web interface, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting `GraceOff` (turn off the UPS gracefully), `GraceReboot` (reboot UPS gracefully), or `GraceSleep` (put the UPS to sleep gracefully) in the command line interface.



For more information about the delays and settings in the following table, see “Configuration Pages” on page 40 and “The sync control option” on page 44. To apply **UPS Alarm Test** to a Synchronized Control Group, see “Diagnostics Page” on page 48.

Action	Definition
Turn UPS On (Web interface) <code>ups -c On</code> (command line interface)	Turns on power at the UPS. <ul style="list-style-type: none"> • For a UPS model with outlet groups, this action then turns on the outlet groups according to the value for Power On Delay for each group. See “The outlet groups option (including automatic load-shedding)” on page 40. • For a Synchronized Control Group, after a delay of a few seconds, the action turns on all enabled group members that have input power.
Turn UPS Off (Web interface) <code>ups -c Off</code> (command line interface)	Turns off the output power of the UPS and (for a UPS model with outlet groups) of all its outlet groups immediately, without a shutdown delay. The UPS and all its outlet groups remain off until you turn on its power again. For a Synchronized Control Group, this action turns off power at all enabled members of the group. No Shutdown Delay value is used. The UPSs turn off after a few seconds and remain off until you turn on their power. See “The shutdown option” on page 42. NOTE: For a synchronized turn-off action that uses the value of the Shutdown Delay of the initiating UPS, use SNMP. For the <code>upsAdvControlUpsOff</code> OID, set the value to <code>turnUpsSyncGroupOffAfterDelay (5)</code> .

Action	Definition
<p>ups -c GraceOff (command line interface)</p>	<p>Turns off outlet power of the UPS and (for a UPS model with outlet groups) all its outlet groups after the Maximum Required Delay and the configured Shutdown Delay. See “The PowerChute clients option” on page 44.</p>
<p>Reboot UPS (Web interface) ups -c Reboot (command line interface)</p>	<p>Restarts the attached equipment by doing the following:</p> <ul style="list-style-type: none"> • Turns off power at the UPS after Shutdown Delay. • Turns on power at the UPS after the UPS battery capacity returns to at least the percentage configured for Minimum Battery Capacity or can support the load for the time configured for Return Runtime Duration. (The parameter differs by UPS model.) The UPS then waits the time specified as Return Delay. See “The shutdown option” on page 42. • For a UPS with outlet groups, Power On Delay occurs after the UPS turns on and before an outlet group turns on. On the UPS tab, configure Power On Delay for each outlet group by using the settings option under Outlet Groups. See “The outlet groups option (including automatic load-shedding)” on page 40. <p>For a Synchronized Control Group action:</p> <ol style="list-style-type: none"> 1. This option turns off power at the UPS devices that are enabled group members after waiting the time configured as Shutdown Delay for the initiating UPS devices. See “The shutdown option” on page 42. 2. The initiating UPS waits up to the number of seconds specified as Power Synchronized Delay to allow time for group members to regain input power. If all group members already regained input power, this delay is omitted. If all group members regain input power during the delay, the rest of the delay is cancelled. To configure Power Synchronized Delay, see “Configure a Synchronized Control Group member” on page 46. 3. Return Delay starts when the initiating UPS is at its configured Minimum Battery Capacity (or Return Runtime Duration). See “The shutdown option” on page 42. Minimum Battery Capacity (or Return Runtime Duration) of the initiating UPS is also required of group members. However, you can reduce a group member’s requirement by configuring that member’s Minimum Battery Capacity Offset (or Return Runtime Duration Offset), e.g., if the initiator’s Minimum Battery Capacity is 50%, and a member’s Minimum Battery Capacity Offset is 5%, that member needs battery capacity of 45% to reboot. See “Configure a Synchronized Control Group member” on page 46.
<p>ups -c GraceReboot (command line interface)</p>	<ul style="list-style-type: none"> • This action is similar to Reboot UPS, but with an additional delay before the shutdown. Attached equipment shuts down only after the UPS (or the initiating UPS, for a Synchronized Control Group action) waits the Maximum Required Delay, which is calculated as described in “This option enables you to use the PowerChute Network Shutdown utility to shut down a maximum of 50 servers on the network that use a client version of the utility.” on page 42. • For a UPS with outlet groups, Power On Delay occurs after the UPS turns on and before an outlet group turns on. On the UPS tab, you configure Power On Delay for each outlet group through the settings option under Outlet Groups. See “The outlet groups option (including automatic load-shedding)” on page 40.

Action	Definition
<p>Put UPS To Sleep (Web interface)</p> <pre>ups -c Sleep</pre> <p>(command line interface)</p>	<p>Puts the UPS into sleep mode by turning off its output power for a defined period of time:</p> <ul style="list-style-type: none"> • The UPS turns off output power after waiting the time configured as Shutdown Delay. See “The shutdown option” on page 42. • When input power returns, the UPS turns on output power after two configured periods of time: Sleep Time and Return Delay. See “The shutdown option” on page 42. • For a synchronized control group action, the NMC of the initiating UPS waits up to the number of seconds configured as Power Synchronized Delay for enabled group members to regain input power before it starts the Return Delay. If all group members already regained input power, the Power Synchronized Delay is omitted. If all group members regain input power during the delay, the rest of the delay is cancelled. See “Configure a Synchronized Control Group member” on page 46.
<pre>ups -c GraceSleep</pre> <p>(command line interface)</p>	<p>Puts the UPS into sleep mode (turns off power for a defined period of time):</p> <ul style="list-style-type: none"> • The UPS turns off output power after waiting the Maximum Required Delay to allow time for PowerChute Network Shutdown to shut down its server safely, and its Shutdown Delay. See “Maximum Required Delay” on page 42 and “The shutdown option” on page 42. • When input power returns, the UPS turns on output power after two configured periods of time: its Sleep Time and Return Delay Time. See “The shutdown option” on page 42. • For a synchronized control group action, the Management Card of the UPS initiating the action waits up to the number of seconds configured as its Power Synchronized Delay for enabled group members to regain input power before it starts the Return Delay. If all group members have already regained input power, the Power Synchronized Delay is omitted. If all group members regain input power during the delay, the remainder of the delay is cancelled. See “Configure a Synchronized Control Group member” on page 46.
<p>Put UPS In Bypass and Take UPS Off Bypass (Web interface)</p> <pre>ups -b Enter</pre> <pre>ups -b Exit</pre> <p>(command line interface)</p>	<p>Controls the use of bypass mode, which allows maintenance to be performed at a Symmetra UPS and some Smart-UPS models without turning off power at the UPS.</p>

outlet groups option

In order to turn on, turn off, or restart any outlet group (while the output of the UPS is on), select the **UPS** tab and **Control - outlet groups**.

This screen page lists by name and state (including on or off) each outlet group that is configured through the **Configuration - outlet groups** option.

You can select any of the following actions (or no action) for the group.

- When the state of the outlet group is **off**:
 - **On Immediately**: Turn on the group immediately.
 - **On with Delay**: Turn on the group after the number of seconds configured as **Power On Delay**.
- When the state of the outlet group is **on**:
 - **Off Immediately**: Turn off the group immediately
 - **Off with Delay**: Turn off the group after the number of seconds configured as **Power Off Delay**.
 - **Reboot Immediately**: Turn off the group immediately, then turn it on after the number of seconds configured as **Reboot Duration** and **Power On Delay**
 - **Reboot with Delay**: Turn the outlet group off after the number of seconds configured as **Power Off Delay**, then turn it on after the number of seconds configured as **Reboot Duration** and **Power On Delay**.
- For some UPS models, when the state of the outlet group is **on** and the UPS is on battery:
 - **Shutdown Immediately, AC Restart**: Turn off the group immediately. After the number of seconds configured as **Reboot Duration** and **Power On Delay**, check that AC utility power has returned and the UPS can support the minimum return runtime demand, then turn on the group.
 - **Shutdown with Delay, AC Restart**: Turn off the group after the number of seconds configured as **Power Off Delay**. After the number of seconds configured as **Reboot Duration** and **Power On Delay**, check that AC utility power has returned and the UPS can support the minimum return runtime demand, then turn on the group.

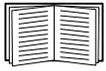
After you select an action, click **Next>>** to view a detailed description of the action, including the duration of any delays. Click **Apply** to commence the action.

Configuration Pages



Note: The Configuration Pages are not available on the MGE Galaxy 300 and MGE Galaxy 7000 UPS.

What are Outlet Groups?



Outlet grouping is available on some UPS models only. To determine whether your UPS model supports outlet groups, see your UPS documentation.

The available settings differ based on the UPS model. For detailed information about fields and values specific to your UPS model, see the online help.

Main outlet groups . Some UPS models provide AC power to one main outlet group.



Note: *The main outlet group controls the distribution of power to all switched outlet groups for the UPS.*

- If the main outlet group is off, the switched outlet groups cannot be turned on.
- If you turn off the main outlet group, the UPS turns off the switched outlet groups first, then turns off the main outlet group
- To turn on a switched outlet group, the UPS must turn on the main outlet group first, and then turn on the switched outlet group

Switched outlet groups . Some UPS models provide power to switched outlet groups. Each group can perform actions independently of the other groups. By controlling each outlet group remotely, you can start or stop devices sequentially and restart locked devices.

How outlet groups turn on and off depends on how they are configured and how you turn the UPS on or off:

- Until you configure the actions described in “outlet groups option” on page 38 and their related delays described in “The outlet groups option (including automatic load-shedding)” on page 40, when you turn on the UPS output, any outlet group that is off turns on by default and applies power to all devices attached to the outlets in that group.
- After you configure the actions and delays, the actions and delays control how outlet groups turn on and off when you turn the UPS on or off from the user interface of the Network Management Card or the display interface at the UPS.

The outlet groups option (including automatic load-shedding)

Choose **Configuration - outlet groups** to view this option.

Outlet group name and status. View the name and state of the outlet group on this screen page. Click the name of an outlet group to view or configure its settings on another screen page (see “Sequencing settings” on this page).

Setting or Field	Description
Name	A name for the outlet group displayed with the outlet group number wherever the interface displays that outlet group number.
State	Displays the state of the outlet group (on or off).

Sequencing settings. Settings vary by UPS model. Use the sequencing options to define how the UPS will respond to user-issued commands.

Setting or Field	Description
Power On Delay	<p>When this outlet group is off, it waits this delay (in seconds, the value varies with different UPS devices) before turning on when Delayed On, Reboot, or Delayed Reboot is selected as the action.</p> <p>Never check box (only available with some UPS devices): To override Power On Delay, select the Never check box. Only the Immediate On action will turn on outlets when Never is marked.</p>
Power Off Delay	<p>When this outlet group is on, it waits this delay (in seconds, the value varies with different UPS devices) before turning off when Delayed Off, Reboot, or Delayed Reboot is selected as the action. (During a delayed reboot, the outlet group then waits the number of seconds configured as Reboot Duration and Power On Delay before it turns on.)</p> <p>Never check box (only available with some UPS devices): To override the Power Off Delay, select the Never check box. Only the Immediate Off action will turn off outlets when Never is marked.</p>
Reboot Duration	<p>When this outlet group is on:</p> <ul style="list-style-type: none"> • If Reboot is selected as the action, the outlet group turns off immediately and then waits this delay (in seconds, the value varies with different UPS devices) before turning on • If Delayed Reboot is selected as the action, the outlet group waits these three delays: Power Off Delay before turning off, and Reboot Duration followed by Power On Delay before turning on.
Min Return Runtime	The minimum amount of time the UPS must be able to support the load before it can turn on again.

