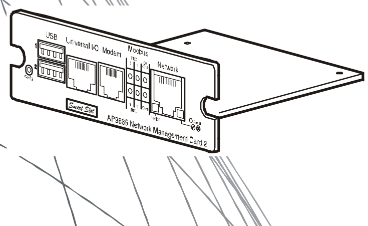
User’s Guide

Network Management Card

AP9635



This manual is available in English on the enclosed CD.

Dieses Handbuch ist in Deutsch auf der beiliegenden CD-ROM verfügbar.

Este manual está disponible en español en el CD-ROM adjunto.

Questo manuale è disponibile in italiano nel CD-ROM allegato.

本マニュアルの日本語版は同梱の CD-ROM からご覧になれます。

동봉된 CD 안에 한국어 매뉴얼이 있습니다 .

Instrukcja obsługi w języku polskim jest dostępna na CD.

O manual em Português está disponível no CD-ROM em anexo.

您可以从包含的 CD 上获得本手册的中文版本。

您可以从付属的ＣＤ上获得本手册的中文版本。

Contents

Introduction

Product Description

Features

The American Power Conversion Network Management Card (AP9635) 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 Network Management Card:

- Provides data and event logs
- Provides support for the PowerChute® Network Shutdown utility
- Supports using a Dynamic Host Configuration Protocol (DHCP) or BOOTstrap Protocol (BOOTP) server to provide the network (TCP/IP) values of the Management Card
- Supports using the Remote Monitoring Service (RMS)
- Supports remote monitoring over modem using Tele Service Connect (TLS) (MGE® Galaxy® 300 and MGE Galaxy 7000 only). Contact APC Support for information.
- 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® Central
- Supports Modbus RTU over a serial RS485 port
- Supports Modbus over TCP (Symmetra® PX 250 and 500 only)

Devices in which you can install the Management Card. The AP9635 Network Management Card can be installed into the Symmetra PX 250, Symmetra PX 500, MGE Galaxy 300, and MGE Galaxy 7000 UPS devices.

Note: The Network Management Card ships with the firmware for the MGE Galaxy 300 and MGE Galaxy 7000 already installed. If you are ordering the card as a replacement part for a Symmetra PX 250 or Symmetra PX 500, you will need to install the Symmetra-specific firmware. Contact APC Worldwide Customer Support for more information. See “APC Worldwide Customer Support” on page 96.

Initial setup

You must define three TCP/IP settings for the Network 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 a Management Card, see "TCP/IP and Communication Settings" on page 54.

Network management features

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

- PowerChute Network Shutdown—Provide unattended remote graceful shutdown of computers that are connected to American Power Conversion UPS devices.
- PowerNet® Management Information Base (MIB) with a standard MIB browser—Perform SNMP SETs and GETs and to use SNMP traps.
- InfraStruxure Central—Provide enterprise-level power management and management of Amercian Power Conversion agents, UPS devices, and environmental monitors.
- Device IP Configuration Wizard—Configure the basic settings of one or more Network Management Cards over the network.
- Security Wizard—Create components needed for high security for the Network 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 Management Card.

For more information about the internal user interfaces, see "Web Interface" on page 28 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

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

See "SNMP" on page 61 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 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 delete data or use file transfer options. 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 50.

How to Recover from a Lost Password

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

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

   ```
   user -an yourAdministratorName
   ```

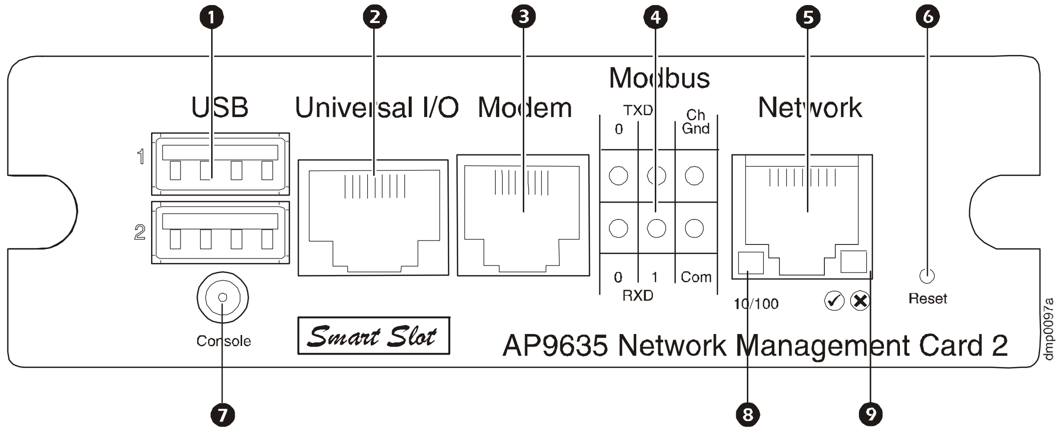
   ```
   user -ap yourAdministratorPassword
   ```

