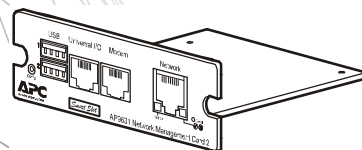




# User's Guide

## Network Management Card

AP9631-IBM





# Contents

---

<b>Introduction .....</b>	<b>1</b>
<b>Product Description .....</b>	<b>1</b>
Features .....	1
Initial setup .....	1
Network management features .....	2
<b>Internal Management Features .....</b>	<b>3</b>
Overview .....	3
Access priority for logging on .....	3
Types of user accounts .....	3
<b>How to Recover from a Lost Password .....</b>	<b>4</b>
<b>Front Panel of the Management Card .....</b>	<b>5</b>
Features .....	5
<b>LED Descriptions .....</b>	<b>5</b>
Status LED .....	5
Link-RX/TX (10/100) LED .....	6
<b>Watchdog Features.....</b>	<b>6</b>
Overview .....	6
Network interface watchdog mechanism .....	7
Resetting the network timer .....	7
<b>Command Line Interface .....</b>	<b>8</b>
<b>How To Log On .....</b>	<b>8</b>
Overview .....	8
Remote access to the command line interface .....	8
Local access to the command line interface .....	9
<b>Main Screen.....</b>	<b>9</b>
Sample main screen .....	9
Information and status fields .....	9

<b>How to Use the Command Line Interface.</b>	<b>11</b>
Overview	11
How to enter commands	11
Command syntax	11
Syntax examples	12
<b>Command Response Codes</b>	<b>12</b>
<b>Command Descriptions</b>	<b>13</b>
?	13
about	13
alarmcount	13
boot	14
cd	15
date	15
delete	16
dir	16
eventlog	16
exit	16
format	17
FTP	17
help	17
ping	18
portSpeed	18
prompt	18
quit	19
radius	19
reboot	20
resetToDef	20
system	20
tcpip	20
ups	21
user	22
web	22
xferINI	23
xferStatus	23

## **Web Interface..... 24**

<b>Introduction.</b>	<b>24</b>
Overview	24
Supported Web browsers	24
<b>How to Log On</b>	<b>24</b>
Overview	24
URL address formats	25

<b>Home Page</b> .....	<b>25</b>
Overview .....	25
Quick status icons .....	25
Recent Device Events .....	26
<b>How to Use the Tabs, Menus, and Links</b> .....	<b>26</b>
Tabs .....	26
Menus .....	27
Quick links .....	27
<b>Monitor and Configure the UPS</b> .....	<b>28</b>
<b>Overview Page</b> .....	<b>28</b>
Operating state .....	28
Quick Status .....	28
Recent UPS Events .....	28
<b>Status Page</b> .....	<b>29</b>
Status displayed for every UPS model .....	29
Model-specific status displayed .....	29
<b>Control Page</b> .....	<b>29</b>
Synchronized Control Group guidelines .....	30
The synchronization process .....	30
Actions (for a single UPS and Synchronized Control Groups) ...	30
<b>Configuration Pages</b> .....	<b>33</b>
The power option .....	33
The shutdown option .....	33
The general option .....	34
The reset UPS defaults option .....	34
The self-test schedule option .....	34
<b>Diagnostics Page</b> .....	<b>35</b>
<b>Scheduling Page (for Shutdowns)</b> .....	<b>35</b>
<b>Sync Control Page</b> .....	<b>36</b>
Guidelines for Synchronized Control Groups .....	36
Display status of a Synchronized Control Group member .....	36
Configure a Synchronized Control Group member .....	36
<b>PowerChute Options</b> .....	<b>37</b>
PowerChute Network Shutdown clients .....	37
PowerChute Network Shutdown configuration parameters .....	38
<b>About Page</b> .....	<b>38</b>

<b>Environmental Monitoring .....</b>	<b>39</b>
<b>Overview Page .....</b>	<b>39</b>
Environmental events .....	39
<b>Temperature and Humidity Page.....</b>	<b>39</b>
Brief status .....	39
Detailed status and configuration .....	39
<b>Input Contacts Page.....</b>	<b>41</b>
Brief status .....	41
Detailed status and configuration .....	41
<b>Output Relay Page .....</b>	<b>41</b>
<b>About Page .....</b>	<b>42</b>
<b>Logs .....</b>	<b>43</b>
<b>Use the Event and Data Logs .....</b>	<b>43</b>
Event log .....	43
Data log .....	44
How to use FTP or SCP to retrieve log files .....	46
<b>Administration: Security.....</b>	<b>48</b>
<b>Local Users .....</b>	<b>48</b>
Setting user access .....	48
<b>Remote Users .....</b>	<b>48</b>
Authentication .....	48
RADIUS .....	49
<b>Configuring the RADIUS Server .....</b>	<b>49</b>
Summary of the configuration procedure .....	49
Configuring a RADIUS server on UNIX® with shadow passwords .....	50
Supported RADIUS servers .....	50
<b>Inactivity Timeout .....</b>	<b>50</b>
<b>Administration: Network Features.....</b>	<b>51</b>
<b>TCP/IP and Communication Settings .....</b>	<b>51</b>
TCP/IP settings .....	51
DHCP response options .....	52

Port Speed .....	54
DNS.....	54
Web.....	55
Console .....	57
SNMP .....	58
SNMPv1 .....	58
SNMPv3 .....	59
FTP Server .....	60
WAP .....	61
<b>Administration: Notification .....</b>	<b>62</b>
Event Actions.....	62
Types of notification .....	62
Configuring event actions .....	62
Active, Automatic, Direct Notification .....	64
E-mail notification .....	64
SNMP traps .....	66
SNMP Trap Test .....	66
Remote Monitoring Service .....	67
Syslog .....	67
<b>Administration: General Options .....</b>	<b>69</b>
Identification .....	69
Set the Date and Time.....	69
Method .....	69
Daylight saving .....	70
Format .....	70
Use an .ini File .....	70
Event Log, Temperature Units, and Log-In Page .....	71
Color-code event log text .....	71
Change the default temperature scale .....	71
Specify a default login page .....	71
Reset the Management Card .....	71

Configure Links .....	72
About the Management Card .....	72
<b>Device IP Configuration Wizard .....</b>	<b>73</b>
Capabilities, Requirements, and Installation .....	73
How to use the Wizard to configure TCP/IP settings .....	73
System requirements .....	73
Installation .....	73
Use the Wizard .....	73
Launch the Wizard .....	73
Configure the basic TCP/IP settings remotely .....	73
Configure or reconfigure the TCP/IP settings locally .....	74
<b>How to Export Configuration Settings .....</b>	<b>75</b>
Retrieving and Exporting the .ini File .....	75
Summary of the procedure .....	75
Contents of the .ini file .....	75
Detailed procedures .....	75
The Upload Event and Error Messages .....	77
The event and its error messages .....	77
Messages in config.ini .....	77
Errors generated by overridden values .....	77
Related Topics .....	78
<b>File Transfers .....</b>	<b>79</b>
How to Upgrade Firmware .....	79
Benefits of upgrading firmware .....	79
Firmware files (Network Management Card) .....	79
Obtain the latest firmware version .....	79
Firmware File Transfer Methods .....	80
Use FTP or SCP to upgrade one Management Card .....	80
How to upgrade multiple Management Cards .....	81
Use XMODEM to upgrade one Management Card .....	81

Verifying Upgrades and Updates . . . . .	82
Verify the success or failure of the transfer . . . . .	82
Last Transfer Result codes . . . . .	82
Verify the version numbers of installed firmware. . . . .	82
<b>Troubleshooting . . . . .</b>	<b>83</b>
Management Card Access Problems . . . . .	83
SNMP Issues . . . . .	84
Synchronization Problems . . . . .	84
<b>Appendix A: Supported Commands . . . . .</b>	<b>85</b>
<b>Appendix B: Getting Help and Technical Assistance</b>	<b>86</b>
Before You Call . . . . .	86
Using the Documentation . . . . .	86
Getting Help and Information from the World Wide Web . . . . .	87
Software Service and Support . . . . .	87
Hardware Service and Support . . . . .	87
IBM Taiwan Product Service . . . . .	87
<b>Appendix C: Notices . . . . .</b>	<b>88</b>
Edition Notice . . . . .	88
Trademarks . . . . .	89
Important Notes . . . . .	89
<b>Index . . . . .</b>	<b>90</b>

# Introduction

---

## Product Description

### Features

The Network Management Card is a Web-based product that manages supported devices using multiple, open standards such as Hypertext Transfer Protocol (HTTP), Telnet, Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS), Secure SHell (SSH), Simple Network Management Protocol (SNMP), File Transfer Protocol (FTP), and Secure CoPy (SCP).

The following is a list of some of the Network Management Card features:

- Provides UPS control and self-test scheduling features
- Provides data and event logs
- Provides support for the PowerChute<sup>®</sup> 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 Management Card
- Supports using the APC Remote Monitoring Service (RMS)
- Enables you to configure notification through event logging (by the Management Card 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<sup>®</sup> Central
- Provides two USB ports
- Supports two universal input/output ports, to which you can connect:
  - Temperature or temperature/humidity sensors
  - Relay input/output connectors that support two input contacts and one output relay



**Note:** Relay input/output connectors are not supported in firmware version 5.0.0. See the IBM Support Web site, <http://www.ibm.com/systems/support>, to download a firmware upgrade that supports this feature.

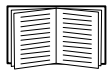
### Initial setup

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

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



**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 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 the Management Card, see “TCP/IP settings” on page 51.

## Network management features

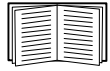
These applications and utilities work with an IBM UPS that connects to the network through a Management Card.

- PowerChute Network Shutdown—Provide unattended remote graceful shutdown of computers that are connected to IBM UPSs
- PowerNet<sup>®</sup> Management Information Base (MIB) with a standard MIB browser—Perform SNMP SETs and GETs and use SNMP traps
- APC InfraStruXure Central—Provide enterprise-level power management and management of UPSs and environmental monitors.
- Device IP Configuration Wizard—Configure the basic settings of one or more Management Cards over the network
- Security Wizard—Create components needed for high security for the Management Card 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 Management Card.

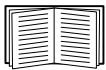


For more information about the internal user interfaces, see “Web Interface” on page 24 and “Command Line Interface” on page 8.

## 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



See “SNMP” on page 58 for information about how SNMP access to the Management Card is controlled.

## Types of user accounts

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

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

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

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

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



To set **User Name** and **Password** values for the three account types, see “Setting user access” on page 48.