Load-shedding options. Settings vary by UPS model. Use the load-shedding options to define how the UPS will respond to alarms. The UPS provides automatic, sequenced, load shedding when a problem occurs with input voltage or battery capacity and provides automatic sequenced start-up of outlet groups when the problem is resolved.

Setting	Description
Settings that turn off this outlet group (some of these are not available with all outlet groups)	<ul style="list-style-type: none"> • When a power failure is longer than the number of seconds you specify. • When the remaining UPS runtime is less than the number of seconds you specify. • The UPS is overloaded (the power demand of the devices connected to the UPS exceeds the amount of power the UPS can provide). • Skip outlet off delays. (Turn the outlet group off immediately, without waiting the number of seconds configured as Power Off Delay. By default, this option is disabled.) • Stay off after power returns. (Remain off when AC utility power returns. By default, this option is disabled, and the UPS waits the number of seconds configured as Power On Delay, then turns on the outlet groups.)
Settings that turn on this outlet group	<ul style="list-style-type: none"> • The outlet group has waited the number of seconds you specify. • The battery recharges to the percentage of full capacity you specify.

Outlet group events and traps. A change in the state of an outlet group generates the event **UPS: Outlet Group turned on** with a severity of Informational, or **UPS: Outlet Group turned off** with a severity of Warning. The format of event messages is “UPS: Outlet Group *group_number*, *group_name*, *action* due to *reason*”. For example:

```
UPS: Outlet Group 1, Web Server, turned on.
UPS: Outlet Group 3, Printer, turned off.
```

By default, the event generates an event log entry, e-mail, and a Syslog message.

If you configure trap receivers for the events, trap 298 is generated when an outlet group turns on, and trap 299 is generated when an outlet group turns off. The event message is the trap argument. The default severity level is the same as for the event.

The power settings option

This option is available for all UPS models except the MGE Galaxy 300 and MGE Galaxy 7000.



The available settings differ based on the UPS model. For detailed information about fields and values available through the **power** option and specific to your UPS model, see the online help.

You can configure the following types of model-specific items:

- **Voltage** settings that determine the voltage at which the UPS begins to use automatic voltage regulation or switches to battery operation and that determine how sensitive the UPS is to voltage variation
- **Bypass** settings define conditions under which the UPS can switch to bypass mode
- **Alarm thresholds** based on available runtime and redundant power and on UPS load

The shutdown option

This option enables you to use the PowerChute Network Shutdown utility to shut down a maximum of 50 servers on the network that use a client version of the utility.

Setting	Definition
Low Battery Duration	How long the UPS can run on battery power after a low-battery condition occurs. Note: This setting also defines the time available for PowerChute to shut down servers safely in response to the Scheduling option Initiate PowerChute Network Shutdown .
Shutdown Delay	For SMX, SMT and SURTD UPS devices, this is only applicable to a Synchronized Control Group. How long the UPS waits before it shuts down in response to a turn-off command.
Maximum Required Delay	Specifies the delay defined by the Maximum Required Delay setting, which can be set through the PowerChute option on the left navigation menu.
Basic Signaling Shutdown	When enabled, provides safe system shutdown and notification, but without the advanced features available with advanced signaling. Enable basic-signaling shutdown if your computer is connected to the UPS by a basic-signaling cable, and the type of UPS either does not support advanced signaling or is configured to communicate in basic signaling.

Setting	Definition
Basic Low Battery Duration	Available only for some UPS models. Defines the amount of available battery runtime at which the UPS sends the signal for a low-battery shutdown if basic-signaling shutdown is enabled.
Sleep Time	How long the UPS sleeps (keeps its outlet power turned off) when you use the Control option Put UPS To Sleep .
Return Runtime Duration	Most UPS devices support one of the following settings to ensure that the UPS batteries have time to charge. Then, if input power fails soon after the UPS restarts, the UPS can perform a safe shutdown. (The UPS must also wait the time defined as Return Delay before it turns on.)
Minimum Battery Capacity	Return Runtime Duration: How long the UPS must be able to support the load by battery power in order for the UPS to end its sleep time (or turn back on when rebooted) and resume providing output power Minimum Battery Capacity: The minimum battery capacity, as a percentage of full capacity, required in order for the UPS to end its sleep time (or turn back on when rebooted) and resume providing output power.
Return Delay	For SMX, SMT and SURTD UPS devices, this is only applicable to a Synchronized Control Group. How long the UPS waits before it turns on after a shutdown that was caused by a power failure or after a scheduled shutdown. NOTE: The UPS must also have the capacity specified by the Minimum Battery Capacity setting or the available runtime specified as Return Runtime Duration before it can turn on.
Maximum Required Delay - Force Negotiation	Displays the delay required to ensure that each PowerChute client has enough time to shut down safely when either the UPS or the PowerChute client initiates a safe shutdown. When the Force Negotiation check box is selected, PowerChute polls each server listed as a PowerChute Network Shutdown client for information on the time it needs for a safe shutdown. PowerChute recalculates this delay whenever the NMC interface of the UPS turns on or is reset. This option is not available on the MGE Galaxy 300 or MGE Galaxy 7000. Maximum Required Delay is the longest shutdown delay needed by any server on the list, plus two additional minutes to allow for unforeseen circumstances. The negotiation can take up to 10 minutes. If you do not select Force Negotiation , two minutes is used by default as the shutdown delay for all clients.
On-Battery Shutdown Behavior	After the PowerChute Network Shutdown clients shut down their computer systems, this parameter determines whether the UPS turns on automatically or must be turned on manually when input power is restored. Note: This option is not available on the MGE Galaxy 300 or MGE Galaxy 7000 UPS.
Authentication Phrase	The case-sensitive phrase of 15 to 32 ASCII characters to be used during MD5 authentication for PowerChute communication. The default Administrator setting is admin user phrase .

The general option

Settings vary by UPS model. Each UPS model supports only some of the following:

Setting	Definition
UPS Name	A name to identify the UPS.
UPS Position	The physical orientation of the UPS, rack or tower.

Setting	Definition
Audible Alarm	Enable or disable the audible alarm of the UPS, and, for some UPS models, define the condition that will cause the alarm to sound.
Last Battery Replacement	The month and year of the most recent battery replacement.
Number of Batteries or External Batteries	The number of batteries, excluding built-in batteries, that the UPS has. Some models that have more than 16 batteries must add batteries in quantities of 16 (e.g., 16, 32, 48, etc.), but can then be adjusted to the correct value.
External Battery Cabinet	The battery cabinet Amp-Hour rating of an external battery source.

The self-test schedule option

Use this option to define when the UPS will initiate a self-test.

The firmware update option

This option is not available for all UPS devices. Use this option to initiate an update of the UPS firmware. The firmware update file must have been previously sent using FTP to the NMC and stored in the /upswf/ directory.

The PowerChute clients option

Click **Add Client** to enter the IP address of a new PowerChute Network Shutdown client. To delete a client, click the IP address of that client in the list, and then click **Delete Client**.

The list can contain the IP addresses of up to 50 clients.



Note: When you install a PowerChute Network Shutdown client on your network, it is added to the list automatically, and when you uninstall a PowerChute Network Shutdown client, it is removed from the list automatically.

The sync control option



Note: The Sync Control page is not available on the MGE Galaxy 300, MGE Galaxy 7000 UPS, or the Symmetra UPS.

What is the synchronization process? If you apply an action to a Synchronized Control Group, enabled members of the group behave as follows:

- Each UPS receives the command regardless of output status (e.g., low battery).
- The action uses the delay periods (such as **Shutdown Delay**, **Sleep Time**, and **Return Delay**) configured for the initiating UPS.
- When the action begins, a UPS that is unable to participate retains its present output status while the other UPS devices perform the action. If a UPS is already in an output state that the action

requires (e.g., a UPS is already off when the Reboot UPS action starts), that UPS logs an event, but performs the rest of the action, if any.

- All participating UPS devices synchronize their performance of the action (within a one-second time period under ideal conditions for Smart-UPS, but sometimes longer).
- In reboot and sleep actions:
 - Immediately before the initiating UPS begins waiting the time specified as **Return Delay**, by default it waits up to 120 seconds (its configurable **Power Synchronized Delay**) for any UPS that does not have input power to regain that power. Any UPS that fails to regain input power during that delay does not participate in the synchronized restart, but waits until its own input power returns before restarting.
 - The LEDs on the front of the UPS do not sequence their lights as they do for a normal (not synchronized) reboot or sleep action.
- UPS status and events are reported in the same way for synchronized actions as for actions on individual UPS devices.

Guidelines for Synchronized Control Groups. Before you configure this UPS as a Synchronized Control Group member, review these guidelines:

- All UPS devices in a Synchronized Control Group must be the same model.
- Synchronized Control Groups are supported for any Smart-UPS with a card slot that accepts a Network Management Card.
- When its membership in a Synchronized Control Group is enabled, the NMC blocks UPS communications from a connected management device on the serial communications port. However, the NMC still allows access to the command line interface on the serial communications port.
- For detailed information, see the Knowledge Base on the support page of the APC website and search for 11135.

Display status of a Synchronized Control Group member. The following information is displayed about the Synchronized Control Group membership of this group member when its group membership is enabled.

Status item	Description
IP Address	The IP address of the Network Management Card of this group member (UPS).
Input Status	The state of the input power of this group member: good (acceptable) or bad (not acceptable).
Output Status	The status of the output power of this group member: On or Off

Configure a Synchronized Control Group member

Parameter	Description
Group Membership	Determines whether this Synchronized Control Group member is an active member of its group. If you disable group membership, this UPS functions as if it were not a member of any Synchronized Control Group. When you enable or disable Group Membership, the change causes the management interface to reboot the next time you log out. The change takes effect at that time.
Control Group Number	The unique identifier of the Synchronized Control Group of which this NMC's UPS is a member. This value must be a number from 1 through 65534. A UPS can be a member of only one Synchronized Control Group. All members of a Synchronized Control Group must have the same Control Group Number and Multicast IP Address.
Multicast IP Address	The IP address used to communicate among members of a Synchronized Control Group. For IPv6, any valid IPv6 multicast address can be used. For IPv4, the allowed range is 224.0.0.3 to 224.0.0.254. All members of a Synchronized Control Group must have the same Control Group Number and Multicast IP Address.
Power Synchronized Delay	The maximum time (120 seconds by default) that the initiating UPS waits, if necessary, for other group members to regain input power when the initiating UPS is ready to turn on. When this delay expires, the initiating UPS waits to recharge its battery to the runtime specified as Return Runtime Duration or the battery capacity specified as Minimum Battery Capacity, if necessary, then waits the time specified as Return Delay, and then turns on. NOTE: For information about configuring the Return Runtime Duration, see "Return Runtime Duration" on page 43. For information about configuring the Minimum Battery Capacity, see "Minimum Battery Capacity" on page 43.
Minimum Battery Capacity Offset or Return Runtime Duration Offset	A UPS supports only one of these parameters, depending on UPS model. You can configure this value differently for each member of the Synchronized Control Group through the management interface of that member. Minimum Battery Capacity Offset: A percentage of battery capacity that is subtracted from Minimum Battery Capacity of the UPS that initiates a synchronized action to determine the battery capacity required for this group member to turn on during synchronized actions. For information about configuring the Minimum Battery Capacity, see "Minimum Battery Capacity" on page 43. Return Runtime Duration Offset: A number of seconds that is subtracted from the Return Runtime Duration of the UPS that initiates a synchronized action to determine the available runtime required for this group member to turn on during synchronized actions. For information about configuring the Return Runtime Duration, see "Return Runtime Duration" on page 43.
Authentication Phrase	The case-sensitive phrase (15 to 32 ASCII characters) used to authenticate members of a Synchronized Control Group. All members of a Synchronized Control Group must have the same authentication phrase. The default is APC SCG auth phrase .
Encryption Phrase	The encryption key for the protocol that ensures secure communication among members of a Synchronized Control Group. All members of a Synchronized Control Group must have the same encryption phrase. The default is APC SCG crypt phrase .
Synchronized Control Port	The network port that Synchronized Control Groups use to communicate. Use any non-standard port from 5000 to 32768.