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

   ```
   user -an Admin
   ```

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

Front Panel



Features

	Item	Description
❶	USB ports	Reserved for future use.
❷	Universal I/O sensor port	Connects external sensors to the Network Management Card. (
❸	Modem port	Used for Tele Service Connect (TLS) (MGE Galaxy 300 and MGE Galaxy 7000 only).
❹	Modbus connector	Connects the Management Card to a Building Management System (BMS)
❺	10/100 Base-T connector	Connects the Management Card to the Ethernet network.
❻	Reset button	Resets the Management Card while power remains on.
❼	Serial configuration port	Connects the Management Card to a local computer to configure initial network settings or access the command line interface.
❽	Link-RX/TX (10/100) LED	See “Link-RX/TX (10/100) LED” on page 6.
❾	Status LED	See “Status LED” on page 6.

Status LED

This LED indicates the status of the Management Card.

Condition	Description
Off	One of the following situations exists: • The Management Card is not receiving input power. • The Management Card is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support. See "APC Worldwide Customer Support" on page 96.
Solid green	The Management Card has valid TCP/IP settings.
Solid orange	A hardware failure has been detected in the Management Card. Contact APC Worldwide Customer Support. See "APC Worldwide Customer Support" on page 96.
Flashing green	The Management Card does not have valid TCP/IP settings.[1]
Flashing orange	The Management Card is making BOOTP requests.[1]
Alternately flashing green and orange	If the LED is alternately flashing slowly, the Management Card is making DHCP[2] requests.[1] If the LED is alternately flashing rapidly, the Management Card is starting up.

[1] If you do not use a BOOTP or DHCP server, see the Network Management Card *Installation and Quick Start Manual* provided in printed format and on the Network Management Card *Utility* CD to configure the TCP/IP settings of the Management Card manually.

[2] To use a DHCP server, see "TCP/IP and Communication Settings" on page 54.

Link-RX/TX (10/100) LED

This LED indicates the network status.

Condition	Description
Off	One or more of the following situations exist: • The Management Card is not receiving input power. • The cable that connects the Management Card to the network is disconnected or defective. • The device that connects the Management Card to the network is turned off or not operating correctly. • The Management Card itself is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support. See "APC Worldwide Customer Support" on page 96.
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 Mbps.
Flashing green	The Management Card is receiving or transmitting data packets at 10 Mbps.
Flashing orange	The Management Card is receiving or transmitting data packets at 100 Mbps.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the Management Card uses internal, system-wide watchdog mechanisms. When it restarts to recover from an internal problem, a **System: 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 network as the Network 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.

Note: The command line interface does not display information about the Symmetra PX 250 or Symmetra PX 500 UPS.

Remote access to the command line interface

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

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

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

To use Telnet to access the command line interface:

1. From a computer that has access to network on which the Management Card is installed, 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. (These are commands for general usage: some clients don’t allow you to specify the port as an argument and some types of Linux might want extra commands).

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

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

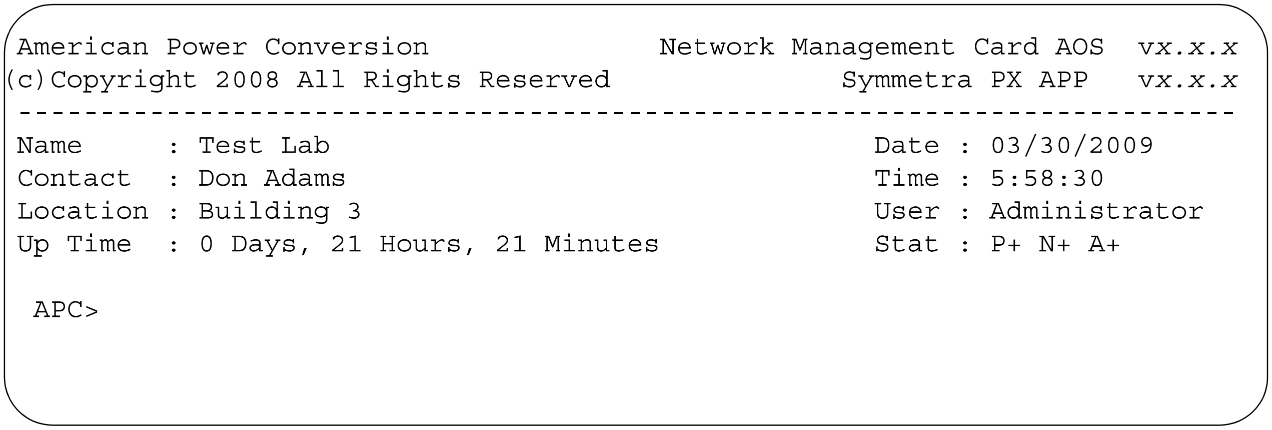
Local access to the command line interface. For local access, use a computer that connects to the Management Card through the serial port to access the command line interface:

1. Select a serial port at the computer and disable any service that uses the port.
2. Connect the provided serial cable (part number 940-0299) from the selected port on the computer to the configuration port at the 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 twice. 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            Symmetra PX 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 APC operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the device that connects to the network through this Management Card. In the example above, the Management Card uses the application firmware for a Symmetra PX UPS.

  ```
  Network Management Card AOS    vx.x.x
  Symmetra PX 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 and view the number of active alarms.

```
User : Administrator
```

Main screen status fields.

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

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

`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 APC Customer Support. See “APC Worldwide Customer Support” on page 96.

To view the status of the UPS, you must access the Web interface of the Management Card. For more information, see “Web Interface” on page 28.

Using the Command Line Interface

Overview

The command line interface provides options to configure the network settings and monitor the Management Card.

To view the status of the UPS, you must access the Web interface of the Management Card. For more information, see “Web Interface” on page 28.

Entering 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.

At the command line interface, you can also use these keyboard shortcuts:

- 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, then press the TAB key to scroll through a list of valid commands that match the text you typed in the command line.
- 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: `-dp <device password>`
[ ]	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 APC Web site, **www.apc.com/tools/download**.

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>	dhcp | bootp | manual	Define how the TCP/IP settings will be configured when the Management Card turns on, resets, or restarts. The default setting is `dhcp`. See "TCP/IP and Communication Settings" on page 54 for information about each boot mode setting.
-c	enable | disable	`dhcp` boot mode only. Enable or disable the requirement that the DHCP server provide the APC cookie.
The default values for these three settings generally do not need to be changed: -v <vendor class>: APC -i <client id>: The MAC address of the Network Management Card, which uniquely identifies it on the local area network (LAN) -u <user class>: The name of the application firmware module		

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

1. Define the boot mode setting.
   ```
   boot -b dhcp
   ```
2. Enable the requirement that the DHCP server provide the APC cookie.
   ```
   boot -c enable
   ```

cd

Access: Administrator, Device User

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

console

Access: Administrator only

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

Option	Argument	Description
-S	disable | telnet | ssh	Configure access to the command line interface, or use the `disable` command to prevent access.. Enabling SSH enables SCP and disables Telnet.
-pt	<telnet port n>	Define the Telnet port used to communicate with the Management Card (23 by default).
-ps	<SSH port n>	Define the SSH port used to communicate with the Management Card (22 by default).
-b	2400 | 9600 | 19200 | 38400	Configure the speed of the serial port connection (9600 bps by default).

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

```
console -S ssh
```

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

```
console -pt 5000
```

date

Access: Administrator only

Definition: To configure an NTP server to define the date and time for the Management Card, see “Set the Date and Time” on page 72.

Option	Argument	Description
-d	<“datestring”>	Configure the date used by the Management Card. Use the date format specified by the `date -f` 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 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. The format `mmm` represents a three-letter month name.
-z	<time zone offset>	Set the difference with GMT in order to specify your time zone. This enables you to synchonize with other people in different time zones.

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

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

Example 2: To define the date as October 30, 2010, using the format configured in the preceding example, type:

```
date -d “2010-10-30”
```

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

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

delete

Access: Administrator only

Description: Delete 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:

1. Navigate to the folder that contains the file to delete. For example, to delete the event log, type this command to navigate to the `logs` folder:

   ```
   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.

dns

Access: Administrator

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

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

eventlog

Access: Administrator, Device User

Description: View the date and time you retrieved the event log, the status of the UPS, and the status of sensors connected to the 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.