# 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 (APC 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
```

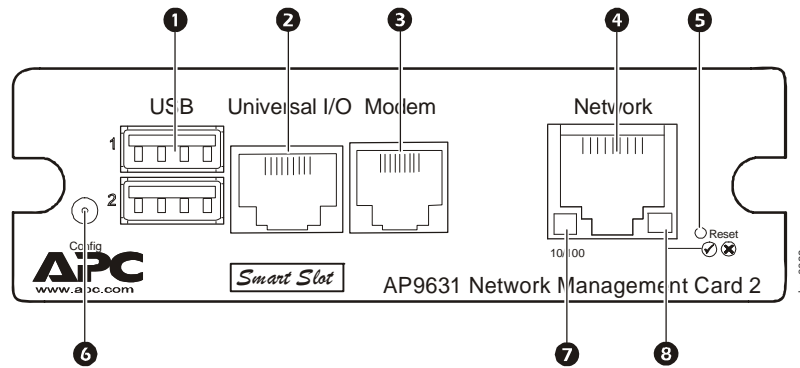
```
user -ap yourAdministratorPassword
```

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 of the Management Card



## Features

	Item	Description
❶	USB ports	Reserved for future use.
❷	Sensor ports	Connect temperature sensors, temperature/humidity sensors, or relay input/output connectors that support two input contacts and one output relay. <b>NOTE:</b> Relay input/output connectors are not supported in firmware version 5.0.0. See the IBM Support Web site, <a href="http://www.ibm.com/systems/support">http://www.ibm.com/systems/support</a> , to download a firmware upgrade that supports this feature.
❸	Modem connector	Reserved for future use.
❹	10/100 Base-T connector	Connects the Management Card to the Ethernet network.
❺	Reset button	Resets the Management Card while power remains on.
❻	Serial configuration port	Connects the Management Card to a local computer to configure initial network settings or access the command line interface.
❼	Link-RX/TX (10/100) LED	See “Link-RX/TX (10/100) LED” on page 6.
❽	Status LED	See “Status LED” on this page.

## LED Descriptions

### Status LED

This LED indicates the status of the Management Card.

Condition	Description
Off	<p>One of the following situations exists:</p> <ul style="list-style-type: none"> <li>The Management Card is not receiving input power.</li> <li>The Management Card is not operating properly. It may need to be repaired or replaced. Contact IBM Support.</li> </ul>
<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 Management Card.</p> <p>2. To use a DHCP server, see “TCP/IP and Communication Settings” on page 51.</p>	

Condition	Description
Solid green	The Management Card has valid TCP/IP settings.
Solid orange	A hardware failure has been detected in the Management Card. Contact IBM Support.
Flashing green	The Management Card does not have valid TCP/IP settings. <sup>1</sup>
Flashing orange	The Management Card is making BOOTP requests. <sup>1</sup>
Alternately flashing green and orange	<p>If the LED is alternately flashing slowly, the Management Card is making DHCP<sup>2</sup> requests.<sup>1</sup></p> <p>If the LED is alternately flashing rapidly, the Management Card is starting up.</p>
<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 Management Card.</p> <p>2. To use a DHCP server, see "TCP/IP and Communication Settings" on page 51.</p>	

## Link-RX/TX (10/100) LED

This LED indicates the network status of the Management Card.

Condition	Description
Off	<p>One or more of the following situations exist:</p> <ul style="list-style-type: none"> <li>• The Management Card is not receiving input power.</li> <li>• The cable that connects the Management Card to the network is disconnected or defective.</li> <li>• The device that connects the Management Card to the network is turned off or not operating correctly.</li> <li>• The Management Card itself is not operating properly. It may need to be repaired or replaced. Contact IBM Support.</li> </ul>
Solid green	The Management Card is connected to a network operating at 10 Megabits per second (Mbps).
Solid orange	The Management Card is connected to a network operating at 100 Megabits per second (Mbps).
Flashing green	The Management Card is receiving or transmitting data packets at 10 Megabits per second (Mbps).
Flashing orange	The Management Card is receiving or transmitting data packets at 100 Megabits per second (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: Warmstart** 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 most of the time and is on the same subnet. The network traffic of that computer will restart the 9.5-minute timer frequently enough to prevent the Management Card from restarting.

# Command Line Interface

---

## How To Log On

### Overview

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection with a computer on the same local area network (LAN) as the Management Card to access the command line interface.

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 on the same network as the Management Card, at a command prompt, type `telnet` and the IP address for the Management Card (for example, `telnet 139.225.6.133`, when the Management Card uses the default Telnet port of 23), and press ENTER.

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

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

**SSH for high-security access.** If you use the high security of SSL for the Web interface, use 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 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 (APC part number 940-0299) from the selected port on the computer to the configuration port at the Management Card.
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 Management Card.

```
American Power Conversion          Network Management Card AOS vx.x.x
(c) Copyright 2008 All Rights Reserved APP vx.x.x
-----
Name       : Test Lab              Date    : 03/30/2009
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 operating system (AOS) and application (APP) firmware versions.

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

- Three fields identify the system name, contact person, and location of the Management Card. (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 Management Card 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 : 03/30/2009

Time : 5:58:30

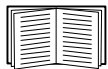
- The **User** field reports whether you logged in through the **Administrator** or **Device Manager** account. (The **Read Only User** account cannot access the command line interface.)  
When you log on as Device Manager (equivalent to Device User in the Web interface), you can access the event log,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

User : Administrator

- The **Stat** field reports the Management Card status.

Stat : P+ N+ A+

Status	Description
P+	The operating system (AOS) is functioning properly.
N+	The network is functioning properly.
N?	A BOOTP request cycle is in progress.
N-	The Management Card failed to connect to the network.
N!	Another device is using the IP address of the Management Card.
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 IBM Support.



**Note:** To view the status of the UPS, type `ups -st`.

# 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 Management Card.

## How to enter commands

At the command line interface, use commands to configure the Management Card. 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 &lt;device password&gt;</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 the preceding 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 the preceding 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
E100	Command failed
E101	Command not found
E102	Reserved
E103	Reserved
E104	Reserved
E200	Reserved

# Command Descriptions

?

**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 IBM Support Web site, <http://www.ibm.com/systems/support>.

## alarmcount

**Access:** Administrator, Device User

**Description:**

Option	Arguments	Description
-p	all	View the number of active alarms reported by the Management Card. 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 Management Card 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>	dhcpBootp   dhcp   bootp   manual	Define how the TCP/IP settings will be configured when the Management Card turns on, resets, or restarts. See “TCP/IP settings” on page 51 for information about each boot mode setting.
-a	remainDhcpBootp   gotoDhcpOrBootp	dhcpBootp boot mode only. Specify whether the Management Card will retain the dhcpBootp boot mode setting or switch to bootp or dhcp boot mode after it receives its network settings.
-o	stop   prevSettings	bootp and dhcpBootp boot modes only. If the Management Card receives no valid response to five requests for a network assignment, stop requesting network settings until the Management Card is restarted or use the previously configured settings so the Management Card remains accessible.
-f	<#>	bootp and dhcpBootp boot modes only. Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.
-c	enable   disable	dhcp and dhcpBootp boot modes only. Enable or disable the requirement that the DHCP server provide the APC cookie.
-s	<#>	dhcp and dhcpBootp boot modes only. Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.
<p>The default values for these three settings generally do not need to be changed:</p> <ul style="list-style-type: none"><li>-v &lt;vendor class&gt;: APC</li><li>-i &lt;client id&gt;: The MAC address of the Network Management Card, which uniquely identifies it on the local area network (LAN)</li><li>-u &lt;user class&gt;: The name of the application firmware module</li></ul>		

**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`
3. Define the number of retries that will occur if the Management Card does not receive a valid response from the initial request: `boot -s 5`

## cd

**Access:** Administrator, Device User

**Description:** Navigate to a folder in the directory structure of the Network Management Card.

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

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 ..
```

## date

**Access:** Administrator only

**Definition:** To configure an NTP server to define the date and time for the Management Card, see “Set the Date and Time” on page 69.

Option	Argument	Description
-d	<“datestring”>	Configure the date used by the Management Card. 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.

**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 November 30, 2008, using the format configured in the preceding example, type:

```
date -d "2008-11-30"
```

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

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

## delete

**Access:** Administrator only

**Description:** Delete the event or data log, or delete a file in the file system.

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

**Example:** To delete the event log:

1. Navigate to the folder that contains the file to delete. For example, to navigate to the `logs` folder, type:  
`cd logs`
2. To view the files in the `logs` folder, type:  
`dir`  
The file `event.txt` is listed.
3. Type `delete event.txt`

## dir

**Access:** Administrator, Device User

**Description:** View the files and folders stored on the Management Card.

## 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 Management Card. 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. Use this command to view events that were recorded after you last retrieved 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 Management Card and erase all security certificates, encryption keys, configuration settings, and the event and data logs.



**Warning:** Use caution when issuing the format command. This command reformats the file system of the Management Card, deleting all security certificates, encryption keys, configuration settings, and the event and data logs.

To reset the Management Card 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 Management Card (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 the help command: `user help`

**Example 1:** To view a list of commands available to a Device User, type:

```
help
```

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

```
alarmcount ?
```

## ping

**Access:** Administrator, Device User

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

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

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

```
ping 150.250.6.10
```

## portSpeed

**Access:** Administrator

**Description:**

Option	Arguments	Description
-s	auto   10H   10F   100H   100 F	Define the communication speed of the Ethernet port. The <code>auto</code> command enables the Ethernet devices to negotiate to transmit at the highest possible speed. See “Port Speed” on page 54 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&gt;</code>

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

```
prompt -s long
```

## quit

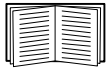
**Access:** Administrator, Device User

**Description:** Exit from the command line interface session.

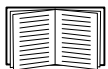
## radius

**Access:** Administrator only

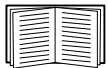
**Description:** View the existing RADIUS settings, enable or disable RADIUS authentication, and configure basic authentication parameters for up to two RADIUS servers.



For a summary of RADIUS server configuration and a list of supported RADIUS servers, see “Configuring the RADIUS Server” on page 49.



Additional authentication parameters for RADIUS servers are available at the Web interface of the Management Card. See “RADIUS” on page 49 for more information.



For detailed information about configuring your RADIUS server, see the *Security Handbook*, available on the Network Management Card *Utility CD*.

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. <b>NOTE:</b> 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 Management Card.
-t1 -t2	<server timeout>	The time in seconds that the Management Card waits for a response from the primary or secondary RADIUS server.

### Example 1:

To view the existing RADIUS settings for the Management Card, 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 Management Card.

## resetToDef

**Access:** Administrator only

**Description:**

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 Management Card, type:

```
resetToDef -p keepip
```

## system

**Access:** Administrator only

**Description:**

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. <b>NOTE:</b> 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 Management Card's SNMP agent.
-c	<system contact>	
-l	<system location>	

**Example 1:** To configure the device location as Test Lab, type:

```
system -l "Test Lab"
```

**Example 2:** To configure the system name as Don Adams, type:

```
system -n "Don Adams"
```

## tcpip

**Access:** Administrator only

**Description:** Manually configure these network settings for the Management Card:

Option	Argument	Description
-i	<IP address>	Type the IP address of the Management Card, using the format <i>xxx.xxx.xxx.xxx</i>
-s	<subnet mask>	Type the subnet mask for the Management Card.
-g	<gateway>	Type the IP address of the default gateway. <b>Do not</b> 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 Management Card will use.

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

**Example 2:** To manually configure an IP address of `150.250.6.10` for the Management Card, type:

```
tcpip -i 150.250.6.10
```

## ups

**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 “Actions (for a single UPS and Synchronized Control Groups)” on page 30 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"><li>• Because a calibration temporarily depletes the UPS batteries, you can perform a calibration only if battery capacity is at 100%.</li><li>• For some UPSs, the load must be at least 7% for a calibration to be performed.</li></ul>
-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 “Actions (for a single UPS and Synchronized Control Groups)” on page 30 for detailed information.
-st		View the status of the UPS.

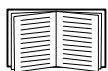
**Example:** To initiate a runtime calibration, type:

```
ups -r start
```

## 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. Blank passwords (passwords with no characters) are not allowed.
-t	<minutes>	Configure the time (3 minutes by default) that the system waits before logging off an inactive user.

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

```
user -an XYZ
```

To change the Administrator password to XYZ, type:

```
user -ap XYZ
```

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

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

Option	Argument	Definition
-S	disable   http   https	Configure access to the Web interface. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate.
-ph	<http port #>	Define the TCP/IP port used by HTTP to communicate with the Management Card (80 by default).
-ps	<https port #>	Define the TCP/IP port used by HTTPS to communicate with the Management Card (443 by default).

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