The parallel units option (Smart-UPS VT UPS devices)

Setting	Description
Parallel Unit Configuration	Lists all parallel units (UPS devices of the same type that share a load, continuing to provide power to the load if a parallel unit fails). The UPS to which you are logged on is listed first.
Add Unit	Use this button to add a unit (up to a maximum of 9) or to change the name of a configured unit. Specify a name for the unit (up to 8 characters) and specify its IP address.

Diagnostics Page

You can run a self-test or a runtime calibration for any UPS from this company. The UPS audible alarm test is model-specific and may not be available for your UPS.



Note: The Diagnostics Page is not available on the MGE Galaxy 300 and MGE Galaxy 7000 UPS.

Field	Description
Self-test	The result (passed, failed, or unavailable) and date of the last UPS self-test.
Calibration	The result of the last runtime calibration. A calibration recalculates remaining runtime and requires the following: <ul style="list-style-type: none">• Because a calibration temporarily depletes the UPS batteries, you can perform a calibration only if battery capacity is at 100%.• For some UPSs, the load must be at least 7% for a calibration to be performed.
Initiate	Select a diagnostic procedure to perform immediately: a test of the UPS audible alarm, a UPS self-test, or a runtime calibration. When you test the audible alarm of a member of a Synchronized Control Group: <ul style="list-style-type: none">• In the Web interface, this option tests the alarms of all enabled members of the group.• In SNMP, you can set the OID upsAdvControlFlashAndBeep to flashAndBeep (2) to test the alarm of an individual UPS or to flashAndBeepSyncGroup (3) to test the alarms of all enabled group members.

Scheduling Page (for Shutdowns)



Note: The **Scheduling - UPS** page is not available on the MGE Galaxy 300 and MGE Galaxy 7000 UPS.

For both the UPS and outlet group options

You can schedule a shutdown for a UPS device under **UPS** or for an individual outlet group (if applicable) under **outlet groups**.

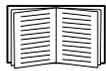
The configured schedules display along the top of the page when you select UPS or outlet groups, with the details, including whether they are currently enabled or disabled.

Edit, Enable, Disable, or Delete a Scheduled Shutdown. Click the schedule name in the list of schedules along the top of either the **UPS** or **outlet groups** page, in order to access and edit the parameters of a scheduled shutdown, including disabling it temporarily by clearing the **Enable** check box, or deleting it permanently.

Creating a UPS or outlet group shutdown schedule.

1. Select either **UPS** or **outlet group** under **Scheduling**.
2. Select the type of shutdown to schedule, **One-time Shutdown**, **Daily Shutdown**, or **Weekly Shutdown** (at 1, 2, 4, or 8 week intervals), and click the **Next** button.
3. To disable a schedule temporarily, clear the **Enable** button.
4. Define a name, and a schedule date and time.
For a weekly shutdown, specify the frequency using the drop-down box.
5. Specify whether the device or outlet group should turn back on after the shutdown:

Turn back on: Define whether the UPS will turn on at a specific day and time, **Never** (the UPS must be turned on manually), or **Immediately** (the UPS will turn on after waiting 6 minutes and the time specified as the Return Delay).



To configure the Return Delay, see “Return Delay” on page 43

6. For an outlet group only, specify the group by selecting the appropriate button.
7. **Signal PowerChute Network Shutdown Clients:** Specify whether to notify clients listed as “The PowerChute clients option”.

For the UPS option only

Schedule a synchronized shutdown. All scheduled shutdowns will be synchronized when the UPS whose NMC initiates the shutdown is a member of a Synchronized Control Group and its status as a member is enabled. Always schedule all shutdowns through the same member of the group. For a scheduled synchronized UPS shutdown to occur, a network connection to each UPS in the group must exist at the time at which the action is scheduled to occur.



Caution: Do not schedule shutdowns through more than one group member. Such scheduling may cause unpredictable results.

About Page

This option provides the following information about the UPS and the firmware of its Network Management Card:

- **Model:** The model name of the UPS.
- **Position:** The physical orientation of the UPS, **rack** or **tower** (only for rack- or tower-mounted UPS devices). (Not available on the MGE Galaxy 300 or MGE Galaxy 7000 models.)
- **Serial Number:** The unique identification number of the UPS, also provided on the outside of the UPS.
- **Firmware Version:** The revision numbers of the firmware modules currently installed on the UPS.
- **Manufacture Date:** The date on which the manufacturing of this UPS was completed. (Not available on the MGE Galaxy 300 or MGE Galaxy 7000 models.)

The MGE Galaxy 300 and MGE Galaxy 7000 UPS devices report the following additional information:

- **Product Name:** The brand name of the UPS.
- **Technical Level:** The technical level of the UPS.
- **UPS Time:** The local time at the location of the UPS.
- **Country:** The country where the UPS is located. (MGE Galaxy 7000 only)
- **Manufacturer Name:** The manufacturer of the UPS.

Environmental Monitoring



Note: The **Universal I/O** menu tab displays when you have installed the temperature and humidity sensors AP9335T/ TH or the Dry Contact I/O Accessory (AP9810).

The **Environment** menu options display only when an External Environmental Monitoring card (AP9612TH) is connected to a UPS with the AP9631 NMC.

Overview Page

The **Overview** page lists the status of environmental monitoring devices associated with the AP9631 NMC.

Heading	Displayed Information
Temperature and Humidity	Lists all sensors and, for each sensor, the alarm status, temperature currently recorded, and humidity (if supported) currently recorded. For detailed status or to reconfigure a sensor's parameters, click the sensor's name.
Input Contacts	Lists each enabled input contact and its alarm status and current state (open or closed). For detailed status of an enabled input contact or to reconfigure that contact's parameters, click the name of the contact. Note: To view or configure the parameters of a disabled contact, or to enable it, you must access the interface page for that contact through Input Contacts on the left navigation menu
Output Relay	Lists the alarm status and the current state (open or closed) of the output relay of the integrated Environmental Monitor. For detailed status of that output relay or to reconfigure its parameters, click its name.
Recent Environmental Events	The Recent Environmental Events field lists, in reverse chronological order, the most recent environmental events. To view the entire event log, click More Events at the lower right.

Temperature and Humidity Page

Brief status

Click **Temp & Humidity** on the left navigation menu to display the name, alarm status, temperature, and humidity (if supported) for each sensor.

Detailed status and configuration

Click the name of a sensor for detailed alarm status or to configure its values:

Identification and alarm status.

Parameter	Description
Name	A name for this sensor. <i>Maximum:</i> 20 characters.

Parameter	Description
Location	This physical location of the sensor. <i>Maximum</i> : 20 characters.
Alarm Status	One of the following is displayed: <ul style="list-style-type: none"> • Normal if this sensor is not reporting an alarm condition. • If this sensor is in an alarm state, the text of the alarm, indicating which threshold is violated, and the severity of the alarm, indicated by color (red for critical, orange for warning).
Thresholds	See the next two sections for descriptions of the configurable thresholds and Hysteresis values.

Thresholds. For each sensor, you set the same types of thresholds for temperature and (if supported) humidity measured at the sensor.

Threshold	Description
Maximum	If the threshold for maximum temperature or for maximum humidity for the sensor is exceeded, an alarm occurs.
High	If the threshold for high temperature or for high humidity for the sensor is exceeded, an alarm occurs.
Low	If the temperature or humidity drops below its low threshold for the sensor, an alarm occurs.
Minimum	If the temperature or humidity drops below its minimum threshold for the sensor, an alarm occurs.

Hysteresis. Use the Hysteresis value to avoid getting repeated alarms for the same temperature or humidity violation. With the Hysteresis value you can specify how far past a threshold the temperature or humidity must go to clear the threshold violation. (After a threshold violation is cleared, it is subject to being breached again, and therefore it can cause another alarm).

- For maximum and high threshold violations, the clearing point is the threshold *minus* the hysteresis value you input.
- For minimum and low threshold violations, the clearing point is the threshold *plus* the hysteresis value.

If the temperature or humidity that causes a violation tends to waver slightly up and down, you could increase the value for temperature hysteresis or humidity hysteresis to avoid multiple alarms. When the hysteresis value is too low, such wavering can cause and clear a threshold violation repeatedly, triggering multiple alarms.

Example of falling but wavering temperature: The minimum temperature threshold is 12°C, and the temperature hysteresis is 2°C. The temperature drops below 12°C, violating the threshold and causing an alarm. It then wavers up to 13°C and then down to 11°C repeatedly, but — because of the 2°C hysteresis value — no clearing event and therefore no new violation or alarm occurs. For the existing violation to clear, the temperature would have to rise above 14°C (more than 2°C above the threshold).

Example of rising but wavering humidity: The maximum humidity threshold is 65%, and the humidity hysteresis is 10%. The humidity rises above 65%, violating the threshold. It then wavers down to 60% and up to 70% repeatedly, but no clearing event and therefore no new violation occur. For the existing violation to clear, the humidity would have to drop below 55% (10% past the threshold).

Input Contacts Page

Brief status

Click **Input Contacts** on the left navigation menu to display the name, alarm status, and state (open or closed) of each input contact.

Detailed status and configuration

Click the name of an input contact for detailed status or to configure its values:

Parameter	Description
Input Contact	Enable or disable this input contact. When disabled, the contact generates no alarm even when it is in the abnormal position
Name	A name for this input contact. <i>Maximum: 20 characters.</i>
Location	The location of this input contact. <i>Maximum: 20 characters.</i>
Alarm Status	Normal if this input contact is not reporting an alarm, or the severity of the alarm, if this input contact is reporting an alarm
State	The current state of this input contact: Closed or Open .
Normal State	The normal (non-alarm) state of this input contact: Closed or Open .
Severity	The severity of the alarm that the abnormal state of this input contact generates: Warning or Critical .

Output Relay Page

This option is only available for devices with installed Dry Contact I/O Accessories. Select the Environment tab, then **Universal I/O** from the top menu bar. Click **Output Relay** to display the status of the output relay and configure its values.