Note: 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 ?
```

modbus

Access: Administrator only

Description: Manually configure these Modbus settings for the Management Card:

Option	Argument	Description
-p		Display the configured Modbus parameters.
-a	enable | disable	Enable or disable the Modbus feature.
-br	9600 | 19200	Set the baud rate.
-pr	even | odd | none	Set the parity bit.
-s	<slave # in hex>	Set the Modbus slave address.
-o	master | slave	Define the mode of operation for the Modbus feature. (MGE Galaxy models only)
-rt	<timeout in mSec>	Set the response timeout in milliseconds for query packets in Master mode. (MGE Galaxy models only)

Option	Argument	Description
-sr	<scan rate in mSec>	Set the scan rate for query packets in Master mode. (MGE Galaxy models only)
-rep	<# of repetitions>	Set the number of repetitions for query packets in Master mode. (MGE Galaxy models only)
-ResetToDef		Reset the modbus settings to their default values.

netstat

Access: Administrator, Device User

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

ntp

Access: Administrator

Description: View and configure the network time protocol parameters.

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

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

```
ntp -OM enable
```

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

```
ntp -p 150.250.6.10
```

ping

Access: Administrator, Device User

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

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

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

```
ping 150.250.6.10
```

portSpeed

Access: Administrator

Description:

Option	Arguments	Description
-s	auto | 10H | 10F | 100H | 100F	Define the communication speed of the Ethernet port. The `auto` command enables the Ethernet devices to negotiate to transmit at the highest possible speed. See “Port Speed” on page 57 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: `APC>`

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 52.

Additional authentication parameters for RADIUS servers are available at the Web interface of the Management Card. See "RADIUS" on page 51 for more information.

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

Option	Argument	Description
-a	local | radiusLocal | radius	Configure RADIUS authentication: • `local`—RADIUS is disabled. Local authentication is enabled. • `radiusLocal`—RADIUS, then Local Authentication. RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used. • `radius`—RADIUS is enabled. Local authentication is disabled.
-p1 -p2	<server IP>	The server name or IP address of the primary or secondary RADIUS server. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.
-s1 -s2	<server secret>	The shared secret between the primary or secondary RADIUS server and the 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: Resets the Management Card.

resetToDef

Access: Administrator only

Description:

Option	Arguments	Description
-p	all | keepip	Reset all configuration changes, including event actions 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
```

snmp, snmp3

Access: Administrator only

Description: Enable or disable SNMP 1 or SNMP 3.

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

Example: To enable SNMP version 1, type:

```
snmp -S enable
```

system

Access: Administrator only

Description:

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. These values are also used by InfraStruxure Central and the Management Card's SNMP agent. **NOTE:** If you define a value with more than one word, you must enclose the value in quotation marks.
-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
-S	enable | disable	Enable or disable TCP/IP..
-i	<IP address>	Type the IP address of the Management Card, using the format *xxx.xxx.xxx.xxx*
-s	<subnet mask>	Type the subnet mask for the Management Card.
-g	<gateway>	Type the IP address of the default gateway. **Do not** use the loopback address (127.0.0.1) as the default gateway.
-d	<domain name>	Type the DNS name configured by the DNS server.
-h	<host name>	Type the host name that the 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
```

tcpip6

Access: Administrator only

Description: Enable IPv6 and view and manually configure these network settings for the Management Card:

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

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

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

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

tls

Access: Administrator only

Description: Manually configure the TLS settings for the Management Card. TLS is an optional remote monitoring service available on the MGE Galaxy 300 and MGE Galaxy 7000 UPS systems.:

Option	Argument	Description
-p		Display the configured parameters for the tls command
-a	enable | disable	Enable or disable the TLS feature.
-m	<slave number in hex>	Identify the valid alarms that cause an alert to be sent to the TLS service.
	<call cause mask in hex>	
-t	<primary | secondary>	Determine what primary or secondary number to call to establish a TLS connection. The telephone number should be configured with country code, area code, and number. Only used for master configuration - a slave UPS can store the information, but it will not be used.
	<telephone#>	
-si	<# of connected UPS>	Store the number of UPS systems connected to the Master system, and the slave IDs of each connected UPS in hexadecimal format.
	<slave ID1 in hex> <slave ID2 in hex> <slave ID3 in hex>...	
-id	<slave ID in hex>	Store the slave ID of the UPS in hexadecimal format.
	<id>	Five character unique ID of the UPS.
-d	<delay in seconds>	Specify delay before second connection if first attempt is unsuccessful.
-test	<appearance | disappearance>	Create a test alarm. Only alarms specified by the Call Cause mask will be raised.
	<bit position>	Specify the bit position (0 - 15) that will be set in the appearance and disappearance register.
-initstr	<apc | mge | any other string>	Set the modem INIT string.
-dialstr	<apc | mge | any other string>	Set the modem DIAL string.
-ResetToDef		Restore the default settings for the TLS feature.

uio

Access: Administrator, Device User

Description: This command is available for an AP9631 and AP9635 Network Management Card with a connected Dry Contact I/O Accessory (AP9810).

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

Example 1: To open the output, type:

```
uio -rc 2 open
```

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

```
uio -st 2
```

ups

|

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

Access: Administrator, Device User

Description: View UPS status information.

Option	Argument	Description
-input	<phase#> | all	Display the input measurements for the chosen phase of the UPS. Typing “all” displays the information for all phases of the UPS.
	voltage | current | frequency | all	Specify the input measurement for the `ups` command. **Example:** `ups -input 2 frequency` Displays the frequency for phase 2 of the UPS.
-bypass	<phase#> | all	Display the input measurements for the chosen phase of the bypass main. Typing “`all`” displays all phases of the bypass main.
	voltage | current | frequency | all	Specify the input measurement for the `ups` command. **Example:** `ups -bypass 2 current` Displays the current for phase 2 of the bypass main.

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

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.

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 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 “Use a USB drive to transfer the files” on page 87 for descriptions of the transfer result codes.

Web Interface

Introduction

Overview

The Web interface provides options to manage the Management Card and view the status of its UPS.

See “Web” on page 59 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.

Note: All UPS settings and alarm thresholds must be configured at the user interface display of the UPS.

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 by American Power Conversion.

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

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

Note: If you are using HTTPS (SSL/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 30.

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:

Icon	Description
✖	**Critical**: A critical alarm exists, which requires immediate action.
⚠	**Warning**: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
✔	**No Alarms**: 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, configure PowerChute Network Shutdown, and view information about the UPS.
- **Sensor**: View and configure temperature sensor data. (Only present if a Dry Contact Sensor (AP9810), Temperature Sensor (AP9335T), or Temperature and Humidity Sensor (AP9335TH) is connected.)
- **Logs**: View and configure event and data logs.
- **Administration**: Configure security, network connection, notification, and general settings.

Menus

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

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

Top menu bar. The **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 American Power Conversion Web-enabled products
- **Link 3**: Information on Remote Monitoring Services

To reconfigure the links, see “Configure Links” on page 75.

Monitor the UPS and Configure Shutdowns

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, icons and accompanying text indicate the operating state of the UPS:

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

Quick Status

The following information is displayed.

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

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

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

- In a list:
  - **Input Voltage**: The AC voltage (VAC) being received by each phase of the UPS.
  - **Output Voltage**: The AC voltage (VAC) each phase of the UPS is providing to its load.
  - **Ambient Temperature**: The highest internal temperature reported by the power modules in the UPS. (Symmetra models only)
  - **Runtime Remaining**: How long the UPS can use battery power to support its attached equipment.
  - **Module Redundancy**: The number of power modules which can fail or be removed without causing the Symmetra PX UPS to switch to bypass operation. For example, with n+2 redundancy, two power modules could fail or be removed without causing the UPS to enter bypass mode. (Symmetra models only)
  - **System Redundancy**: (applicable for Parallel configurations only) This displays the number of backup or redundant UPS devices set up on your parallel system. For example, n+0 indicates that there is no redundant UPS power, n+1 indicates that there is one UPS for redundant power, etc. When the load on your system starts using some of the redundant power, the system generates an alarm.
  - **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 an option under the **Status** heading on the left navigation menu of the **UPS** tab.

Model-specific status displayed

To view detailed information about status items specific to the UPS model associated with the Management Card, click the Help link in the upper right corner of the user interface.

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

- **Internal Temperature**—The temperature inside the UPS
- **Voltage, Current, and Frequency information**, such as input and output voltage, input and output current, input frequency, input voltage in bypass mode, and minimum and maximum input voltage during the last minute.
- **UPS Load information**, such as the load placed on the UPS in kVA or as a percentage of available kVA or Watts.
- **Fault Tolerance information**, such as redundant power available.
- **Battery information**, such as available battery capacity, percentage of full battery capacity, battery output current, rated voltage capacity of batteries, amp-hour rating of battery cabinets, number of batteries installed, and number of faulty batteries.
- **Status of internal and external components**, such as intelligence and power modules, circuit breaker box, external switch gear, and transformer.

The PowerChute Option

The **PowerChute** option, available in the left navigation menu of the **UPS** tab, 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 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

The PowerChute Network Shutdown software must be installed on each client you add.

Click **Add Client** for a field in which to enter the IP address of a new PowerChute Network Shutdown client. The list can contain the IP addresses of up to 50 clients.

To delete a client, click the IP address of that client in the list, and then click **Delete Client**.

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	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. When **Force Negotiation** is selected, the Network Management Card polls each server listed as a PowerChute Network Shutdown client for information on the time it needs for a graceful shutdown. This delay is recalculated whenever the management interface of the UPS turns on or is reset. (This option is not available for the Galaxy 300 or Galaxy 7000 UPS devices.) **Maximum Required Delay** is the longest shutdown delay needed by any server on the list, plus two additional minutes to allow for unforeseen circumstances. The negotiation can take up to 10 minutes. If you do not select **Force Negotiation**, two minutes is used by default as the shutdown delay for all clients.
On-Battery Shutdown Behavior	After the PowerChute Network Shutdown clients shut down their computer systems, this parameter determines whether the UPS turns on automatically or must be turned on manually when input power is restored. **Note:** This option is not available on the MGE Galaxy 300 or MGE Galaxy 7000 UPS.
Authentication Phrase	The case-sensitive phrase of 15 to 32 ASCII characters to be used during MD5 authentication for PowerChute communication. The default Administrator setting is **admin user phrase**.

Note: By default, the PowerChute clients initiate a graceful shutdown when the UPS has 120 seconds of runtime remaining. If the servers need additional time to shut down safely, configure the **Low battery alarm threshold** setting at the user interface display of the Symmetra PX 250 or Symmetra PX 500 UPS. From the UPS System screen on the user interface display, select **User Configuration**, then **Alarm Settings**. The valid range for the **Low battery alarm threshold** is 0 (no shutdown will occur) to 3600 seconds (1 hour).

For MGE Galaxy models, you must use the UPS Tuner to set the shutdown time.

The About Option

This option provides the following information about the UPS:

- **Model**: The model name of the UPS.
- **Serial Number**: The unique identification number of the UPS, also provided on the UPS.
- **Firmware Revision:** The revision numbers of the firmware modules installed on the UPS
- **Manufacture Date**: The date on which the manufacturing of this UPS was completed. (Symmetra models only)