```
web -S disable
```

## xferINI

**Access:** Administrator only

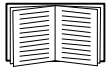
**Description:** Use XMODEM to upload an .ini file while you are accessing the command line interface through a serial connection. After the upload completes:

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

## xferStatus

**Access:** Administrator only

**Description:** View the result of the last file transfer.



See “Verifying Upgrades and Updates” on page 82 for descriptions of the transfer result codes.

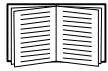
# Web Interface

---

## Introduction

### Overview

The Web interface provides options to manage the UPS and the Management Card.



See “Web” on page 55 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 Management Card through its Web interface. Other commonly available browsers may work but have not been fully tested.

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

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

## How to Log On

### Overview

You can use the DNS name or System IP address of the Management Card 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.



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



For information about the Web page displayed when you log on, see “Home Page” on page 25.

## URL address formats

Type the DNS name or IP address of the Management Card 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.


# 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
	<b>Critical:</b> A critical alarm exists, which requires immediate action.

Symbol	Description
	<b>Warning:</b> An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
	<b>No Alarms:</b> No alarms are present, and the UPS and Management Card 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 Management Card.
- **Environment:** View the status of each temperature sensor, temperature and humidity sensor, input contact, or output relay connected to the Management Card. View active environmental alarms and recent environmental events. Configure thresholds and other parameters related to environmental monitoring.



**Note:** For a 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:

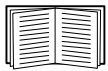
- If a heading has indented option names below it, the heading itself is not a navigational link. Click an option to display or configure parameters.
- If a heading has no indented option names, the heading itself is a navigational link. Click the heading to display or configure parameters.

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



To reconfigure the links, see “Configure Links” on page 72.




# Monitor and Configure the UPS

## Overview Page

The **Overview** page is displayed by default when you click the **UPS** tab or when you click **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		<b>No Alarms:</b> No alarms are present, and the UPS and Management Card are operating normally.
In an alarm state (Accompanying text names the alarm condition and gives a brief description of the alarm.)		<b>Critical:</b> A critical alarm exists, which requires immediate action to avoid data loss or equipment damage.
		<b>Warning:</b> 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.
  - **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.
  - **Output Voltage:** The AC voltage (VAC) the UPS is providing to its load.
  - **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.

### 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**.

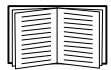
# Status Page

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

## Status displayed for every UPS model

- **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

## Model-specific status displayed



To view detailed information about status items specific to the UPS model associated with the Management Card, see the online help.

The types of model-specific information displayed include the following values:

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

# Control Page

For UPS control actions, click **Control** on the left navigation menu of the UPS tab.

- To initiate a control action for the UPS of this Management Card only, select **No** for **Apply to Sync Group?**
- To initiate a control action for all members of a Synchronized Control Group to which this Management Card belongs (if the option is allowed for Synchronized Control Groups), select **Yes** for **Apply to Sync Group?**



**Note:** The option to apply an action to a Synchronized Control Group is displayed only if the UPS supports Synchronized Control Groups and if its Management Card is an active (enabled) group member.

## Synchronized Control Group guidelines

- All UPSs in a Synchronized Control Group must be the same model.
- Synchronized Control Groups are supported for any IBM UPS with a card slot that accepts a Management Card.



To configure a Management Card to be a member of a Synchronized Control Group, see “Sync Control Page” on page 36.

## The synchronization process

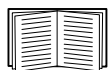
If you apply an action to a Synchronized Control Group, enabled members of the group behave as follows:

- Each UPS receives the command regardless of output status (for example, 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 UPSs perform the action. If a UPS is already in an output state that the action requires (for example, 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 UPSs synchronize their performance of the action (within a one-second time period under ideal conditions).
- 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 UPSs.

## Actions (for a single UPS and Synchronized Control Groups)

Use the actions described in the following table for individual UPSs and for Synchronized Control Groups, within these guidelines:

- All actions except **Put UPS In Bypass** and **Take UPS Off Bypass** are supported:
  - For Synchronized Control Groups
  - For individual IBM UPSs
- **Put UPS in Bypass** and **Take UPS Off Bypass** are supported:
  - Only for individual UPSs, not for Synchronized Control Groups
  - Only for some IBM UPSs



For more information about the delays and settings in the following table, see “Configuration Pages” on page 33 and “Sync Control Page” on page 36. To apply **UPS Alarm Test** to a Synchronized Control Group, see “Diagnostics Page” on page 35.



**Note:** When you select **Yes** for **Signal PowerChute Server 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.

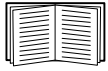
Action	Definition
<b>Turn UPS On</b> (Web interface)  ups -c On (command line interface)	Turns on power at the UPS. For a Synchronized Control Group, after a delay of a few seconds, the action turns on all enabled group members that have input power.
<b>Turn UPS Off</b> (Web interface)  ups -c Off (command line interface)	<p>Turns off the output power of the UPS immediately, without a shutdown delay. The UPS remains off until you turn on its power again.</p> <p>For a Synchronized Control Group, this action turns off power at all enabled members of the group. No <b>Shutdown Delay</b> 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 33.</p> <p><b>NOTE:</b> For a synchronized turn-off action that uses the value of the <b>Shutdown Delay</b> of the initiating UPS, use SNMP. For the <b>upsAdvControlUpsOff</b> OID, set the value to <b>turnUpsSyncGroupOffAfterDelay (5)</b>.</p>
ups -c GraceOff (command line interface)	Turns off outlet power of the UPS after the <b>Maximum Required Delay</b> and the configured <b>Shutdown Delay</b> . See “PowerChute Options” on page 37.
<b>Reboot UPS</b> (Web interface)  ups -c Reboot (command line interface)	<p>Restarts the attached equipment by doing the following:</p> <ul style="list-style-type: none"><li>• Turns off power at the UPS after <b>Shutdown Delay</b>.</li><li>• Turns on power at the UPS after the UPS battery capacity returns to at least the percentage configured for <b>Minimum Battery Capacity</b> or can support the load for the time configured for <b>Return Runtime Duration</b>. (The parameter differs by UPS model.) The UPS then waits the time specified as <b>Return Delay</b>. See “The shutdown option” on page 33.</li></ul> <p>For a Synchronized Control Group action:</p> <ol style="list-style-type: none"><li>1. This option turns off power at the UPSs that are enabled group members after waiting the time configured as <b>Shutdown Delay</b> for the initiating UPSs. See “The shutdown option” on page 33.</li><li>2. The initiating UPS waits up to the number of seconds specified as <b>Power Synchronized Delay</b> 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 <b>Power Synchronized Delay</b>, see “Configure a Synchronized Control Group member” on page 36.</li><li>3. <b>Return Delay</b> starts when the initiating UPS is at its configured <b>Minimum Battery Capacity</b> (or <b>Return Runtime Duration</b>). See “The shutdown option” on page 33. <b>Minimum Battery Capacity</b> (or <b>Return Runtime Duration</b>) of the initiating UPS is also required of group members. However, you can reduce a group member’s requirement by configuring that member’s <b>Minimum Battery Capacity Offset</b> (or <b>Return Runtime Duration Offset</b>), for example, if the initiator’s <b>Minimum Battery Capacity</b> is 50%, and a member’s <b>Minimum Battery Capacity Offset</b> is 5%, that member needs battery capacity of 45% to reboot. See “Configure a Synchronized Control Group member” on page 36.</li></ol>

Action	Definition
ups -c GraceReboot (command line interface)	This action is similar to <b>Reboot UPS</b> , 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 <b>Maximum Required Delay</b> , which is calculated as described in “PowerChute Network Shutdown configuration parameters” on page 38.
<b>Put UPS To Sleep</b> (Web interface)  ups -c Sleep (command line interface)	Puts the UPS into sleep mode by turning off its output power for a defined period of time: <ul style="list-style-type: none"> <li>• The UPS turns off output power after waiting the time configured as <b>Shutdown Delay</b>. See “The shutdown option” on page 33.</li> <li>• When input power returns, the UPS turns on output power after two configured periods of time: <b>Sleep Time</b> and <b>Return Delay</b>. See “The shutdown option” on page 33.</li> <li>• For a synchronized control group action, the Management Card of the initiating UPS waits up to the number of seconds configured as <b>Power Synchronized Delay</b> for enabled group members to regain input power before it starts the <b>Return Delay</b>. If all group members already regained input power, the <b>Power Synchronized Delay</b> 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 36.</li> </ul>
ups -c GraceSleep (command line interface)	Puts the UPS into sleep mode (turns off power for a defined period of time): <ul style="list-style-type: none"> <li>• The UPS turns off output power after waiting the <b>Maximum Required Delay</b> to allow time for PowerChute Network Shutdown to shut down its server safely, and its <b>Shutdown Delay</b>. See “Maximum Required Delay” on page 33 and “The shutdown option” on page 33.</li> <li>• When input power returns, the UPS turns on output power after two configured periods of time: its <b>Sleep Time</b> and <b>Return Delay Time</b>. See “The shutdown option” on page 33.</li> <li>• 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 <b>Power Synchronized Delay</b> for enabled group members to regain input power before it starts the <b>Return Delay</b>. If all group members have already regained input power, the <b>Power Synchronized Delay</b> 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 36.</li> </ul>
<b>Put UPS In Bypass and Take UPS Off Bypass</b> (Web interface)  ups -b Enter ups -b Exit (command line interface)	Controls the use of bypass mode, which allows maintenance to be performed at some UPS models without turning off power at the UPS.

# Configuration Pages

## The power option

This option is available for all UPS models.



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

Setting	Definition
Low Battery Duration	How long the UPS can run on battery power after a low-battery condition occurs.  <b>NOTE:</b> This setting also defines the time available for PowerChute to shut down servers safely in response to the <b>Control</b> option <b>Signal PowerChute Server Shutdown</b> .
Maximum Required Delay	Reports the delay defined by the <b>Maximum Required Delay</b> setting, accessible through the <b>PowerChute</b> option on the left navigation menu.  <b>NOTE:</b> For information about PowerChute features, including how <b>Maximum Shutdown Time</b> is determined, see “PowerChute Network Shutdown configuration parameters” on page 38.
Shutdown Delay	How long the UPS waits before it shuts down in response to a turn-off command.
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.
Basic Low Battery Duration	<b>Available only for some UPS models.</b> 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 <b>Control</b> option <b>Put UPS To Sleep</b> .

Setting	Definition
Return Runtime Duration	Most IBM UPSs 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 graceful shutdown. (The UPS must also wait the time defined as <b>Return Delay</b> before it turns on.)
Minimum Battery Capacity	<p><b>Return Runtime Duration:</b> 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</p> <p><b>Minimum Battery Capacity:</b> 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.</p>
Return Delay	<p>How long the UPS waits before it turns on after a shutdown that was caused by a power failure or after a scheduled shutdown.</p> <p><b>NOTE:</b> The UPS must also have the capacity specified by the <b>Minimum Battery Capacity</b> setting or the available runtime specified as <b>Return Runtime Duration</b> before it can turn on.</p>

## 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. Maximum length: 8 characters.
UPS Position	The physical orientation of the UPS, rack or tower.
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 (for example, 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 reset UPS defaults option

Mark this checkbox to reset all UPS configuration settings to their default values, except **UPS Name** and **Output Voltage**. The time required to reset configuration settings may be a minute or more.

## The self-test schedule option

Use this option to define when the UPS will initiate a self-test (never, at start-up and then weekly, at start-up and every two weeks, or at start-up only).

# Diagnostics Page

You can run a self-test or a run-time calibration for any IBM UPS. The UPS audible alarm test is model-specific and may not be available for your 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"><li>• Because a calibration temporarily depletes the UPS batteries, you can perform a calibration only if battery capacity is at 100%.</li><li>• For some UPSs, the load must be at least 7% for a calibration to be performed.</li></ul>
Initiate	Select a diagnostic procedure to perform immediately: a test of the UPS audible alarm, a UPS self-test, or a run-time calibration.  When you test the audible alarm of a member of a Synchronized Control Group: <ul style="list-style-type: none"><li>• In the Web interface, this option tests the alarms of all enabled members of the group.</li><li>• In SNMP, you can set the OID <b>upsAdvControlFlashAndBeep</b> to <b>flashAndBeep (2)</b> to test the alarm of an individual UPS or to <b>flashAndBeepSyncGroup (3)</b> to test the alarms of all enabled group members.</li></ul>

## Scheduling Page (for Shutdowns)

Select the type of shutdown to schedule, **One-time Shutdown**, **Daily Shutdown**, or **Weekly Shutdown** (at 1, 2, 4, or 8 week intervals), and then use these options:

- **Name:** Define a name for the shutdown.
- **Shutdown daily at, Shutdown, or Shutdown on:** Define when the shutdown will begin, and for a weekly shutdown, the number of weeks between shutdowns.
- **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 “Return Delay” (see “Return Delay” on page 34).
- **Signal PowerChute Server Shutdown:** Select whether to notify clients listed as “PowerChute Network Shutdown clients” to initiate graceful shutdown.

**Schedule a synchronized shutdown.** All scheduled shutdowns will be synchronized when the UPS whose Management Card 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.



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

**Edit, Enable, Disable, or Delete a Scheduled Shutdown.** To access and edit the parameters of a scheduled shutdown, disable it temporarily, or delete it permanently, click the shutdown name in the list of shutdowns, and follow the on-screen instructions.

# Sync Control Page

## Guidelines for Synchronized Control Groups

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

- All UPSs in a Synchronized Control Group must be the same model.
- Synchronized Control Groups are supported for any IBM UPS with a card slot that accepts a Network Management Card.