Parameter	Description
Name	A name for this output relay. <i>Maximum: 20 characters.</i>
Location	The location of this output relay. <i>Maximum: 20 characters.</i>
Alarm Status	Normal if this output relay is not reporting an alarm, or the severity of the alarm if this output relay is reporting an alarm.
State	The current state of this output relay: Closed or Open .
Normal State	The normal (non-alarm) state of this output relay: Closed or Open .
Control	To change the current state of this output relay, check-mark the setting.
Delay	The number of seconds a selected alarm condition must exist before the output relay is activated. Use this setting to avoid activating an alarm for brief transient conditions. NOTE: Even if additional mapped alarms occur after the delay begins, the delay does not restart but continues until the output relay is activated.
Hold	The minimum number of seconds the output relay remains activated after the alarm occurs. Even if the activating alarm condition is corrected, the output relay remains activated until this time period expires.

About Page

Click **About** on the left navigation menu of the top menu bar option **Environment** to display what environmental monitoring devices are in use with this UPS and their firmware versions.

Configuring the Control Policy

For an AP9631 NMC with up to two connected Dry Contact I/O Accessories (AP9810), you can configure its outputs to respond to events, and you can configure the UPS and outputs to respond to input alarms.



Note: The MGE Galaxy 300 and MGE Galaxy 7000 UPS devices cannot be configured to respond to input alarms.

Configuring an output to respond to an event

1. Select the **UPS** tab, **Control Policy** in the top menu bar, and **by event** under **Event Actions** on the left navigation menu.
2. Click a category name to view all of the events in the category, or click a sub-category name to view the events in that sub-category.
3. In the list of events, review the marked columns to see whether the required event is already configured to change the state of the output relay.
4. To change the current configuration, click the event name, select the output relay that will change state when this event is detected, and click **Apply**.

Configuring the UPS or output to respond to an input alarm

1. Select the **UPS** tab, **Control Policy** in the top menu bar, and **by event** under **Event Actions** on the left navigation menu.
2. Click **I/O Contact**, then click the name of the event to configure.
3. The NMC supports up to four inputs. You must specify the input that will be associated with this event.
 - a. In the **Port** drop-down list, select the Universal Sensor Port number (**1** or **2**) to which the Dry Contact I/O Accessory is installed.
 - b. In the **Zone** drop-down list, select the zone letter (**A** or **B**) of the contact to which the input is installed.
4. Define the action the UPS will perform when the input changes state, and select the output that will change state when this event is detected.
5. Click **Display** to review your changes, then click **Apply**.



Note: The action you configure occurs once. If you restore the input to its normal state before the alarm condition clears, the output will not change state unless the alarm condition clears and then reoccurs.

Logs

Use the Event and Data Logs

Event log

Path: Logs > Events > *options*

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

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



See “Configuring by event” on page 77.

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

- By default, view the event log as a page of the Web interface. The most recent event is recorded on page 1. In the navigation bar below the log:
 - Click a page number to open a specific page of the log.
 - Click **Previous** or **Next** to view the events recorded immediately before or after the events listed on the open page.
 - Click << to return to the first page or click >> to view the last page of the log.
- To see the listed events on one page, click **Launch Log in New Window** from the event log page to display a full-screen view of the log.



Note: In your browser's options, JavaScript must be enabled for you to use the **Launch Log in New Window** button.



You can also use FTP or Secure CoPy (SCP) to view the event log. See “How to use FTP or SCP to retrieve log files” on page 59.

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

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

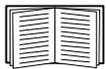


Note: Events are processed through the filter using **OR** logic.

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

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

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



To disable the logging of events based on their assigned severity level or their event category, see “Configuring by group” on page 77.

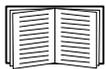
To configure reverse lookup (Logs > Events > reverse lookup):

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

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

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

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



See “How to use FTP or SCP to retrieve log files” on page 59.

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

Data log

Path: Logs > Data > *options*

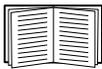
View a log of measurements about the UPS, the power input to the UPS, and the ambient temperature of the UPS and batteries. Each entry is listed by the date and time the data was recorded.

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

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



Note: In your browser's options, JavaScript[®] must be enabled for you to use the **Launch Log in New Window** button.



Alternatively, you can use FTP or SCP to view the data log. See “How to use FTP or SCP to retrieve log files” on page 59.

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

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

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

To delete the data log:

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

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

Define, in the **Log Interval** setting, how frequently data is sampled and stored in the data log, and view the calculation of how many days of data the log can store, based on the interval you selected. When the log is full, the oldest entries are deleted. To avoid automatic deletion of older data, enable and configure data log rotation, described in the next section.

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

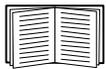
Set up a password-protected data log repository on a specified FTP server. Enabling rotation causes the contents of the data log to be appended to the file you specify by name and location. Updates to this file occur at the upload interval you specify.

Parameter	Description
Data Log Rotation	Enable or disable (the default) data log rotation.
FTP Server Address	The location of the FTP server where the data repository file is stored.

Parameter	Description
User Name	The user name required to send data to the repository file. This user must also be configured to have read and write access to the data repository file and the directory (folder) in which it is stored.
Password	The password required to send data to the repository file.
File Path	The path to the repository file.
Filename	The name of the repository file (an ASCII text file), e.g. <code>data1og.txt</code> . Any new data is appended to this file, it does not overwrite it.
Unique Filename	Select this check box to save the log as <code>mmddyyyy_<filename>.txt</code> . Filename is derived from what you specified in the Filename field above. Any new data is appended to the file but each day has its own file.
Delay <i>X</i> hours between uploads.	The number of hours between uploads of data to the file.
Upload every <i>X</i> minutes	The number of minutes between attempts to upload data to the file after an upload failure.
Up to <i>X</i> times	The maximum number of times the upload will be attempted after an initial failure.
Until Upload Succeeds	Attempt to upload the file until the transfer is completed.

To resize the data log (Logs > Data > size):

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



See “How to use FTP or SCP to retrieve log files” on page 59.

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

How to use FTP or SCP to retrieve log files

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

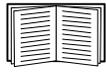
- The file reports all events or data recorded since the log was last deleted or (for the data log) truncated because it reached maximum size.
- The file includes information that the event log or data log does not display.
 - The version of the file format (first field)
 - The date and time the file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



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

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

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



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

To use SCP to retrieve the files. Enable SSH on the NMC.

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

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

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

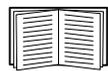
```
scp username@hostname_or_ip_address:data.txt ./data.txt
```

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

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

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

```
ftp>open ip_address port_number
```



To set a non-default port value to enhance security for the FTP Server, see “FTP Server” on page 75. You can specify any port from 5001 to 32768.

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

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

or

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

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

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

or

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

You will not be asked to confirm the deletion.

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

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

Administration: Security

Local Users

Setting user access

Path: Administration > Security > Local Users > options

The Administrator user account always has access to the UPS Network Management Card 2 (NMC).

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

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



For information on the permissions granted to each account type (Administrator, Device User, and Read-Only User), see “Types of user accounts” on page 3.

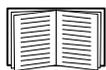
Account Type	Default User Name	Default Password	Permitted Access
Administrator	apc	apc	Web interface and command line interface
Device User	device	apc	
Read-Only User	readonly	apc	Web interface only

Remote Users

Authentication

Path: Administration > Security > Remote Users > Authentication Method

Use this option to select how to administer remote access to the NMC.



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

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

- When a user accesses the Network Management Card or other network-enabled device that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user’s permission level.
- RADIUS user names used with the Network Management Card are limited to 32 characters.

Select one of the following:

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



Note: If **RADIUS Only** is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, remote access is unavailable to all users. You must use a serial connection to the command line interface and change the **access** setting to **local** or **radiusLocal** to regain access. For example, the command to change the access setting to **local** would be:

```
radius -a local
```

RADIUS

Path: Administration > Security > Remote Users > RADIUS

Use this option to do the following:

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

RADIUS Setting	Definition
RADIUS Server	The server name or IP address (IPv4 or IPv6) of the RADIUS server. Click on a link to configure the server. NOTE: RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.
Secret	The shared secret between the RADIUS server and the NMC.
Timeout	The time in seconds that the NMC waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path.

Configuring the RADIUS Server

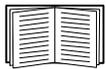
Summary of the configuration procedure

You must configure your RADIUS server to work with the NMC.



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

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



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

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

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

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

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

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

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

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

Supported RADIUS servers

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

Inactivity Timeout

Path: Administration > Security > Auto Log Off

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



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

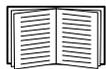
Administration: Network Features

TCP/IP and Communication Settings

TCP/IP settings

Path: Administration > Network > TCP/IP > IPv4 settings

The **TCP/IP** option on the left navigation menu, selected by default when you choose **Network** on the top menu bar, displays the current IPv4 address, subnet mask, default gateway, MAC address, and boot mode of the UPS Network Management Card 2 (NMC).



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

Setting	Description
Enable	Enable or disable IPv4 with this check box.
Manual	Configure IPv4 manually by entering the IP address, subnet mask, and default gateway.
BOOTP	<p>A BOOTP server provides the TCP/IP settings. At 32-second intervals, the NMC requests network assignment from any BOOTP server:</p> <ul style="list-style-type: none">• If the NMC receives a valid response, it starts the network services.• If the NMC finds a BOOTP server, but a request to that server fails or times out, the NMC stops requesting network settings until it is restarted.• By default, if previously configured network settings exist, and the NMC receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible. <p>The default values for these three settings on the configuration pages generally do not need to be changed:</p> <ul style="list-style-type: none">• Vendor Class: APC• Client ID: The MAC address of the Network Management Card, which uniquely identifies it on the local area network (LAN)• User Class: The name of the application firmware module
DHCP	<p>The default setting. At 32-second intervals, the NMC requests network assignment from any DHCP server.</p> <ul style="list-style-type: none">• If the NMC receives a valid response, it does not (as previously) require the APC cookie from the DHCP server in order to accept the lease and start the network services.• If the NMC finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted¹.• Require vendor specific cookie to accept DHCP Address: By selecting this check box, you can require the DHCP server to provide a cookie which supplies information to the NMC.

DHCP response options

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

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

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

Option 43 communicates to the NMC that a DHCP server is configured to service devices.

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

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

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

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

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

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

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

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

Ping Response

Path: Administration > Network > Ping Response

Select the Enable check box for **IPv4 Ping Response** to allow the Network Management Card 2 to respond to network pings. Clear the check box to disable an NMC response. This does not apply to IPv6.