In addtion to the information listed above, the MGE Galaxy 300 and MGE Galaxy 7000 UPS systems report the following information:

- **Product Name**: The brand name of the UPS
- **Technical Level**: The revision numbers of the firmware modules currently installed on the UPS.
- **Country**: The country where the UPS is located. (MGE Galaxy 7000 only)
- **Manufacturer Name**: The manufacturer of the UPS.
- **UPS Time**: The local time at the location of the UPS.

Environmental Monitoring

Note: If you install a Dry Contact I/O Accessory, AP9810, at your Network Management Card, the **Environment** tab displays two top menu bar options, **Universal I/O** and **Environment**. Except where noted, the settings described in this chapter are available for both options.

Overview Page

The **Overview** page lists the status of environmental monitoring devices associated with the AP9635 Network Management Card on a Symmetra-series or MGE Galaxy UPS.

Note: The AP9635 can only have one universal sensor attached at a time. Depending on which sensor is attached, a subset of the following headings will be displayed.

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

Temperature and Humidity Page

Brief status

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

Detailed status and configuration

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

Identification and alarm status.

Parameter	Description
Name	A name for this sensor. *Maximum*: 20 characters.
Location	This physical location of the sensor. *Maximum*: 20 characters.
Alarm Status	One of the following is displayed: • **Normal** if this sensor is not reporting an alarm condition. • If this sensor is in an alarm state, the text of the alarm, indicating which threshold is violated, and the severity of the alarm, indicated by color (red for critical, orange for warning).
Thresholds	See the next two sections for descriptions of the configurable thresholds and **Hysteresis** values.

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

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

Hysteresis. 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

Brief status

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

Detailed status and configuration

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

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

Output Relay Page

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

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

About Page

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

Configuring the Control Policy

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

Configuring an output to respond to an event

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

Configuring the UPS or output to respond to an input alarm

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

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

Logs

Use the Event and Data Logs

Event log

Path: Logs > Events > ***options***

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

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

See "Configuring by event" on page 66.

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 47.

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**. Unmark the check box of an event category or alarm severity level to remove it from view. Text at the upper right corner of the event log page indicates that a filter is active. As Administrator, click **Save As Default** to save this filter as the default log view for all users. If you do not click **Save As Default**, the filter is active until you clear it or until the Management Card restarts. Non-Administrator filters are active until the user logs out, then the default is re-applied.To remove an active filter, click **Filter Log**, then **Clear Filter (Show All)**.

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

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

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

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

To disable the logging of events based on their assigned severity level or their event category, see “Configuring by group” on page 66.

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 47.

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 Secure CoPy (SCP) to view the data log. See "How to use FTP or SCP to retrieve log files" on page 47.

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 graph the log data (Logs > Data > graphing):

Note: Graphing is only available on the MGE Galaxy 300 and MGE Galaxy 7000 UPS.

Data log graphing provides a graphical display of logged data and is an enhancement of the existing data log feature. How the graphing enhancement displays data and how efficiently it performs will vary depending on your computer hardware, computer operating system, and the Web browser you use to access the interface of the unit.

Many advanced JavaScript® features are required for data log graphing; to use this enhancement, JavaScript must be enabled in your browser. Alternatively, you can use FTP or SCP to import the data log into a spreadsheet application, and graph data in the spreadsheet.

Graphing large amounts of data may cause performance problems on the computer and Web browser you are using. Reducing the number of data points or data lines being graphed may improve performance.

Parameter	Description
Graph Data	To graph multiple data items, select the data items that correspond to the abbreviated column headings in the data log. Only four items can be selected at a time.
Graph Time	To graph all records, or to change the number of hours, days, or weeks for which data log information is graphed, select Last. Select an option from the drop-down menu, then click Apply. To graph data logged during a specific time range, select From. Specify the beginning and ending dates and times for which to graph data, then click Apply. **Note:** Enter the time using the 24-hour clock format.

To display the graph containing the selected data on the current web page, click **Apply**.

To display the graph in a new window, click **Launch Graph in New Window**.

For instructions on graph navigation and details, please see the online help, available by clicking **Help** in the upper right corner of the web page.

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

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

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

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

Parameter	Description
Data Log Rotation	Enable or disable (the default) data log rotation.
FTP Server Address	The location of the FTP server where the data repository file is stored.
User Name	The user name required to send data to the repository file. This user must also be configured to have read and write access to the data repository file and the directory (folder) in which it is stored.
Password	The password required to send data to the repository file.
File Path	The path to the repository file.
Filename	The name of the repository file (an ASCII text file).
Unique File Name	When checked, the current datestamp will be appended to the selected file before sending the data to the FTP server.

Parameter	Description
Delay *X* hours between uploads.	The number of hours between uploads of data to the file.
Upload every *X* minutes	The number of minutes between attempts to upload data to the file after an upload failure.
Up to *X* times	The maximum number of times the upload will be attempted after an initial failure.
Until Upload Succeeds	Attempt to upload the file until the transfer is completed.

To 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 47.

When the log is full, 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.csv*) or data log file (*data.csv*) 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.csv* 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 SCP to retrieve the log file.

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

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

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

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

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

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

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

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

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

   ```
   ftp>open ip_address port_number
   ```

   To set a non-default port value to enhance security for the FTP Server, see "Modbus" on page 63. 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.csv
   ```