- When its membership in a Synchronized Control Group is enabled, the Management Card blocks UPS communications from a connected APC management device on the serial communications port. However, the Management Card still allows access to the command line interface on the serial communications port.

## 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: <b>good</b> (acceptable) or <b>bad</b> (not acceptable).
Output Status	The status of the output power of this group member: <b>On</b> or <b>Off</b>

## 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 Management Card'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. 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.

Parameter	Description
Minimum Battery Capacity 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.
or	<b>Minimum Battery Capacity Offset:</b> 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.
Return Runtime Duration Offset	<b>Return Runtime Duration Offset:</b> 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.
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 <b>APC SCG auth phrase</b> .
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 <b>APC SCG crypt phrase</b> .
Synchronized Control Port	The network port that Synchronized Control Groups use to communicate. Use any non-standard port from 5000 to 32768.

## PowerChute Options

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.



See these HTML files and flowcharts on the Network Management Card *Utility* CD:

- *PowerChute Network Shutdown Installation Guide* in the \pcns folder
- *PowerChute Network Shutdown Release Notes* in the \pcns folder
- *PCNS Shutdown Behavior.pdf*, *PCNS Low-Battery Shutdown Behavior.pdf*, and *PCNS Maximum Shutdown Time Negotiation.pdf* in the \trouble folder

### PowerChute Network Shutdown clients

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.

## PowerChute Network Shutdown configuration parameters

Parameter	Description
Maximum Required Delay	<p>Displays the delay required to ensure that each PowerChute client has enough time to shut down safely when the UPS or the PowerChute client initiates a graceful shutdown.</p> <p>When <b>Force Negotiation</b> is selected, PowerChute polls each server listed as a PowerChute Network Shutdown client for information on the time it needs for a graceful shutdown. PowerChute recalculates this delay whenever the management interface of the UPS turns on or is reset.</p> <p><b>Maximum Required Delay</b> 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.</p> <p>If you do not select <b>Force Negotiation</b>, two minutes is used by default as the shutdown delay for all clients.</p>
On-Battery Shutdown Behavior	<p>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.</p>
Authentication Phrase	<p>The case-sensitive phrase of 15 to 32 ASCII characters to be used during MD5 authentication for PowerChute communication. The default Administrator setting is <b>admin user phrase</b>.</p>

## 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 UPSs).
- **Serial Number:** The unique identification number of the UPS, also provided on the outside of the UPS.
- **Firmware Revision** 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.

# Environmental Monitoring

---

## Overview Page

The **Overview** page, displayed when you select the **Environment** tab, lists the status of environmental monitoring devices associated with the Network Management Card of the UPS.

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	<p>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.</p> <p><b>NOTE:</b> To view or configure the parameters of a disabled contact, or to enable it, you must access the interface page for that contact through <b>Input Contacts</b> on the left navigation menu</p>
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.

### 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 of the **Environment** tab 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.
Location	This physical location of the sensor. <i>Maximum:</i> 20 characters.

Parameter	Description
Alarm Status	One of the following is displayed: <ul style="list-style-type: none"> <li>• <b>Normal</b> if this sensor is not reporting an alarm condition.</li> <li>• 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).</li> </ul>
Thresholds	See the next two sections for descriptions of the configurable thresholds and <b>Hysteresis</b> 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.** This value specifies how far past a threshold the temperature or humidity must return to clear a threshold violation.

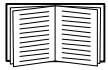
- For Maximum and High threshold violations, the clearing point is the threshold minus the hysteresis.
- For Minimum and Low threshold violations, the clearing point is the threshold plus the hysteresis.

Increase the value for Temperature Hysteresis or Humidity Hysteresis to avoid multiple alarms if temperature or humidity that has caused a violation then wavers slightly up and down. If the hysteresis value is too low, such wavering can cause and clear a threshold violation repeatedly.

**Example of falling but wavering temperature:** The minimum temperature threshold is 55°F, and the temperature hysteresis is 3°F. The temperature drops below 55°F, violating the threshold. It then wavers up to 56°F and then down to 53°F repeatedly, but no clearing event and no new violation occur. For the existing violation to clear, the temperature would have to rise above 58°F (3°F past 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 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



Relay input/output connectors are not supported in firmware version 5.0.0. See the IBM Support Web site, <http://www.ibm.com/systems/support>, to download a firmware upgrade that supports this feature.

## Brief status

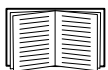
Click **Input Contacts** on the left navigation menu of the **Environment** tab to display the name, alarm status, and state (open or closed) of each input contact.

## 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:</i> 20 characters.
Location	The location of this input contact. <i>Maximum:</i> 20 characters.
Alarm Status	<b>Normal</b> 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: <b>Closed</b> or <b>Open</b> .
Normal State	The normal (non-alarm) state of this input contact: <b>Closed</b> or <b>Open</b> .
Severity	The severity of the alarm that the abnormal state of this input contact generates: <b>Warning</b> or <b>Critical</b> .

# Output Relay Page



Relay input/output connectors are not supported in firmware version 5.0.0. See the IBM Support Web site, <http://www.ibm.com/systems/support>, to download a firmware upgrade that supports this feature.

Click **Output Relay** on the left navigation menu of the **Environment** tab to display the status of the output relay and configure its values.

Parameter	Description
Name	A name for this output relay. <i>Maximum:</i> 20 characters.
Location	The location of this output relay. <i>Maximum:</i> 20 characters.
Alarm Status	<b>Normal</b> 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: <b>Closed</b> or <b>Open</b> .
Normal State	The normal (non-alarm) state of this output relay: <b>Closed</b> or <b>Open</b> .

Parameter	Description
Control	To change the current state of this output relay, check-mark the setting.
Map Output to	Select one or more options. For each option, the number of alarms selected from the number available is in brackets. Click an option name to view available alarms or to change the selection. When a selected alarm occurs, the output relay changes to its alarm state.
Delay	<p>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.</p> <p><b>NOTE:</b> Even if additional mapped alarms occur after the delay begins, the delay does not restart but continues until the output relay is activated.</p>
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 **Environment** tab to display what environmental monitoring devices are in use with this UPS and their firmware versions.

# Logs

---

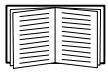
## Use the Event and Data Logs

### 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.



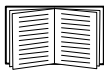
See “Configuring by event” on page 63.

#### 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 46.

#### 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 Management Card 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 Management Card restarts.
- **Filtering the log by event:** To specify the events that display in the log, click **Filter Log**. Clear the checkbox of an event category or alarm severity level to remove it from view. Text at the upper right corner of the event log page indicates that a filter is active.  
As Administrator, click **Save As Default** to save this filter as the default log view for all users. If you do not click **Save As Default**, the filter is active until you clear it or until the Management Card 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.



**Note:** To disable the logging of events based on their assigned severity level or their event category, see “Configuring by group” on page 63.

#### 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 46.

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

## Data log

#### Path: Logs > Data > *options*

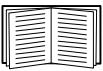
View a log of measurements about the UPS, the power input to the UPS, and the ambient temperature of the UPS and batteries. Each entry is listed by the date and time the data was recorded.

### 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 46.

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

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

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

### To delete the data log:

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

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

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

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

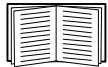
Set up a password-protected data log repository on a specified FTP server. Enabling rotation causes the contents of the data log to be appended to the file you specify by name and location. Updates to this file occur at the upload interval you specify.

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

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).
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 46.

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

#### How to use FTP or SCP to retrieve log files

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

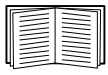
- The file reports all events or data recorded since the log was last deleted or (for the data log) truncated because it reached maximum size.
- The file includes information that the event log or data log does not display.
  - The version of the file format (first field)
  - The date and time the file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



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

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

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



See the *Security Handbook*, available on the Network Management Card *Utility* CD, for information on available protocols and methods for setting up the type of security you need.

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

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

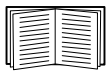
To use SCP to retrieve the *data.txt* file, use the following command:

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

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

1. At a command prompt, type `ftp` and the IP address of the Management Card, 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 60. 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

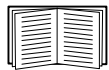
### Setting user access

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

The Administrator user account always has access to the Management Card.

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 10 characters for a user name and 32 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.

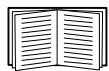
Account Type	Default User Name	Default Password	Permitted Access
Administrator	apc	apc	Web interface and command line interface
Device User	device	apc	
Read-Only User	readonly	apc	Web interface only

## Remote Users

### Authentication

**Path: Administration > Security > Remote Users > Authentication Method**

Use this option to select how to administer remote access to the Management Card.



For information about local authentication (not using the centralized authentication of a RADIUS server), see the *Security Handbook*, available on the *Utility CD*.

The authentication and authorization functions of RADIUS (Remote Authentication Dial-In User Service) are 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 Management Card and the time-out period for each.
- Click **Add Server**, and configure the parameters for authentication by a new RADIUS server.
- Click a listed RADIUS server to display and modify its parameters.

RADIUS Setting	Definition
RADIUS Server	The server name or IP address of the RADIUS server. <b>NOTE:</b> 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 Management Card.
Timeout	The time in seconds that the Management Card waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path.
Switch Server Priority	Change which RADIUS server will authenticate users if two configured servers are listed and <b>RADIUS, then Local Authentication</b> or <b>RADIUS Only</b> is the enabled authentication method.

## Configuring the RADIUS Server

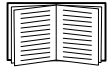
### Summary of the configuration procedure

You must configure your RADIUS server to work with the Management Card.



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



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

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

## Configuring a RADIUS server on UNIX® with shadow passwords

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

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

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

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

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

## Supported RADIUS servers

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

# Inactivity Timeout

## Path: Administration > Security > Auto Log Off

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



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

# Administration: Network Features

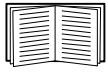
## TCP/IP and Communication Settings

### TCP/IP settings

**Path:** Administration > Network > TCP/IP

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

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



For information on DHCP and DHCP options, see [RFC2131](#) and [RFC2132](#).

Setting	Description
Manual	The IP address, subnet mask, and default gateway must be configured manually. Click <b>Next&gt;&gt;</b> , and enter the new values.
BOOTP	<p>A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Management Card requests network assignment from any BOOTP server:</p> <ul style="list-style-type: none"><li>•If the Management Card receives a valid response, it starts the network services.</li><li>•If the Management Card finds a BOOTP server, but a request to that server fails or times out, the Management Card stops requesting network settings until it is restarted.</li><li>•By default, if previously configured network settings exist, and the Management Card receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible.</li></ul> <p>Click <b>Next&gt;&gt;</b> to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail <sup>1</sup>:</p> <ul style="list-style-type: none"><li>•<b>Maximum retries:</b> Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.</li><li>•<b>If retries fail:</b> Select <b>Use prior settings</b> (the default) or <b>Stop BOOTP request</b>.</li></ul>
<p>1. The default values for these three settings on the configuration pages generally do not need to be changed:</p> <ul style="list-style-type: none"><li>•<b>Vendor Class:</b> APC</li><li>•<b>Client ID:</b> The MAC address of the Network Management Card, which uniquely identifies it on the local area network (LAN)</li><li>•<b>User Class:</b> The name of the application firmware module</li></ul>	

Setting	Description