Port Speed

Path: Administration > Network > Port Speed

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

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

DNS

Path: Administration > Network > DNS > options

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

- Select **Primary DNS Server** or **Secondary DNS Server** to specify the IPv4 or IPv6 addresses of the primary and optional secondary DNS server. For the NMC to send e-mail, you must at least define the IP address of the primary DNS server.
 - The NMC waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the NMC does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the NMC or on a nearby segment (but not across a wide-area network [WAN]).
 - After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for that computer.
- **Host Name:** After you configure a host name here and a domain name in the **Domain Name** field, users can enter a host name in any field in the NMC interface (except e-mail addresses) that accepts a domain name.
- **Domain Name (IPv4):** You need to configure the domain name here only. In all other fields in the NMC interface (except e-mail addresses) that accept domain names, the NMC adds this domain name when only a host name is entered.
 - To override all instances of the expansion of a specified host name by the addition of the domain name, set the domain name field to its default, `somedomain.com`, or to `0.0.0.0`.
 - To override the expansion of a specific host name entry (for example, when defining a trap receiver), include a trailing period. The NMC recognizes a host name with a trailing period (such as `mySnmpServer.`) as if it were a fully-qualified domain name and does not append the domain name.
- **Domain Name (IPv6):** Specify the IPv6 domain name here.
- Select **test** to send a DNS query that tests the setup of your DNS servers:
 - As **Query Type**, select the method to use for the DNS query, see table below
 - As **Query Question**, identify the value to be used for the selected query type:

Query Type Selected	Query Question to Use
by Host	The host name
by FQDN	The fully-qualified domain name, <code>my_server.my_domain</code> .
by IP	The IP address of the server
by MX	The Mail Exchange address

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

Web

Path: Administration > Network > Web > options

Option	Description
access	<p>To activate changes to any of these selections, log off from the NMC:</p> <ul style="list-style-type: none">• Disable: Disables access to the Web interface. (To re-enable access, log in to the command line interface, then type the command <code>http -S enable</code>. For HTTPS access, type <code>https -S enable</code>.)• Enable HTTP (the default): Enables Hypertext Transfer Protocol (HTTP), which provides Web access by user name and password, but does not encrypt user names, passwords, and data during transmission.• Enable HTTPS: Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL). SSL encrypts user names, passwords, and data during transmission, and authenticates the NMC by digital certificate. When HTTPS is enabled, your browser displays a small lock icon. <p>See “Creating and Installing Digital Certificates” in the <i>Security Handbook</i> on the Network Management Card <i>Utility</i> CD to choose among the several methods for using digital certificates.</p> <p>HTTP Port: The TCP/IP port (80 by default) used to communicate by HTTP with the NMC.</p> <p>HTTPS Port: The TCP/IP port (443 by default) used to communicate by HTTPS with the NMC.</p> <p>For either of these ports, you can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114:</p> <pre>http://152.214.12.114:5000 https://152.214.12.114:5000</pre>

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

Console

Path: Administration > Network > Console > *options*

Option	Description
access	<p>Choose one of the following for access by Telnet or Secure SHell (SSH):</p> <ul style="list-style-type: none"> • Disable: Disables all access to the command line interface. • Enable Telnet (the default): Telnet transmits user names, passwords, and data without encryption. • Enable SSH: SSH transmits user names, passwords, and data in encrypted form, providing protection from attempts to intercept, forge, or alter data during transmission. <p>Configure the ports to be used by these protocols:</p> <ul style="list-style-type: none"> • Telnet Port: The Telnet port used to communicate with the NMC (23 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) or a space, as required by your Telnet client program, to specify the non-default port. For example, for port 5000 and an IP address of 152.214.12.114, your Telnet client requires one of the these commands: <pre>telnet 152.214.12.114:5000 telnet 152.214.12.114 5000</pre> • SSH Port: The SSH port used to communicate with the NMC (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port.
ssh host key	<p>Status indicates the status of the host key (private key):</p> <ul style="list-style-type: none"> • SSH Disabled: No host key in use: When disabled, SSH cannot use a host key. • Generating: The NMC is creating a host key because no valid host key was found. • Loading: A host key is being activated on the NMC. • Valid: One of the following valid host keys is in the /ssh directory (the required location on the Network Management Card): <ul style="list-style-type: none"> • A 1024-bit or 2048-bit host key created by the Security Wizard • A 2048-bit RSA host key generated by the Network Management Card <p>Add or Replace: Browse to and upload a host key file created by the Security Wizard.</p> <p>To use the Security Wizard, see the <i>Security Handbook</i> on the Network Management Card <i>Utility CD</i>.</p> <p>NOTE: To reduce the time required to enable SSH, create and upload a host key in advance. If you enable SSH with no host key loaded, the NMC takes up to one minute to create a host key, and the SSH server is not accessible during that time.</p> <p>Remove: Remove the current host key.</p>



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

SNMP

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

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



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

SNMPv1

Path: Administration > Network > SNMPv1 > options

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

SNMPv3

Path: Administration > Network > SNMPv3 > options

For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users. An SNMPv3 user must have a user profile assigned in the MIB software program to perform GETs and SETs, browse the MIB, and receive traps.



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

The NMC supports SHA or MD5 authentication and AES or DES encryption.

Option	Description
access	SNMPv3 Access: Enables SNMPv3 as a method of communication with this device.
user profiles	<p>By default, lists the settings of four user profiles, configured with the user names apc snmp profile1 through apc snmp profile4, and no authentication and no privacy (no encryption). To edit the following settings for a user profile, click a user name in the list.</p> <p>User Name: The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters.</p> <p>Authentication Passphrase: A phrase of 15 to 32 ASCII characters (<code>apc auth passphrase</code>, by default) that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time.</p> <p>Privacy Passphrase: A phrase of 15 to 32 ASCII characters (<code>apc crypt passphrase</code>, by default) that ensures the privacy of the data (by means of encryption) that an NMS is sending to this device or receiving from this device through SNMPv3.</p> <p>Authentication Protocol: The implementation of SNMPv3 supports SHA and MD5 authentication. Authentication will not occur unless an authentication protocol is selected.</p> <p>Privacy Protocol: The implementation of SNMPv3 supports AES and DES as the protocols for encrypting and decrypting data. Privacy of transmitted data requires that a privacy protocol is selected and that a privacy passphrase is provided in the request from the NMS. When a privacy protocol is enabled but the NMS does not provide a privacy passphrase, the SNMP request is not encrypted.</p> <p>NOTE: You cannot select the privacy protocol if no authentication protocol is selected.</p>

Option	Description
access control	<p>You can configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles, but you can edit these settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks.</p> <ul style="list-style-type: none"> • If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device. • If you configure multiple access entries for one user profile, the limit of four entries requires that one or more of the other user profiles must have no access control entry. If no access control entry is listed for a user profile, no NMS that uses that profile has any access to this device. <p>To edit the access control settings for a user profile, click its user name.</p> <p>Access: Mark the Enable checkbox to activate the access control specified by the parameters in this access control entry.</p> <p>User Name: From the drop-down list, select the user profile to which this access control entry will apply. The choices available are the four user names that you configure through the user profiles option on the left navigation menu.</p> <p>NMS IP/Host Name: The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows:</p> <ul style="list-style-type: none"> • 149.225.12.255: Access only by an NMS on the 149.225.12 segment. • 149.225.255.255: Access only by an NMS on the 149.225 segment. • 149.255.255.255: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

FTP Server

Path: Administration > Network > FTP Server

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

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



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

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



For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available on the Network Management Card *Utility* CD or from the APC Web site.

Administration: Notification

Event Actions

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

Types of notification

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

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



You can also log system performance data to use for device monitoring. See “Data log” on page 57 for information on how to configure and use this data logging option.

- Queries (SNMP GETs)



For more information, see “SNMP” on page 73. SNMP enables an NMS to perform informational queries. For SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without the risk of allowing remote configuration changes.

Configuring event actions

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

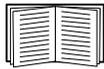
Parameter	Description
Delay x time before sending	If the event persists for the specified time, notification is sent. If the condition clears before the time expires, no notification is sent.
Repeat at an interval of x time	The notification is sent at the specified interval (e.g., every 2 minutes).
Up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

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

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



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



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

- "Identifying Syslog servers" on page 81
- "E-mail recipients" on page 78
- "Trap Receivers" on page 79

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

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

Active, Automatic, Direct Notification

E-mail notification

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

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

- The IP addresses of the primary and, optionally, the secondary Domain Name System (DNS) servers. (See “DNS” on page 69.)
- The IP address or DNS name for **SMTP Server** and **From Address**. (See “SMTP” on page 78.)
- The e-mail addresses for a maximum of four recipients. (See “E-mail recipients” on page 78.)



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

SMTP.

Path: Administration > Notification > E-mail > server

Setting	Description
Local SMTP Server	The IPv4/ IPv6 address or DNS name of the local SMTP server. NOTE: This definition is required only when SMTP Server is set to Local . See “E-mail recipients” on page 78.
From Address	The contents of the From field in e-mail messages sent by the NMC: <ul style="list-style-type: none">• In the format <i>user@ [IP_address]</i> (if an IP address is specified as Local SMTP Server)• In the format <i>user@domain</i> (if DNS is configured and the DNS name is specified as Local SMTP Server) in the e-mail messages. NOTE: The local SMTP server may require that you use a valid user account on the server for this setting. See the server’s documentation.

E-mail recipients.

Path: Administration > Notification > E-mail > recipients

Identify up to four e-mail recipients.

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

Setting	Description
E-mail Generation	Enables (default) or disables sending e-mail to the recipient.
SMTP Server	Select one of the following methods for routing e-mail: <ul style="list-style-type: none"> • Local: Through the site-local SMTP server. This recommended setting ensures that the e-mail is sent using the site-local SMTP server. • Recipient: Through the recipient's SMTP server. The NMC performs an MX record look-up on the recipients e-mail address and uses that as its SMTP server.
Format	The long format contains Name, Location, Contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.
Language	Chose a language from the drop-down list and any mails will be sent in that language. It is possible to use different languages for different users. See “Adding and Changing Language Packs” on page 101.
User Name Password Confirm Password	If your mail server requires authentication, type your user name and password here. This performs a simple authentication, not SSI.
Port	The SMTP port number, with a default of 25.

E-mail test.

Path: Administration > Notification > E-mail > test

Send a test message to a configured recipient.

SNMP traps

Trap Receivers.

Path: Administration > Notification > SNMP Traps > trap receivers

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

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

Item	Definition
Trap Generation	Enable (the default) or disable trap generation for this trap receiver.
NMS IP/Host Name	The IPv4/ IPv6 address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.

Item	Definition
Language	Chose a language from the drop-down list. This can differ from the UI and from other trap receivers.

SNMPv1 option.

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

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



See “SNMPv3” on page 74 for information on creating user profiles and selecting authentication and encryption methods.

SNMP Trap Test

Path: Administration > Notification > SNMP Traps > test

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

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

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

Remote Monitoring Service

Path: Administration > Notification > Remote Monitoring

The Remote Monitoring Service (RMS) is an optional service that monitors your system from a remote operation center 24 hours a day, 7 days a week, and notifies you of device and system events.



To purchase the RMS service, contact your vendor or click on the link on the top part of this screen page: **RMS Web site**.

Registration. To activate RMS for the NMC, select **Enable Remote Monitoring Service.**, choose between **Register Company and Device** and **Register Device Only**, complete the form, and click **Send RMS Registration**.

Use the **Reset Remote Monitoring Service Registration** check box to discontinue the service, whether permanently or temporarily (for example, if you are moving an NMC).

Syslog

Path: Logs > Syslog > *options*

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



This user's guide does not describe Syslog or its configuration values in detail. See [RFC3164](#) for more information about Syslog.

Identifying Syslog servers.

Path: Logs > Syslog > servers

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

Syslog settings.