   or

   ```
   ftp>get data.csv
   ```

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

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

   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.csv* file records the event.

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

Syslog servers

Administrators can configure up to four Syslog servers to recieve notifications of events.

Managing the Syslog servers (Logs > Syslog > servers):

To add a new Syslog server, click **Add Server.**

To modify an existing Syslog server, click the server's name.

Parameter	Description
Syslog Server	The server's IP address or host name.
Port	The port number to which Syslog messages will be sent. The default and well known port is 514.
Protocol	Choose a protocol.
Language	Choose a language.

Configuring the Syslog settings (Logs > Syslog > settings):

Parameter	Description
Message Generation	Enable the generation (and therefore the logging) of Syslog messages for events that have Syslog configured as a notification method. To configure notification methods for events, select the **Administration** tab, the **Network** menu on the top menu bar, and one of the Event Actions options on the left navigation menu.
Facility Code	Messages of this device will be categorized by the facility selected. Categorization allows Syslog messages from different devices to be placed in separate logs.
Severity Mapping	Maps each severity level of an American Power Conversion device event or system event to an available Syslog priority in the drop-down list. The local severity options are Critical, Warning, and Informational.

Testing the Syslog settings (Logs > Syslog > test):

Parameter	Description
Last Test Result	The result of the last test performed.
Server	The message will be sent to all configured servers.
Severity	Select a severity level (Syslog priority) for the test message.
Test Message	Format the message to consist of the event type (APC, System, or Device, for example) followed by a colon, a space, and the event text. The message can have a maximum of 50 characters.

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 and on the APC Web site at **www.apc.com**.

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

- 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.

⚠ **Caution:** 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 on a link, and configure the parameters for authentication by a new RADIUS server.
- Click a listed RADIUS server to display and modify its parameters.

RADIUS Setting	**Definition**
RADIUS Server	The server name or IP address (IPv4 or IPv6) of the RADIUS server. Click on a link to configure the server. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.
Secret	The shared secret between the RADIUS server and the 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.