DHCP	<p>At 32-second intervals, the Management Card requests network assignment from any DHCP server. By default, the number of retries is unlimited.</p> <ul style="list-style-type: none"> <li>•If the Management Card receives a valid response, by default it requires the APC cookie from the DHCP server in order to accept the lease and start the network services.</li> <li>•If the Management Card finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted.</li> </ul> <p>To change these values, click <b>Next&gt;&gt;</b> for the <b>DHCP Configuration</b> page<sup>1</sup>:</p> <ul style="list-style-type: none"> <li>•<b>Require vendor specific cookie to accept DHCP Address:</b> Disable or enable the requirement that the DHCP server provide the APC cookie.</li> <li>•<b>Maximum retries:</b> Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.</li> </ul>
DHCP & BOOTP	<p>The default setting. The Management Card tries to obtain its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server. If it obtains its TCP/IP settings from either server, it switches this setting to <b>BOOTP</b> or <b>DHCP</b>, depending on the type of server that supplied the TCP/IP settings to the Management Card.</p> <p>Click <b>Next&gt;&gt;</b> to configure the same settings that are on the <b>BOOTP Configuration</b> and <b>DHCP Configuration</b> pages<sup>1</sup> and to specify that the <b>DHCP and BOOTP</b> setting be retained after either type of server provides the TCP/IP values.</p>
<p>1. The default values for these three settings on the configuration pages generally do not need to be changed:</p> <ul style="list-style-type: none"> <li>•<b>Vendor Class:</b> APC</li> <li>•<b>Client ID:</b> The MAC address of the Network Management Card, which uniquely identifies it on the local area network (LAN)</li> <li>•<b>User Class:</b> The name of the application firmware module</li> </ul>	

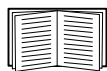
## DHCP response options

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

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

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

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



To disable the requirement of an APC cookie, see “DHCP” on page 52.

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

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

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

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

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

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

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

**TCP/IP options.** The Management Card 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 Management Card.
- **Subnet Mask** (option 1): The Subnet Mask value that the Management Card needs to operate on the network.
- **Router**, that is, Default Gateway (option 3): The default gateway address that the Management Card needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the Management Card.
- **Renewal Time, T1** (option 58): The time that the Management Card 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 Management Card must wait after an IP address lease is assigned before it can seek to rebind that lease.

**Other options.** The Management Card 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 Management Card can use.
- **Time Offset** (option 2): The offset of the Management Card'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 Management Card can use.
- **Host Name** (option 12): The host name that the Management Card will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the Management Card 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 Management Card will download the .ini file. After the download, the Management Card uses the .ini file as a boot file to reconfigure its settings.

# Port Speed

**Path: Administration > Network > Port Speed**

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

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

## DNS

**Path: Administration > Network > DNS > options**

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

- Select **servers** to specify the IP addresses of the primary and optional secondary DNS server. For the Management Card to send e-mail, at least the IP address of the primary DNS server must be defined.
  - The Management Card 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 Management Card does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the Management Card or on a nearby segment (but not across a wide-area network [WAN]).
  - After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for that computer.
- Select **naming** to define the host name and domain name of the Management Card:
  - **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 Management Card interface (except e-mail addresses) that accepts a domain name.
  - **Domain Name:** You need to configure the domain name here only. In all other fields in the Management Card interface (except e-mail addresses) that accept domain names, the Management Card 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 Management Card recognizes a host name with a trailing period (such as `mySnmpServer.`) as if it were a fully-qualified domain name and does not append the domain name.

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

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

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

## Web

Path: Administration > Network > Web > *options*

Option	Description
access	<p>To activate changes to any of these selections, log off from the Management Card:</p> <ul style="list-style-type: none"> <li>• <b>Disable</b>: 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>.)</li> <li>• <b>Enable HTTP</b> (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.</li> <li>• <b>Enable HTTPS</b>: Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL). SSL encrypts user names, passwords, and data during transmission, and authenticates the Management Card by digital certificate. When HTTPS is enabled, your browser displays a small lock icon.</li> </ul> <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><b>HTTP Port</b>: The TCP/IP port (80 by default) used to communicate by HTTP with the Management Card.</p> <p><b>HTTPS Port</b>: The TCP/IP port (443 by default) used to communicate by HTTPS with the Management Card.</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> <p><code>http://152.214.12.114:5000</code>  <code>https://152.214.12.114:5000</code></p>

Option	Description
ssl certificate	<p>Add, replace, or remove a security certificate.</p> <p><b>Status:</b></p> <ul style="list-style-type: none"> <li>•<b>Not installed:</b> A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Using <b>Add or Replace Certificate File</b> installs the certificate to the correct location, <b>/ssl</b>, on the Network Management Card.</li> <li>•<b>Generating:</b> The Network Management Card is generating a certificate because no valid certificate was found.</li> <li>•<b>Loading:</b> A certificate is being activated on the Management Card.</li> <li>•<b>Valid certificate:</b> A valid certificate was installed or was generated by the Management Card. Click on this link to view the contents of the certificate.</li> </ul> <p><b>If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the Management Card generates a default certificate, a process which delays access to the interface for up to one minute.</b> You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on.</p> <p><b>Add or Replace Certificate File:</b> 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</i> CD to choose a method for using digital certificates created by the Security Wizard or generated by the Management Card.</p> <p><b>Remove:</b> 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"> <li>•<b>Disable:</b> Disables all access to the command line interface.</li> <li>•<b>Enable Telnet</b> (the default): Telnet transmits user names, passwords, and data without encryption.</li> <li>•<b>Enable SSH:</b> SSH transmits user names, passwords, and data in encrypted form, providing protection from attempts to intercept, forge, or alter data during transmission.</li> </ul> <p>Configure the ports to be used by these protocols:</p> <ul style="list-style-type: none"> <li>•<b>Telnet Port:</b> The Telnet port used to communicate with the Management Card (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> </li> <li>•<b>SSH Port:</b> The SSH port used to communicate with the Management Card (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.</li> </ul>
ssh host key	<p><b>Status</b> indicates the status of the host key (private key):</p> <ul style="list-style-type: none"> <li>•<b>SSH Disabled: No host key in use:</b> When disabled, SSH cannot use a host key.</li> <li>•<b>Generating:</b> The Management Card is creating a host key because no valid host key was found.</li> <li>•<b>Loading:</b> A host key is being activated on the Management Card.</li> <li>•<b>Valid:</b> 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"> <li>•A 1024-bit or 2048-bit host key created by the Security Wizard</li> <li>•A 2048-bit RSA host key generated by the Network Management Card</li> </ul> </li> </ul> <p><b>Add or Replace:</b> 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</i> CD.</p> <p><b>NOTE:</b> To reduce the time required to enable SSH, create and upload a host key in advance. <b>If you enable SSH with no host key loaded, the Management Card takes up to one minute to create a host key, and the SSH server is not accessible during that time.</b></p> <p><b>Remove:</b> Remove the current host key.</p>

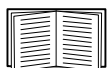


**Note:** To use SSH, you must have an SSH client installed. Most Linux and other UNIX platforms include an SSH client, but Microsoft Windows operating systems do not. Clients are available from various vendors.

# 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 Management Card interface. Read access will allow InfraStruXure Central to receive traps from the Management Card, but Write access is required while you use the interface of the Management Card to set InfraStruXure Central 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*.

## SNMPv1

Path: Administration > Network > SNMPv1 > options

Option	Description
access	<b>Enable SNMPv1 Access:</b> 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 IP 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"><li>•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.</li><li>•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.</li></ul> <p><b>Community Name:</b> 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><b>NMS IP/Host Name:</b> The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows:</p> <ul style="list-style-type: none"><li>•149.225.12.255: Access only by an NMS on the 149.225.12 segment.</li><li>•149.225.255.255: Access only by an NMS on the 149.225 segment.</li><li>•149.255.255.255: Access only by an NMS on the 149 segment.</li><li>•0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.</li></ul> <p><b>Access Type:</b> The actions an NMS can perform through the community.</p> <ul style="list-style-type: none"><li>•<b>Read:</b> GETS only, at any time</li><li>•<b>Write:</b> GETS at any time, and SETS when no user is logged onto the Web interface or command line interface.</li><li>•<b>Write+:</b> GETS and SETS at any time.</li><li>•<b>Disable:</b> No GETS or SETS at any time.</li></ul>

## 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 Management Card supports SHA or MD5 authentication and AES or DES encryption.

Option	Description
access	<b>SNMPv3 Access:</b> 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 <b>apc snmp profile1</b> through <b>apc snmp profile4</b>, 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><b>User Name:</b> 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><b>Authentication Passphrase:</b> A phrase of 15 to 32 ASCII characters (apc auth passphrase, by default) that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time.</p> <p><b>Privacy Passphrase:</b> A phrase of 15 to 32 ASCII characters (apc crypt passphrase, by default) that ensures the privacy of the data (by means of encryption) that an NMS is sending to this device or receiving from this device through SNMPv3.</p> <p><b>Authentication Protocol:</b> This implementation of SNMPv3 supports SHA and MD5 authentication. Authentication will not occur unless an authentication protocol is selected.</p> <p><b>Privacy Protocol:</b> This 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><b>NOTE:</b> 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"> <li>•If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device.</li> <li>•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.</li> </ul> <p>To edit the access control settings for a user profile, click its user name.</p> <p><b>Access:</b> Mark the <b>Enable</b> checkbox to activate the access control specified by the parameters in this access control entry.</p> <p><b>User Name:</b> 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 <b>user profiles</b> option on the left navigation menu.</p> <p><b>NMS IP/Host Name:</b> 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"> <li>•149.225.12.255: Access only by an NMS on the 149.225.12 segment.</li> <li>•149.225.255.255: Access only by an NMS on the 149.225 segment.</li> <li>•149.255.255.255: Access only by an NMS on the 149 segment.</li> <li>•0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.</li> </ul>

## 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 Management Card. The FTP server uses both the specified port and the port one number lower than the specified port.

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



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

At any time that you want a UPS to be accessible for management by InfraStruXure Central, FTP Server must be enabled in the Management Card 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.

# WAP

Use this option to enable (the default) or disable the *Wireless Application Protocol (WAP)*. WAP is a standard for providing cellular phones, pagers, and other handheld devices with secure access to e-mail and text-based Web pages. WAP runs on all major wireless networks and is device-independent, so that it can be used with many phones and handheld devices.

# Administration: Notification

---

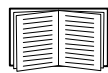
## Event Actions

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

### Types of notification

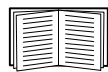
You can configure event actions to occur in response to an event or group of events. These actions notify users of the event in any of several ways:

- Active, automatic notification. The specified users or monitoring devices are contacted directly.
  - E-mail notification
  - SNMP traps
  - APC 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 44 for information on how to configure and use this data logging option.

- Queries (SNMP GETs)



For more information, see “SNMP” on page 58. 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.

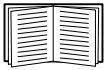
Parameter	Description
Delay $x$ time before sending	If the event persists for the specified time, notification is sent. If the condition clears before the time expires, no notification is sent.
Repeat at an interval of $x$ time	The notification is sent at the specified interval (for example, every 2 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 67
- “E-mail recipients” on page 65
- “Trap Receivers” on page 66

**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.

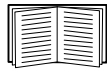
# Active, Automatic, Direct Notification

## 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.

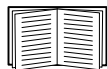
To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and, optionally, the secondary Domain Name System (DNS) servers



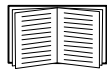
See “DNS” on page 54.

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



See “SMTP” on page 64.

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



See “E-mail recipients” on page 65.



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

## SMTP.

**Path:** Administration > Notification > E-mail > server

Setting	Description
Local SMTP Server	The IP address or DNS name of the local SMTP server.  <b>NOTE:</b> This definition is required only when <b>SMTP Server</b> is set to <b>Local</b> . See “E-mail recipients” on page 65.
From Address	The contents of the <b>From</b> field in e-mail messages sent by the Management Card: <ul style="list-style-type: none"><li>• In the format <i>user@ [IP_address]</i> (if an IP address is specified as <b>Local SMTP Server</b>)</li><li>• In the format <i>user@domain</i> (if DNS is configured and the DNS name is specified as <b>Local SMTP Server</b>) in the e-mail messages.</li></ul> <b>NOTE:</b> 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	<p>The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, myacct100@skytel.com). The pager gateway will generate the page.</p> <p>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, for example, use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.</p> <p><b>NOTE:</b> The recipient's pager must be able to use text-based messaging.</p>