Path: Logs > Syslog > settings

Setting	Definition
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the NMC's Syslog messages (User , by default). NOTE: User best defines the Syslog messages sent by the NMC. Do not change this selection unless advised to do so by the Syslog network or system administrator.

Setting	Definition
Severity Mapping	<p>Maps each severity level of NMC or Environment events to available Syslog priorities. You should not need to change the mappings.</p> <p>The following definitions are from RFC3164:</p> <ul style="list-style-type: none"> • Emergency: The system is unusable • Alert: Action must be taken immediately • Critical: Critical conditions • Error: Error conditions • Warning: Warning conditions • Notice: Normal but significant conditions • Informational: Informational messages • Debug: Debug-level messages <p>Following are the default settings for the Local Priority settings:</p> <ul style="list-style-type: none"> • Severe is mapped to Critical • Warning is mapped to Warning • Informational is mapped to Info <p>NOTE: To disable Syslog messages, see “Configuring event actions” on page 76.</p>

Syslog test and format example.

Path: Logs > Syslog > test

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

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

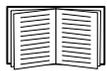
For example, `APC: Test Syslog` is valid.

Administration: General Options

Identification

Path: Administration > General > Identification

Define the **Name** (the device name), **Location** (the physical location), and **Contact** (the person responsible for the device) used by InfraStruxure Central, InfraStruxure Manager, and the SNMP agent of the UPS Network Management Card 2 (NMC). These settings are the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifiers (OIDs).



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

The **Name** and **Location** fields also identify the device when you register for the Remote Monitoring Service. See “Remote Monitoring Service” on page 80 for more information.

Set the Date and Time

Mode

Path: Administration > General > Date & Time > mode

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

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



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

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

Daylight saving

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

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

When customizing Daylight Saving Time (DST):

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

Format

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

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

Use an .ini File

Path: Administration > General > User Config File

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

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



To retrieve and customize the file of a configured NMC, see “How to Export Configuration Settings” on page 91.

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

Event Log, Temperature Units, Language, and Logon Page

Path: Administration > General > Preferences

Color-code event log text

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

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

Change the default temperature scale

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

Specify the UI language

You can specify the default language for the user interface with the **Language** field. This can be set when you log on also. From the drop-down box, select one of the languages displayed.



Note: You can also specify different languages for e-mail recipients and SNMP trap receivers. See “E-mail recipients” on page 78 and “Trap Receivers” on page 79.

Specify a default logon page

Configure the Web page that will display by default when you log on.

Reset the Network Management Card 2

Path: Administration > General > Reset/Reboot

Action	Definition
Reboot Management Interface	Restarts the interface of the NMC.
Reset All ¹	Clear the Exclude TCP/IP check box to reset all configuration values; mark the Exclude TCP/IP check box to reset all values except TCP/IP
Reset Only ¹	TCP/IP settings: Set TCP/IP Configuration to DHCP & BOOTP , its default setting, requiring that the NMC receive its TCP/IP settings from a DHCP or BOOTP server. See “TCP/IP and Communication Settings” on page 66.
	Event configuration: Reset all changes to event configuration, by event and by group, to their default settings.
	UPS to Defaults: Reset only UPS settings, not network settings, to their defaults.
	Lost Environmental Communication Alarms: Clear any environmental alarms that are caused by lost communication with an external sensor. For example, if a temperature sensor is disconnected and therefore causes an alarm, resetting lost environmental alarms returns the alarm status for that sensor to Normal. NOTE: To clear alarms for a sensor that is connected to the universal sensor port of an AP9631 NMC, reconnect the sensor or restart the NMC.
	Control Policy: Reset the settings that define how the NMC will respond to alarms that are detected at the Dry Contact I/O Accessory.
1. Resetting may take up to a minute. The UPS name will not be reset.	

Configure Links

Path: Administration > General > Quick Links

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

By default, these links access the following Web pages:

- **Link 1:** the Knowledge Base page of the APC Web site
- **Link 2:** the Product Information page of the APC Web site
- **Link 3:** the downloads page of the APC Web site

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

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

About the Network Management Card 2

Path: Administration > General > About

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

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

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

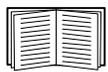
Device IP Configuration Wizard

Capabilities, Requirements, and Installation

How to use the Wizard to configure TCP/IP settings

The Device IP Configuration Wizard configures the IP address, subnet mask, and default gateway of one or more Network Management Cards or network-enabled devices (devices containing an embedded UPS Network Management Card 2 (NMC)). You can use the Wizard in either of the following ways:

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



For detailed information on the Wizard, see the Knowledge Base on the support page of the **APC** website and search for 3061 (the ID of the relevant article).

To use the DHCP Option 12 (AOS 5.1.5 or higher), see Knowledge Base ID 8853.

System requirements

The Wizard runs on Microsoft Windows 2000, Windows Server[®] 2003, and on both 32- and 64-bit versions of Windows XP, Windows Vista, Windows 2008, and Windows 7 operating systems.

Installation

To install the Wizard from the *Utility* CD:

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

To install the Wizard from a downloaded executable file:

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

Use the Wizard

Most software firewalls must be temporarily disabled for the Wizard to discover unconfigured Network Management Cards.

Launch the Wizard

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

Configure the basic TCP/IP settings remotely

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

1. Contact your network administrator to obtain valid TCP/IP settings.
2. If you are configuring multiple unconfigured NMCs or network-enabled devices, obtain the MAC address of each one to identify it when the Wizard discovers it. (The Wizard displays the MAC address on the screen on which you then enter the TCP/IP settings.)
 - For an NMC that you install, the MAC address is on a label on the bottom of the card.
 - For a network-enabled device (with an embedded NMC), the MAC address is on a label on the device.
 - You can also obtain the MAC address from the Quality Assurance slip that came with the NMC or device.

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

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

On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the NMC or device after the Wizard transmits the settings.

4. Click **Finish** to transmit the settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
5. If the Wizard finds another unconfigured NMC or device, it displays the screen to enter TCP/IP settings. Repeat this procedure beginning at step 3, or to skip the NMC or device whose MAC address is currently displayed, click **Cancel**.

Configure or reconfigure the TCP/IP settings locally

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the provided serial configuration cable (part number 940-0299) from an available communications port on your computer to the serial port of the NMC or device. Make sure no other application is using the computer port.
3. From the **Start** menu, launch the Wizard application.
4. If the Network Management Card or network-enabled device is not configured, wait for the Wizard to detect it. Otherwise, click **Next >**.
5. Select **Locally (through the serial port)**, and click **Next >**.
6. Enter the system IP, subnet mask, and default gateway for the NMC or device, and click **Next >**.
7. On the **Transmit Current Settings Remotely** screen, if you select **Start a Web browser when finished**, the default Web browser connects to the NMC or device after the Wizard transmits the settings.
8. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
9. If you selected **Start a Web browser when finished** in step 6, you can now configure other parameters through the Web interface of the NMC or device.

How to Export Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

An Administrator can retrieve the .ini file of a UPS Network Management Card 2 (NMC) and export it to another NMC or to multiple NMCs.

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

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

Contents of the .ini file

The config.ini file you retrieve from an NMC contains the following:

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

Detailed procedures

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

1. If possible, use the interface of an NMC to configure it with the settings to export. Directly editing the .ini file risks introducing errors.
2. To use FTP to retrieve config.ini from the configured NMC:

- a. Open a connection to the NMC, using its IP address:

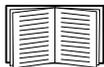
```
ftp> open ip_address
```

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

- c. Retrieve the config.ini file containing the NMC's settings:

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

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



To retrieve configuration settings from multiple NMCs and export them to other NMCs, see *Release Notes: ini File Utility, version 1.0*, available on the Network Management Card Utility CD and at www.apc.com.

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

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

```
NTPEnable=enabled
```

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

Transferring the file to a single NMC. To transfer the `.ini` file to another Network Management Card, do either of the following:

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

```
ftp> open ip_address
```

- b. Export the copy of the customized `.ini` file to the root directory of the receiving NMC:

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

Exporting the file to multiple NMCs. To export the `.ini` file to multiple Network Management Cards:

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



To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* on the Network Management Card *Utility* CD.

The Upload Event and Error Messages

The event and its error messages

The following event occurs when the receiving Network Management Card completes using the .ini file to update its settings.

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

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

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

Messages in config.ini

A device associated with the NMC from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the device (such as a UPS) is not present or is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values. For example:

```
UPS not discovered
```

```
IEM not discovered
```

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

Errors generated by overridden values

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

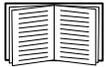


See “Contents of the .ini file” on page 91 for information about which values are overridden.

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

Related Topics

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



See “Device IP Configuration Wizard” on page 88.

File Transfers

How to Upgrade Firmware

Benefits of upgrading firmware

When you upgrade the firmware on the UPS Network Management Card 2 (NMC):

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

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

Firmware files (Network Management Card 2)

A firmware version consists of three modules, and the must be upgraded in this order:

- a boot monitor (**bootmon**) module
- an American Power Conversion Operating System (**AOS**) module
- an **application** module

Each module contains one or more Cyclical Redundancy Checks (CRCs) to protect its data from corruption during transfer.

The AOS, the application, and the boot monitor module files share the same basic format:

```
apc_hardware-version_type_firmware-version.bin
```

- *apc*: Indicates the context.
- *hardware-version*: *hw0x* identifies the hardware version on which you can use this binary file.
- *type*: Identifies the module.
- *version*: The version number of the file.
- *bin*: Indicates that this is a binary file.



Note: If you are unsure whether to upgrade any particular module, then upgrading all three is recommended.

Obtain the latest firmware version



Note: In a manual upgrade, you can skip the bootmon installation if there are no updates. (With the NMC2 Firmware Upgrade Utility, any bootmon update is automatic).

NMC2 Firmware Upgrade Utility for Microsoft Windows systems. The NMC2 Firmware Upgrade Utility automates the transferring of the firmware modules on any supported Windows operating system. You can obtain the latest version of the utility at no cost from www.apcc.com/tools/download. At this Web page, find the latest firmware release for your product and, included in it, the Utility.

Never use an Upgrade Utility designated for one product to upgrade the firmware of another product.

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

To extract the firmware files:

1. Run the NMC2 Firmware Upgrade Utility.
2. At the prompts, click **Next>**, and then specify the directory location to which the files will be extracted.
3. When the **Extraction Complete** message displays, close the dialog box.

Firmware File Transfer Methods



Warning: Upgrade the bootmon module first, then the AOS module, and finally, the application module.

To upgrade the firmware of an NMC, use one of these methods:

- From a networked computer running a Microsoft Windows operating system, use the NMC2 Firmware Upgrade Utility downloaded from the APC Web site.



Note: The utility only works with an NMC that has an IPv4 address.

- From a networked computer on any supported operating system, use FTP or SCP to transfer the individual AOS and application firmware modules.
- For a Network Management Card that is not on your network, use XMODEM through a serial connection to transfer the individual firmware modules from your computer to the NMC.
- Use a USB drive to transfer the individual firmware modules from your computer to the NMC. (AP9631 only)

Use FTP or SCP to upgrade one Network Management Card 2

FTP. To use FTP to upgrade one NMC over the network:

- The NMC must be connected to the network, and its system IP, subnet mask, and default gateway must be configured.
- The FTP server must be enabled at the NMC.
- The firmware files must be extracted from the NMC2 Firmware Upgrade Utility (see “To extract the firmware files:”).