SMTP Server	<p>Select one of the following methods for routing e-mail:</p> <ul style="list-style-type: none"><li>• <b>Local:</b> Through the Management Card's SMTP server. This setting (recommended) ensures that the e-mail is sent before the Management Card's 20-second time-out, and, if necessary, is retried several times. Also do one of the following:<ul style="list-style-type: none"><li>• Enable forwarding at the Management Card's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Check with the administrator of your SMTP server before changing its configuration to allow forwarding.</li><li>• Set up a special e-mail account for the Management Card to forward e-mail to an external mail account.</li></ul></li><li>• <b>Recipient:</b> Directly to the recipient's SMTP server. With this setting, the Management Card tries to send the e-mail only once. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent.</li></ul> <p>When the recipient uses the Management Card's SMTP server, this setting has no effect.</p>
E-mail Generation	<p>Enables (by default) or disables sending e-mail to the recipient.</p>
Format	<p>The long format contains Name, Location, Contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.</p>

## 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 IP address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.

### SNMPv1 option.

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

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



See “SNMPv3” on page 59 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:

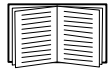
- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver is enabled.
- If a host name is selected for the **To** address, that host name can be mapped to a valid IP address.

**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 APC 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 APC RMS service, contact your APC vendor or see the APC RMS Web site, [rms.apc.com](http://rms.apc.com).

**Registration.** To activate RMS for the Management Card, select **registration**. Complete the form that displays, and click **Send APC RMS Registration**.

**Configuration.** To enable e-mail notification of device and system events detected by RMS, select **configuration** and mark the **APC RMS E-mail Status** checkbox.

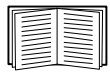


**Note:** If you are unable to submit the registration form, or if RMS data is not being transmitted correctly, you may need to edit the e-mail address of a recipient or edit the SMTP or DNS server settings. For more information, contact IBM Support.

## Syslog

**Path:** Logs > Syslog > *options*

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



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

**Identifying Syslog servers.**

**Path:** Logs > Syslog > servers

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

## Syslog settings.

Path: Logs > Syslog > settings

Setting	Definition
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the Management Card's Syslog messages ( <b>User</b> , by default).  <b>NOTE:</b> <b>User</b> best defines the Syslog messages sent by the Management Card. <b>Do not</b> change this selection unless advised to do so by the Syslog network or system administrator.
Severity Mapping	Maps each severity level of Management Card or Environment events to available Syslog priorities. You should not need to change the mappings.  The following definitions are from RFC3164: <ul style="list-style-type: none"><li>• <b>Emergency:</b> The system is unusable</li><li>• <b>Alert:</b> Action must be taken immediately</li><li>• <b>Critical:</b> Critical conditions</li><li>• <b>Error:</b> Error conditions</li><li>• <b>Warning:</b> Warning conditions</li><li>• <b>Notice:</b> Normal but significant conditions</li><li>• <b>Informational:</b> Informational messages</li><li>• <b>Debug:</b> Debug-level messages</li></ul> Following are the default settings for the <b>Local Priority</b> settings: <ul style="list-style-type: none"><li>• <b>Severe</b> is mapped to <b>Critical</b></li><li>• <b>Warning</b> is mapped to <b>Warning</b></li><li>• <b>Informational</b> is mapped to <b>Info</b></li></ul> <b>NOTE:</b> To disable Syslog messages, see "Configuring event actions" on page 62.

## 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 Management Card.
  - The Header: a time stamp and the IP address of the Management Card.
  - The message (MSG) part:
    - The TAG field, followed by a colon and space, identifies the event type.
    - The CONTENT field is the event text, followed (optionally) by a space and the event code.

For example, APC: Test Syslog is valid.

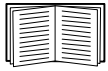
# Administration: General Options

---

## Identification

**Path:** Administration > General > Identification

Define the **Name** (the device name), **Location** (the physical location), and **Contact** (the person responsible for the device) used by InfraStruXure Central and the SNMP agent of the Management Card. 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.

The **Name** and **Location** fields also identify the device when you register for APC Remote Monitoring Service.

## Set the Date and Time

### Method

**Path:** Administration > General > Date & Time > mode

Set the time and date used by the Management Card. 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 Management Card.
  - Mark the checkbox **Apply Local Computer Time** to match the date and time settings of the computer you are using.
- **Synchronize with NTP Server:** Have an NTP Server define the date and time for the Management Card.



**Note:** By default, any Management Card 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 Management Card 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**

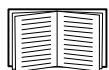
Select the numerical format in which to display all dates in this user interface. In the selections, each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.

# Use an .ini File

**Path: Administration > General > User Config File**

Use the settings from one Management Card to configure another. Retrieve the config.ini file from the configured Management Card, customize that file (for example, to change the IP address), and upload the customized file to the new Management Card. 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 Management Card can use it to set its own configuration.



To retrieve and customize the file of a configured Management Card, see “How to Export Configuration Settings” on page 75.

Instead of uploading the file to one Management Card, you can export the file to multiple Management Cards by using an FTP or SCP script or a batch file and the .ini file utility, available on the Network Management Card *Utility* CD.

# Event Log, Temperature Units, and Log-In Page

Path: Administration > General > Preferences

## Color-code event log text

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

Text Color	Alarm Severity
Red	<b>Critical:</b> A critical alarm exists, which requires immediate action.
Orange	<b>Warning:</b> An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
Green	<b>Alarm Cleared:</b> The conditions that caused the alarm have improved.
Black	<b>Normal:</b> 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 a default login page

Configure the Web page that will display by default when any user logs in.

# Reset the Management Card

Path: Administration > General > Reset/Reboot

Action	Definition
Reboot Management Interface	Restarts the interface of the Management Card.
Reset All <sup>1</sup>	Clear the <b>Exclude TCP/IP</b> checkbox to reset all configuration values; mark the <b>Exclude TCP/IP</b> checkbox to reset all values except TCP/IP settings.
1. Resetting may take up to a minute. The UPS name will not be reset.	

Action	Definition
Reset Only <sup>1</sup>	<b>TCP/IP settings:</b> Set TCP/IP Configuration to <b>DHCP &amp; BOOTP</b> , its default setting, requiring that the Management Card receive its TCP/IP settings from a DHCP or BOOTP server. See “TCP/IP and Communication Settings” on page 51.
	<b>Event configuration:</b> Reset all changes to event configuration, by event and by group, to their default settings.
	<b>UPS to Defaults:</b> Resets only UPS settings, not network settings, to their defaults.
	<b>Lost Environmental Communication Alarms:</b> Clears 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 <b>Normal</b> . <b>NOTE:</b> To clear alarms for a sensor that is connected to the universal sensor port of the Network Management Card, reconnect the sensor or restart the Network Management Card.
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 home page of the APC Web site.
- **Link 2:** A page where you can use samples of APC Web-enabled products.
- **Link 3:** The home page of the APC Remote Monitoring Service.

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

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

## About the Management Card

**Path:** Administration > General > About

The hardware information is useful to IBM Support for troubleshooting problems with the Management Card. The serial number and MAC address are also available on the Management Card itself.

Firmware information for the Application Module, 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 IBM Support Web site, <http://www.ibm.com/systems/support>.

**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. You can use the Wizard in either of the following ways:

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

### System requirements

The Wizard runs on Microsoft Windows 2000, Windows Server<sup>®</sup> 2003, and Windows XP 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 **<http://www.ibm.com/systems/support>**.
2. Download the Device IP Configuration Wizard.
3. Run the executable file in the folder to which you downloaded it.

## Use the Wizard



**Note:** Most software firewalls must be temporarily disabled for the Wizard to discover unconfigured 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 Management Cards, obtain the MAC address of each one to identify it when the Wizard discovers it. (The Wizard displays the MAC address on the screen on which you then enter the TCP/IP settings.)  
The MAC address is on a label on the bottom of the Management Card. You can also obtain the MAC address from the Quality Assurance slip that came with the Management Card.

**Run the Wizard to perform the configuration.** To discover and configure the unconfigured Management Cards over the network:

1. From the **Start** menu, launch the Wizard. The Wizard detects the first Management Card 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 Management Card 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 Management Card 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 Management Card, it displays the screen to enter TCP/IP settings. Repeat this procedure beginning at step 3, or to skip the Management Card 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 Management Card. 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 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 Management Card, 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 Management Card 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 Management Card.

# How to Export Configuration Settings

---

## Retrieving and Exporting the .ini File

### Summary of the procedure

An Administrator can retrieve the .ini file of a Network Management Card and export it to another Management Card or to multiple Management Cards.

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

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

### Contents of the .ini file

The config.ini file you retrieve from a Management Card 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 Management Card 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 Management Card) blocks the exporting of values for the *SystemIP*, *SubnetMask*, *DefaultGateway*, and *BootMode*.

### Detailed procedures

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

1. If possible, use the interface of a Management Card 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 Management Card:
  - a. Open a connection to the Management Card, 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 Management Card's settings:

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

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



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

**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 Management Cards 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 Management Card.** To transfer the .ini file to another Network Management Card, do either of the following:

- From the Web interface of the receiving Management Card, 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, that is, 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 Management Card 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 Management Card:  

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

**Exporting the file to multiple Management Cards.** 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 Management Card.
- Use a batch processing file and the .ini file utility.



To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0*, available 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 Management Card 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 (that is, 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 Management Card 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:

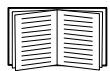
UPS not discovered

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.

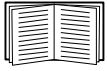


See “Contents of the .ini file” on page 75 for information about which values are overridden.

Because the overridden values are device-specific and not appropriate to export to other Management Cards, 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 Management Card and configure other settings through its user interface.



See “Device IP Configuration Wizard” on page 73.

# File Transfers

---

## How to Upgrade Firmware

### Benefits of upgrading firmware

When you upgrade the firmware on the Network Management Card:

- 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 Management Cards support the same features in the same manner.

### Firmware files (Network Management Card)

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

The Operating System (AOS), application, and boot monitor module files used with the Management Card share the same basic format:

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

- *apc*: Indicates that this is an APC file.
- *hardware-version*: *hw0x* identifies the version of the hardware on which you can use this binary file.
- *type*: Identifies whether the file is the Operating System (AOS) module, the application module, or the boot monitor module for the Management Card.
- *version*: The version number of the file.
- *bin*: Indicates that this is a binary file.

### Obtain the latest firmware version

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



**Note:** If the boot monitor module must be updated, a boot monitor module is included in the firmware release. Otherwise, the boot monitor module that is installed on the card is compatible with the firmware update.

**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 Management Cards by using the separate AOS and application firmware modules.

Obtain the individual firmware modules for your firmware upgrade by downloading the automated tool from <http://www.ibm.com/systems/support>, then extracting the firmware files from the tool.

To extract the firmware files:

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

## Firmware File Transfer Methods

To upgrade the firmware of a Management Card, use one of these methods:

- From a networked computer running a Microsoft Windows operating system, use the firmware upgrade tool downloaded from the IBM Web site.
- From a networked computer on any supported operating system, use FTP or SCP to transfer the individual AOS and application firmware modules.
- For a 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 Management Card.



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

### Use FTP or SCP to upgrade one Management Card

**FTP.** To use FTP to upgrade one Management Card over the network:

- The Management Card 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 Management Card.
- The firmware files must be extracted from the firmware upgrade tool (see “To extract the firmware files:” on page 80).

To transfer the files:

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

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

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

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

```
- apc_hw05_aos_xxx.bin
```

```
- apc_hw05_application_xxx.bin
```

2. Open an FTP client session:

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

3. Type `open` and the IP address of the Management Card, 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 Management Card:

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 Management Card. 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 Management Card.

## How to upgrade multiple Management Cards

**Export configuration settings.** You can create batch files and use an `.ini` utility to retrieve configuration settings from multiple Management Cards and export them to other Management Cards.



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

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

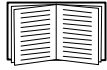
## Use XMODEM to upgrade one Management Card

To use XMODEM to upgrade one Management Card that is not on the network, you must extract the firmware files from the firmware upgrade tool (see “To extract the firmware files:” on page 80).

To transfer the files:

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect the provided serial configuration cable (part number 940-0299) to the selected port and to the serial port at the Management Card.
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 Management Card, 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 Management Card.



For information about the format used for firmware modules, see “Firmware files (Network Management Card)” on page 79.

## Verifying Upgrades and Updates

### Verify the success or failure of the transfer

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

### Last Transfer Result codes

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

### Verify the version numbers of installed firmware.

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

# Troubleshooting

## Management Card Access Problems



**Note:** 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, contact IBM Support.

Problem	Solution
Unable to ping the Management Card	<p>If the Management Card's Status LED is green, try to ping another node on the same network segment as the Management Card. If that fails, it is not a problem with the Management Card. If the Status LED is not green, or if the ping test succeeds, perform the following checks:</p> <ul style="list-style-type: none"><li>• Verify that the Management Card is properly seated in the UPS.</li><li>• Verify all network connections.</li><li>• Verify the IP addresses of the Management Card and the NMS.</li><li>• If the NMS is on a different physical network (or subnetwork) from the Management Card, verify the IP address of the default gateway (or router).</li><li>• Verify the number of subnet bits for the Management Card's subnet mask.</li></ul>
Cannot allocate the communications port through a terminal program	<p>Before you can use a terminal program to configure the Management Card, 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"><li>• 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.</li><li>• For SSH, the Management Card may be creating a host key. The Management Card can take up to one minute to create the host key, and SSH is inaccessible for that time.</li></ul>
Cannot access the Web interface	<ul style="list-style-type: none"><li>• Verify that HTTP or HTTPS access is enabled.</li><li>• Make sure you are specifying the correct URL — one that is consistent with the security system used by the Management Card. SSL requires <b>https</b>, not <b>http</b>, at the beginning of the URL.</li><li>• Verify that you can ping the Management Card.</li><li>• Verify that you are using a Web browser supported for the Management Card. See "Supported Web browsers" on page 24.</li><li>• If the Management Card has just restarted and SSL security is being set up, the Management Card may be generating a server certificate. The Management Card can take up to one minute to create this certificate, and the SSL server is not available during that time.</li></ul>

# SNMP Issues

Problem	Solution
Unable to perform a GET	<ul style="list-style-type: none"> <li>• Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3).</li> <li>• Use the command line interface or Web interface to ensure that the NMS has access. See “SNMP” on page 58.</li> </ul>
Unable to perform a SET	<ul style="list-style-type: none"> <li>• Verify the read/write (SET) community name (SNMPv1) or the user profile configuration (SNMPv3).</li> <li>• 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 58.</li> </ul>
Unable to receive traps at the NMS	<ul style="list-style-type: none"> <li>• Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the NMS as a trap receiver.</li> <li>• For SNMP v1, query the <b>mconfigTrapReceiverTable</b> 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 <b>mconfigTrapReceiverTable</b> OIDs, or use the command line interface or Web interface to correct the trap receiver definition.</li> <li>• For SNMPv3, check the user profile configuration for the NMS, and run a trap test.</li> </ul> <p>See “SNMP” on page 58, “Trap Receivers” on page 66, and “SNMP Trap Test” on page 66.</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 <b>Enabled</b> . 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 <b>Multicast IP Address</b> , <b>Synchronized Control Group Number</b> , and firmware version must match those of other members of the group.

# Appendix A: Supported Commands

---

?	radius
about	[-a <access> [local   radiusLocal   radius]]
alarmcount	[-p# <server IP>]
[-p [all   warning   critical]]	[-s# <server secret>]
	[-t# <server timeout>]
boot	reboot
[-b <dhcpBootp   dhcp   bootp   manual>]	resetToDef
[-a <remainDhcpBootp   gotoDhcpOrBootp>]	[-p [all   keepip]]
[-o <stop   prevSettings>]	system
[-f <retry then fail #>]	[-n <system name>]
[-c <dhcp cookie> [enable   disable]]	[-c <system contact>]
[-s <retry then stop #>]	[-l <system location>]
[-v <vendor class>]	tcPIP
[-i <client id>]	[-i <IP address>]
[-u <user class>]	[-s <subnet mask>]
cd	[-g <gateway>]
console	[-d <domain name>]
[-S <disable   telnet   ssh>]	[-h <host name>]
[-pt <telnet port #>]	ups
[-ps <ssh port #>]	[-c <off   graceoff   on   reboot   gracereboot
[-b <baud rate> [2400   9600   19200   38400]]	sleep   gracesleep>]
date	[-r <start   stop>]
[-d <"datestring">]	[-s <start>]
[-t <00:00:00>]	[-b <enter   exit>]
[-f [mm/dd/yy   dd.mm.yyyy   mmm-dd-yy	[-o# <off   delayoff   on   delayon   reboot>]
dd-mmm-yy   yyyy-mm-dd]]	[-st]
delete	user
dir	[-an <Administrator name>]
eventlog	[-dn <Device User name>]
exit	[-rn <Read-Only User name>]
format	[-ap <Administrator password>]
ftp	[-dp <Device User password>]
[-p <port number>]	[-rp <Read-Only User password>]
[-S <enable   disable>]	[-t <inactivity timeout in minutes>]
help	web
ping	[-S <disable   http   https>]
[-<IP address or DNS name>]	[-ph <http port #>]
portspeed	[-ps <https port #>]
[-s [auto   10H   10F   100H   100F]]	xferINI
prompt	xferStatus
[-s [long   short]]	
quit	

# 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

台灣 IBM 產品服務聯絡方式：  
台灣國際商業機器股份有限公司  
台北市松仁路 7 號 3 樓  
電話：0800-016-888

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

Second Edition (May 2009)

990-2234A

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

©Copyright 2009 APC by Schneider Electric. All rights reserved.

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](http://www.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<sup>®</sup>, 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 Management Card 72
  - for information about the UPS 38
  - for information on environmental monitors 42

### Access

- enabling or disabling methods of access
  - to the command line interface 57
  - to the Web interface 55
- priority for logging on 3
- to the command line interface
  - locally 9
  - remotely 8
- troubleshooting 83

### Administration

- Network menu 51
- Notification menu 62

### Alarm Status

- output relay 41
- temperature and humidity 40

### Alarm Status, input contacts 41

### Apply Local Computer Time 69

### Authenticating users through RADIUS 48

### Authentication Traps setting 66

### Automatic log-off for inactivity 50

## B

### Basic Low Battery Duration 33

### Basic Signaling Shutdown 33

### BOOTP

- BOOTP server providing TCP/IP settings 51
- Status LED reporting BOOTP requests 6

## C

- Certificates, how to create, view, or remove 56

### Command line interface

- command descriptions 13
- configuring access 57
- supported commands 85

### Community Name

- for trap receivers 66
- verifying correct configuration 84

### Configuring

- RADIUS authentication 49
- shutdowns 33

### Contact identification (whom to contact) 69

### Control actions 31

## D

### Data log

- importing into spreadsheet 46
- Log Interval setting 45
- rotation (archiving) 45
- using FTP or SCP to retrieve 46

### Date & Time settings 69

### Date format, configuring 70

### Daylight saving time 70

### Device IP Configuration Wizard

- installation and system requirements 73
- using the wizard
  - for local configuration. 74
  - for remote configuration 73

### DHCP

- APC cookie 52
- DHCP server providing TCP/IP settings 51
- Status LED reporting DHCP requests 6

### Diagnostics 35

### Disable

- e-mail to a recipient 65
- reverse lookup 44
- Telnet 57

### DNS

- defining host and domain names 54
- query types 55
- specifying DNS servers by IP address 54

## E

### E-mail

- configuring notification parameters 64
- configuring recipients 65
- test message 65
- using for paging 65

### Enable

- e-mail forwarding to external SMTP servers 65
- e-mail to a recipient 65
- reverse lookup 44
- Telnet 57
- versions of SSH 57

### Error messages

- from overridden values in .ini file 77

### Ethernet port speed 54

### Event actions 62

- configuring by event 63
- configuring by group 63

### Event log

- displaying and using 43
- errors from overridden values in .ini file 77
- using FTP del command 47
- using FTP or SCP to retrieve 46

### event.txt file

- contents 46
- importing into spreadsheet 46

## F

### Facility Code (Syslog setting) 68

### Firmware

- benefits of upgrading 79
- file transfer methods
  - automated upgrade tool 79
  - FTP or SCP 80
  - XMODEM 81
- obtaining the latest version 79
- upgrading multiple Management Cards 81
- versions displayed on main screen 9

### From Address (SMTP setting) 64

### FTP

- server settings 60
- transferring firmware files 80
- using to retrieve event or data log 46

## G

### GET commands, troubleshooting 84

## H

### Help

- on configuring UPS power options 33

### Host keys

- adding or replacing 57
- status 57

### Host name of trap receivers 66

### Hysteresis 40

## I

### Identification (Name, Location, and Contact)

- in Web interface 69

### Inactivity timeout 50

### ini files, *See* User configuration files

### Input contacts

- brief status 41
- detailed status and configuration 41

## J

### JavaScript, required to launch log in new window 43

## K

### Keywords in user configuration file 75

## L

### Last Transfer Result codes 82

### Launch Log in New Window, JavaScript requirement. 43

### Links, configuration 72

### Local SMTP Server

- defining by IP address or DNS name 64
- recommended option for routing e-mail 65

### Local Users, setting user access 48

### Location (system value) 69

### Logging on

- command line interface 8
- DNS name or IP address matched to common name 24
- Web interface 24

### Login date and time, command line interface 10

### Low-Battery Duration 33

## M

- Main screen of command line interface
  - information fields displayed 9
  - status fields displayed 10
- Management Card
  - preventing restart for inactivity 6
  - troubleshooting access problems 83
- Maximum Required Delay, PowerChute Network Shutdown 33
- Menus
  - Diagnostics 35
  - Logs 43
  - Network 51
  - Notification 62
- Message Generation (Syslog setting) 68

## N

- Network menu 51
- Network Time Protocol (NTP) 69
- Network timer, resetting 7
- NMS IP/Host Name for trap receivers 66
- NMS receiving unidentified trap, troubleshooting 84
- Notification menu 62
- Notification, delaying or repeating 62

## O

- Output relay
  - mapping to alarms 42
- Override keyword, user configuration file 75

## P

- Paging
  - by using e-mail 65
- Passwords
  - default for each account type 24
  - defining for each account type 48
  - for data log repository 46
- Ping utility for troubleshooting access 83
- Port speed, configuring for Ethernet 54
- Ports
  - FTP server 17, 60
  - HTTP and HTTPS 55
  - RADIUS server 19, 49
  - Telnet and SSH 57
- Power option 33

- Primary NTP Server 69
- Put UPS In Bypass 32
- Put UPS To Sleep or To Sleep Gracefully 32

## Q

- Quick Links, configuration 72

## R

- RADIUS
  - configuration 49
  - server configuration 49
  - supported RADIUS servers 50
- Reboot Management Interface 71
- Reboot UPS or Reboot UPS Gracefully 31
- Recent Events
  - Device Events on home page 26
- Recipient SMTP server 65
- Remote Monitoring Service 72
- Remote Users
  - authentication 49
  - setting user access 48
- Reset All 71
- Reset Only 72
- Restart for inactivity, preventing 7
- Return Delay 34
- Reverse lookup 44
- Runtime calibration requirements 21, 35

## S

- Scheduling option, UPS tab 35
- SCP
  - for high-security file transfer 60
  - transferring firmware files 80
  - using to retrieve event or data log 46
- Secondary NTP Server 69
- Section headings, user configuration file 75
- self-test schedule option 34
- SET commands, troubleshooting 84
- Severity Mapping (Syslog setting) 68
- Shutdown Delay parameter 33
- Shutdowns, configuring 33
- Sleep Time 33
- SMTP server
  - selecting for e-mail recipients 65
  - settings 64

## SNMP

- access and access control
  - SNMPv1 58
  - SNMPv3 59
- authentication traps 66
- disabling SNMPv1 for high-security systems 58

## SSH

- host keys 57

## SSL

- how to create, view, or remove certificates 56

## Status

- on command line interface main screen 10

## Synchronize with NTP Server

- (Date & Time) 69

## Synchronized Control Groups

- guidelines 36
- member status 36

## Syslog

- identifying the Syslog server and port 67
- mapping event severity to Syslog priorities 68

## System Name 69

## T

### Take UPS off Bypass 32

### TCP/IP configuration 51

### Temperature units (Fahrenheit or Celsius) 71

## Test

- DNS query 55
- e-mail recipient settings 65
- RADIUS server path 49
- trap receiver 66

### Thresholds, for temperature and humidity 40

### Time setting 69

### Time Zone, for synchronizing with NTP server 69

### Timeout setting for RADIUS 49

### To Address, e-mail recipients 65

### Trap generation, for trap receivers 66

## Traps

- trap receivers 66
- troubleshooting unidentified traps 84

## Troubleshooting

- management card access problems 83
- problems logging on to Web interface 24
- RADIUS only setting when RADIUS is unavailable 49
- verification checklist 83

### Turn UPS Off or On 31

## U

### Unidentified traps, troubleshooting 84

### Unit Preference 71

## Up Time

- command line interface main screen 9
- in Web interface 72

### Update Interval, Date & Time setting 69

### Update Using NTP Now, Date & Time setting 69

### Upgrade firmware 79

## User configuration files

- contents 75
- customizing 76
- exporting system time separately 76
- messages for undiscovered devices 77
- overriding device-specific values 75
- retrieving and exporting 75
- upload event and error messages 77
- using file transfer protocols to transfer 76
- using the APC utility to retrieve and transfer the files 81
- using the file as a boot file with DHCP 53

## User names

- default for each account type 24
- defining for each account type. 48
- maximum number of characters for RADIUS 48

## W

### WAP 61

## Web interface

- configuring access 55
- logging on 24
- troubleshooting access problems 83

### Wireless Application Protocol (WAP) 61

## X

### XMODEM to transfer firmware files 81





Part Number: 43V6148