To transfer the files (this procedure assumes bootmon does not need updating):

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

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

For the listed files below, *nnn* represents the firmware version number:

- `apc_hw05_bootmon_nnn.bin`
- `apc_hw05_aos_nnn.bin`
- `apc_hw05_application_nnn.bin`

2. Open an FTP client session:

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

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

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

```
ftp> open 150.250.6.10 21000
```

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

4. Log on as Administrator; **apc** is the default user name and password.

5. Upgrade the AOS. (In the example, *xxx* is the firmware version number):

```
ftp> bin
ftp> put apc_hw05_aos_xxx.bin
```

6. When FTP confirms the transfer, type `quit` to close the session.

7. After 20 seconds, repeat step 2 through step 6. In step 5, use the application module file name.

SCP. To use Secure CoPy (SCP) to upgrade firmware for the NMC (this procedure assumes bootmon does not need updating):

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

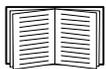
```
scp apc_hw05_aos_xxx.bin apc@158.205.6.185:apc_hw05_aos_xxx.bin
```

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

How to upgrade multiple Network Management Cards

NMC2 Firmware Upgrade Utility. Use this for multiple firmware updates in IPv4 if you have Windows. The utility records all upgrade steps in a log as a good reference to validate the upgrade.

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



See *Release Notes: ini File Utility, version 1.0*, available on the Network Management Card Utility CD.

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

Using the NMC2 Firmware Upgrade Utility for multiple upgrades

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

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

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

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

Use XMODEM to upgrade one NMC

To use XMODEM to upgrade one NMC that is not on the network, you must extract the firmware files from the NMC2 Firmware Upgrade Utility (see “To extract the firmware files:”).

To transfer the files (this procedure assumes bootmon does not need updating):

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect the provided serial configuration cable (part number 940-0299) to the selected port and to the serial port at the NMC.
3. Run a terminal program such as HyperTerminal, and configure the selected port for 57600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press the **Reset** button on the NMC, then immediately press the **Enter** key twice, or until the Boot Monitor prompt displays: `BM>`
5. Type `XMODEM`, then press `ENTER`.
6. From the terminal program’s menu, select `XMODEM`, then select the binary AOS firmware file to transfer using `XMODEM`. After the `XMODEM` transfer is complete, the Boot Monitor prompt returns.
7. To install the application module, repeat step 5 and step 6. In step 6, use the application module file name.
8. Type `reset` or press the Reset button to restart the NMC.



For information about the format used for firmware modules, see “Firmware files (Network Management Card 2)” on page 95.

Use a USB drive to transfer the files (AP9631 only)



Note: Before starting the transfer, make sure the USB drive is formatted in FAT32.

1. Download the update files and unzip them.
2. Create a folder named **apcfirm** on the USB flash drive.
3. Place the extracted files in the `apcfirm` directory.
4. Use a text editor to create a file named **upload.rcf**. (The file extension must be `.rcf`, not `.txt` for example.)
5. In `upload.rcf`, add a line for each firmware module that you want to upgrade. For example, to upgrade to **bootmon** version 1.0.2, **AOS** v5.1.5 and Smart-UPS **application** version v5.1.4:

```
BM=apc_hw05_bootmon_102.bin  
AOS=apc_hw05_aos_515.bin  
APP=apc_hw05_sumx_514.bin
```
6. Place `upload.rcf` in the `apcfirm` folder on the flash drive.
7. Insert the USB drive into any USB port on the NMC.
8. Reset the NMC and wait for the card to reboot fully.
9. Check that the upgrade was completed successfully using the procedures in “Verifying Upgrades and Updates” on page 100.

Verifying Upgrades and Updates

Verify the success or failure of the transfer

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

Last Transfer Result codes

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

Verify the version numbers of installed firmware

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

Adding and Changing Language Packs

Using the Network Management Card 2 language pack files you can display the user interface in different languages. Each language pack contains up to five languages (this is why the **Language** drop-down box has up to five languages to choose from when you log on).

The user interface has nine languages available in all: French, Italian, German, Spanish, Brazilian Portuguese, Russian, Korean, Japanese, and Simplified Chinese.

The language pack files are available on the Network Management Card firmware download area on the APC website, www.apc.com.

The downloaded files all have an .lpk extension and the file naming convention is:

```
<app name>_<app version>_<language codes>.lpk
```

For example, for a Symmetra 3-phase application, the filename would be something like:

```
sy3p_510_esESzhCnjaJAptBrkoKo.lpk
```

```
where esESzhCnjaJAptBrkoKo
```

```
represents Spanish, Chinese, Japanese, Portuguese Brazilian, and Korean.
```

You might want to change the user interface language to one that is not currently available to you. To do this, you need to download the language pack from the website, and follow these steps:

1. Connect to your NMC using FTP.
2. Change to the lang folder of the NMC:

```
cd lang
```
3. Transfer the required language pack to the NMC:

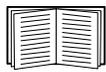
```
put <full path/language pack name>.lpk
```
4. When the file finishes the transfer, log off FTP and the NMC will reboot.
5. When the reboot is complete, the new language pack is ready for use.



Note: Any current language pack on the card is **deleted** before the new pack is transferred. Any problem with the pack transfer leaves the NMC with no language pack. Only English is available in that circumstance. If this happens, try re-loading the new language pack.

Troubleshooting

Network Management Card Access Problems



For problems that are not described here, see the troubleshooting flowcharts on the Network Management Card *Utility* CD. Click the **Troubleshooting** link in the CD interface.

If the problem still persists, see See “Appendix B: Getting Help and Technical Assistance” on page 106..

Problem	Solution
Unable to ping the NMC	<p>If the NMC’s Status LED is green, try to ping another node on the same network segment as the NMC. If that fails, it is not a problem with the NMC. If the Status LED is not green, or if the ping test succeeds, perform the following checks:</p> <ul style="list-style-type: none">• Verify that the NMC is properly seated in the UPS.• Verify all network connections.• Verify the IP addresses of the NMC and the NMS.• If the NMS is on a different physical network (or subnetwork) from the NMC, verify the IP address of the default gateway (or router).• Verify the number of subnet bits for the NMC’s subnet mask.
Cannot allocate the communications port through a terminal program	<p>Before you can use a terminal program to configure the NMC, you must shut down any application, service, or program using the communications port.</p>
Cannot access the command line interface through a serial connection	<p>Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.</p>
Cannot access the command line interface remotely	<ul style="list-style-type: none">• Make sure you are using the correct access method, Telnet or Secure SHell (SSH). An Administrator can enable these access methods. By default, Telnet is enabled. Enabling SSH automatically disables Telnet.• For SSH, the NMC may be creating a host key. The NMC can take up to one minute to create the host key, and SSH is inaccessible for that time.
Cannot access the Web interface	<ul style="list-style-type: none">• Verify that HTTP or HTTPS access is enabled.• Make sure you are specifying the correct URL — one that is consistent with the security system used by the NMC. SSL requires https, not http, at the beginning of the URL.• Verify that you can ping the NMC.• Verify that you are using a Web browser supported for the NMC. See “Supported Web browsers” on page 29.• If the NMC has just restarted and SSL security is being set up, the NMC may be generating a server certificate. The NMC can take up to one minute to create this certificate, and the SSL server is not available during that time.

SNMP Issues

Problem	Solution
Unable to perform a GET	<ul style="list-style-type: none"> • Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3). • Use the command line interface or Web interface to ensure that the NMS has access. See “SNMP” on page 73.
Unable to perform a SET	<ul style="list-style-type: none"> • Verify the read/write (SET) community name (SNMPv1) or the user profile configuration (SNMPv3). • Use the command line interface or Web interface to ensure that the NMS has write (SET) access (SNMPv1) or is granted access to the target IP address through the access control list (SNMPv3). See “SNMP” on page 73.
Unable to receive traps at the NMS	<ul style="list-style-type: none"> • Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the NMS as a trap receiver. • For SNMP v1, query the mconfigTrapReceiverTable MIB OID 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 either is not correct, use SETs to the mconfigTrapReceiverTable OIDs, or use the command line interface or Web interface to correct the trap receiver definition. • For SNMPv3, check the user profile configuration for the NMS, and run a trap test. <p>See “SNMP” on page 73, “Trap Receivers” on page 79, and “SNMP Trap Test” on page 80.</p>
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.

Synchronization Problems

Problem	Solution
A Synchronized Control Group member does not participate in a synchronized action.	Make sure the group member’s status is set to Enabled . Also check the group member’s battery capacity, if the synchronized action required UPSs to turn on.
An attempt to add a member to a Synchronized Control Group fails.	The values for Multicast IP Address , Synchronized Control Group Number , and firmware version must match those of other members of the group.

Appendix A: List of Supported Commands

?	ping
about	[<IP address or DNS name>]
alarmcount	portspeed
[-p [all warning critical]]	[-s [auto 10H 10F 100H 100F]]
boot	prompt
[-b <dhcp bootp manual>]	[-s [long short]]
[-c <dhcp cookie> [enable disable]]	quit
[-v <vendor class>]	radius
[-i <client id>]	[-a <access> [local radiusLocal radius]]
[-u <user class>]	[-p# <server IP>]
cd	[-s# <server secret>]
console	[-t# <server timeout>]
[-S <disable telnet ssh>]	reboot
[-pt <telnet port #>]	resetToDef
[-ps <ssh port #>]	[-p [all keepip]]
[-b <baud rate> [2400 9600 19200 38400]]	snmp, snmp3
date	[-S [enable disable]]
[-d <“datestring”>]	system
[-t <00:00:00>]	[-n <system name>]
[-f [mm/dd/yy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd]]	[-c <system contact>]
[-z <time zone offset>]	[-l <system location>]
delete	tcpip
dir	[-S [enable disable]]
dns	[-i <IP address>]
[-OM [enable disable]]	[-s <subnet mask>]
[-p <primary DNS server>]	[-g <gateway>]
[-s <secondary DNS server>]	[-d <domain name>]
[-d <domain name>]	[-h <host name>]
[-n <domain name IPv6>]	tcpip6
[-h <host name>]	[-S [enable disable]]
eventlog	[-man [enable disable]]
exit	[-auto [enable disable]]
format	[-i <IPv6 address>]
ftp	[-g <IPv6 gateway>]
[-p <port number>]	[-d6 [router stateful stateless never]]
[-S <enable disable>]	uio
help	[-rc <dI> [open close]]
netstat	[-st <port # port #>]
ntp	[-disc <port # port #>]
[-OM [enable disable]]	ups
[-p <primary NTP server>]	[-c <off graceoff on reboot gracereboot
[-s <secondary NTP server>]	sleep gracesleep>]
	[-r <start stop>]
	[-s <start>]
	[-b <enter exit>]

[-o# <off | delayoff | on | delayon | reboot>]
[-os#]
[-st]
[-input [<phase#> | all] [voltage | current | frequency | all]]
[-bypass [<phase#> | all] [voltage | current | frequency | all]]
[-output [<phase#> | all] [voltage | current | frequency | load | percloud | pf | power | all]]
[-batt]
[-about]
[-al [c | w]]

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

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

xferINI

xferStatus

Appendix B: Getting Help and Technical Assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This section contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

Before You Call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Problem Determination and Service Guide* on the IBM Documentation CD that comes with your system.
- Go to the IBM support Web site at <http://www.ibm.com/systems/support/> to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the Documentation

Information about your IBM system and preinstalled software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to <http://www.ibm.com/systems/support/> and follow the instructions. Also, some documents are available through the IBM Publications Center at <http://www.ibm.com/shop/publications/order>.

Getting Help and Information from the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM systems, optional devices, services, and support. The address for IBM System x™ and xSeries® information is <http://www.ibm.com/systems/x/>. The address for IBM BladeCenter® information is <http://www.ibm.com/systems/bladecenter/>. The address for IBM IntelliStation® information is <http://www.ibm.com/intellistation/>. You can find service information for IBM systems and optional devices at <http://www.ibm.com/systems/support/>.

Software Service and Support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with System x and xSeries servers, BladeCenter products, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, see <http://www.ibm.com/services/sl/products/>.

For more information about Support Line and other IBM services, see <http://www.ibm.com/services/>, or see <http://www.ibm.com/planetwide/> for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware Service and Support

You can receive hardware service through your IBM reseller or IBM Services. To locate a reseller authorized by IBM to provide warranty service, go to <http://www.ibm.com/partnerworld/> and click **Find a Business Partner** on the right side of the page. For IBM support telephone numbers, see <http://www.ibm.com/planetwide/>. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan Product Service

IBM Taiwan product service contact information:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Appendix C: Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to this address:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk. IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Edition Notice

Third Edition (March 2011)
990-2234B

©Copyright International Business Machines Corporation 2004, 2009. All rights reserved.

©Copyright 2011 APC by Schneider Electric. All rights reserved.

Network M 89 anagement Card User's Guide

U.S. Government Users—Documentation related to restricted rights—Use, duplication, or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available at on the Web at “Copyright and trademark information” at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc., in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

APC, the APC logo, InfraStruXure, PowerChute, and PowerNet are trademarks of Schneider Electric Industries S.A.S., American Power Conversion Corporation, or their affiliated companies in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Important Notes

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven®, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Index

A

- About options
 - for information about the NMC, 87
 - for information about the UPS, 50
 - for information on environmental monitors, 54
- Access
 - enabling or disabling methods of access
 - to the command line interface, 72
 - to the Web interface, 70
 - priority for logging on, 3
 - to the command line interface
 - locally, 9
 - remotely, 8
 - troubleshooting, 102
- Administration
 - Network menu, 66
 - Notification menu, 76
- Alarm Status
 - output relay, 54
 - temperature and humidity, 52
- Alarm Status, input contacts, 53
- Apply Local Computer Time, 83
- Authenticating users through RADIUS, 62
- Authentication Traps setting, 80
- Automatic log-off for inactivity, 65

B

- Basic Low Battery Duration, 43
- Basic Signaling Shutdown, 42
- BOOTP
 - Status LED reporting BOOTP requests, 6

C

- Certificates, how to create, view, or remove, 71

- Command line interface
 - configuring access, 72
 - remote access, 8
- Community Name
 - for trap receivers, 80
 - verifying correct configuration, 103
- Configuration menu
 - outlet groups settings, 40
- Configuring
 - load-shedding, 40
 - RADIUS authentication, 63
 - shutdowns, 42
- Contact identification (whom to contact), 83
- Control actions, 36

D

- Data log
 - importing into spreadsheet, 59
 - Log Interval setting, 58
 - rotation (archiving), 58
 - using FTP or SCP to retrieve, 59
- Date & Time settings, 83
- Date format, configuring, 84
- Daylight saving time, 84
- Device IP Configuration Wizard
 - installation and system requirements, 88
 - using the wizard
 - for local configuration., 90
 - for remote configuration, 89

DHCP

- APC cookie, 67
- Status LED reporting DHCP requests, 6
- Diagnostics, 48
- Disable
 - e-mail to a recipient, 79
 - reverse lookup, 57
 - Telnet, 72

DNS

- query types, 69
- specifying DNS servers by IP

address, 69

E

- E-mail
 - configuring notification parameters, 78
 - configuring recipients, 78
 - test message, 79
 - using for paging, 78
- Enable
 - e-mail to a recipient, 79
 - reverse lookup, 57
 - Telnet, 72
 - versions of SSH, 72
- Error messages
 - from overridden values in .ini file, 94
- Ethernet port speed, 68
- Event actions, 76
 - configuring by event, 77
 - configuring by group, 77
- Event log
 - displaying and using, 56
 - errors from overridden values in .ini file, 94
 - using FTP del command, 60
 - using FTP or SCP to retrieve, 59
- event.txt file
 - contents, 59
 - importing into spreadsheet, 59
- Events for outlet groups, 42

F

- Facility Code (Syslog setting), 81
- Firmware
 - benefits of upgrading, 95
 - file transfer methods
 - automated upgrade tool, 95
 - FTP or SCP, 96
 - XMODEM, 98
 - obtaining the latest version, 95
 - upgrading multiple NMCs, 97
 - versions displayed on main

- screen, 9
- From Address (SMTP setting), 78
- FTP
 - server settings, 75
 - transferring firmware files, 96
 - using to retrieve event or data log, 59

G

- GET commands, troubleshooting, 103

H

- Help
 - on configuring UPS power options, 40, 42
- Host keys
 - adding or replacing, 72
 - status, 72
- Host name of trap receivers, 79
- Hysteresis, 52

I

- Identification (Name, Location, and Contact)
 - in Web interface, 83
- Inactivity timeout, 65
- ini files, *See* User configuration files
- Input contacts
 - brief status, 53
 - detailed status and configuration, 53

J

- JavaScript, required to launch log in new window, 56

K

- Keywords in user configuration file, 91

L

- Last Transfer Result codes, 100
- Launch Log in New Window, JavaScript

- requirement., 56
- Links, configuration, 86
- Load-shedding with outlet groups, 40
- Local SMTP Server
 - defining by IP address or DNS name, 78
 - recommended option for routing e-mail, 79
- Local Users, setting user access, 62
- Location (system value), 83
- Logging on
 - command line interface, 8
 - Web interface, 29
- Login date and time, command line interface, 10
- Low-Battery Duration, 42

M

- Main screen of command line interface
 - information fields displayed, 9
 - status fields displayed, 10
- Maximum Required Delay, PowerChute Network Shutdown, 42
- Menus
 - Diagnostics, 48
 - Logs, 56
 - Network, 66
 - Notification, 76
- Message Generation (Syslog setting), 81

N

- Network menu, 66
- Network Time Protocol (NTP), 83
- Network timer, resetting, 7
- NMC
 - troubleshooting access problems, 102
- NMS IP/Host Name for trap receivers, 79
- NMS receiving unidentified trap, troubleshooting, 103
- Notification menu, 76
- Notification, delaying or repeating, 76

O

- Outlet groups
 - Control, 38, 47
 - events, 42
 - events and traps, 42
- outlet groups
 - Configuration menu, 40
 - outlet settings option, 40
- Override keyword, user configuration file, 91

P

- Paging
 - by using e-mail, 78
- Passwords
 - default for each account type, 29
 - defining for each account type, 62
 - for data log repository, 59
- Ping utility for troubleshooting access, 102
- Port speed, configuring for Ethernet, 68
- Ports
 - FTP server, 19, 75
 - HTTP and HTTPS, 70
 - RADIUS server, 21, 63
 - Telnet and SSH, 72
- power settings option, 42
- Primary NTP Server, 83
- Put UPS In Bypass, 38
- Put UPS To Sleep or To Sleep Gracefully, 38

Q

- Quick Links, configuration, 86

R

- RADIUS
 - configuration, 63
 - server configuration, 64
 - supported RADIUS servers, 64
- Reboot Management Interface, 86
- Reboot UPS or Reboot UPS Gracefully, 37

- Recent Events
 - Device Events on home page, 31
- Recipient SMTP server, 79
- Remote Users
 - authentication, 63
 - setting user access, 62
- Reset All, 86
- Reset Only, 86
- Restart for inactivity, preventing, 7
- Return Delay, 43
- Reverse lookup, 57
- Runtime calibration requirements, 24, 48

S

- Scheduling option, UPS tab, 49
- SCP
 - for high-security file transfer, 75
 - transferring firmware files, 96
 - using to retrieve event or data log, 59
- Secondary NTP Server, 83
- Section headings, user configuration file, 91
- self-test schedule option, 44
- SET commands, troubleshooting, 103
- Severity Mapping (Syslog setting), 82
- Shutdown Delay parameter, 42
- Shutdowns, configuring, 42
- Sleep Time, 43
- SMTP server
 - selecting for e-mail recipients, 79
 - settings, 78
- SNMP
 - access and access control
 - SNMPv1, 73
 - SNMPv3, 74
 - authentication traps, 80
 - disabling SNMPv1 for high-security systems, 73
 - monitoring outlet groups, 42

- SSH, 8
 - host keys, 72
- SSL
 - how to create, view, or remove certificates, 71
- Status
 - on command line interface main screen, 10
- Synchronize with NTP Server (Date & Time), 83
- Synchronized Control Groups
 - guidelines, 45
 - member status, 45
- Syslog
 - identifying the Syslog server and port, 81
 - mapping event severity to Syslog priorities, 82
- System Name, 83

T

- Take UPS off Bypass, 38
- Telnet, 8
- Temperature units (Fahrenheit or Celsius), 85
- Test
 - DNS query, 69
 - e-mail recipient settings, 79
 - RADIUS server path, 63
 - trap receiver, 80
- Thresholds, for temperature and humidity, 52
- Time setting, 83
- Time Zone, for synchronizing with NTP server, 83
- Timeout setting for RADIUS, 63
- To Address, e-mail recipients, 78
- Trap generation, for trap receivers, 79
- Traps
 - trap receivers, 79
 - traps for outlet groups, 42
 - troubleshooting unidentified traps, 103
- Troubleshooting
 - NMC access problems, 102
 - RADIUS only setting when

- RADIUS is
 - unavailable, 63, 65
 - verification checklist, 102
- Turn UPS Off or On, 37

U

- Unidentified traps, troubleshooting, 103
- Unit Preference, 85
- Up Time
 - command line interface main screen, 10
 - in Web interface, 87
- Update Interval, Date & Time setting, 83
- Update Using NTP Now, Date & Time setting, 83
- Upgrade firmware, 95
- Upload event, 93
- User configuration files
 - contents, 91
 - customizing, 92
 - exporting system time separately, 92
 - messages for undiscovered devices, 93
 - overriding device-specific values, 91
 - retrieving and exporting, 91
 - upload event and error messages, 93
 - using file transfer protocols to transfer, 92
 - using the file as a boot file with DHCP, 67
 - using the utility to retrieve and transfer the files, 91, 97
- User names
 - default for each account type, 29
 - defining for each account type., 62
 - maximum number of characters for
 - RADIUS, 62

W

Web interface

- configuring access, 70

- logging on, 29

- troubleshooting access
problems, 102

X

XMODEM to transfer firmware

- files, 98



Part Number: 90Y3089