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

Configuring a RADIUS server on UNIX® with shadow passwords

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

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

```
DEFAULTAuth-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

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

Inactivity Timeout

Path: Administration > Security > Auto Log Off

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

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

Administration: Network Features

TCP/IP and Communication Settings

TCP/IP settings

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

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

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

Setting	Description
Enable	Enable or disable IPv4 with this check box.
Manual	Configure IPv4 manually by entering the IP address, subnet mask, and default gateway.
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Management Card requests network assignment from any BOOTP server: • If the Management Card receives a valid response, it starts the network services. • 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. • 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. Click **Next>>** to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail [1]: • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. • **If retries fail**: Select **Use prior settings** (the default) or **Stop BOOTP request**.
DHCP	The default setting. At 32-second intervals, the Management Card requests network assignment from any DHCP server. • If the Management Card receives a valid response, it does not (as previously) require the APC cookie from the DHCP server in order to accept the lease and start the network services. • If the 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[1]. • **Require vendor specific cookie to accept DHCP Address**: By selecting this check box, you can require the DHCP server to provide a cookie which supplies information to the Management Card.

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

DHCP response options

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

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 American Power Conversion-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 American Power Conversion devices.

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

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

TCP/IP options. The 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,** i.e., 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 an user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the 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.

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

Setting	Description
Enable	Enable or disable IPv6 with this check box.
Manual	Configure IPv6 manually by entering the IP address and the default gateway.
Auto Configuration	When the Auto Configuration check box is selected, the system obtains addressing prefixes from the router (if available). It uses those prefixes to automatically configure IPv6 addresses.
DHCPv6 Mode	**Router Controlled**: Selecting this option means that DHCPv6 is controlled by the Managed(M) and Other(O) flags received in IPv6 router advertisements. When a router advertisement is received, the Management Card checks whether the M or the O flag is set. The Management Card interprets the state of the M (Managed Address Configuration Flag) and O (Other Stateful Configuration Flag) "bits" for the following cases: • *Neither is set*: Indicates the local network has no DHCPv6 infrastructure. The Management Card uses router advertisements and manual configuration to get addresses that are not link-local and other settings. • *M, or M and O are set*: In this situation, full DHCPv6 address configuration occurs. DHCPv6 is used to obtain addresses AND other configuration settings. This is known as `DHCPv6 stateful`. Once the M flag has been received, the DHCPv6 address configuration stays in effect until the interface in question has been closed. This is true even if subsequent router advertisement packets are received in which the M flag is not set. If an O flag is received first, then an M flag is received subsequently, the Management Card performs full address configuration upon receipt of the M flag • *Only O is set*: In this situation, the Management Card sends a DHCPv6 Info-Request packet. DHCPv6 will be used to configure “other” settings (such as location of DNS servers), but NOT to provide addresses. This is known as `DHCPv6 stateless`. **Address and Other Information:** With this radio box selected, DHCPv6 is used to obtain addresses AND other configuration settings. This is known as `DHCPv6 stateful`. **Non-Address Information Only**: With this radio box selected, DHCPv6 will be used to configure "other" settings (such as location of DNS servers), but NOT to provide addresses. This is known as `DHCPv6 stateless`. **Never**: Select this to disable DHCPv6.

Ping Response

Path: Administration > Network > Ping Response

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

Port Speed

Path: Administration > Network > Port Speed

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

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

DNS

Path: Administration > Network > DNS > *options*

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

- Select **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 (IPv4)**: 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.
- **Domain Name (IPv6)**: Specify the IPv6 domain name here.

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

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

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

Web

Path: Administration > Network > Web > *options*

Option	Description

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

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

Console

Path: Administration > Network > Console > *options*

Option	Description

access	Choose one of the following for access by Telnet or Secure SHell (SSH):
	• **Disable**: Disables all access to the command line interface.
	• **Enable Telnet** (the default): Telnet transmits user names, passwords, and data without encryption.
	• **Enable SSH**: SSH transmits user names, passwords, and data in encrypted form, providing protection from attempts to intercept, forge, or alter data during transmission.
	
	Configure the ports to be used by these protocols:
	• **Telnet Port**: 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:
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• **SSH Port**: 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.

ssh host key	**Status** indicates the status of the host key (private key): • **SSH Disabled: No host key in use**: When disabled, SSH cannot use a host key. • **Generating**: The Management Card is creating a host key because no valid host key was found. • **Loading**: A host key is being activated on the Management Card. • **Valid**: One of the following valid host keys is in the **/ssh** directory (the required location on the Network Management Card): •A 1024-bit or 2048-bit host key created by the Security Wizard •A 2048-bit RSA host key generated by the Network Management Card **Add or Replace**: Browse to and upload a host key file created by the Security Wizard. To use the Security Wizard, see the *Security Handbook* on the APC Network Management Card *Utility* CD. **NOTE:** To reduce the time required to enable SSH, create and upload a host key in advance. **If you enable SSH with no host key loaded, the Management Card takes up to one minute to create a host key, and the SSH server is not accessible during that time.** **Remove**: Remove the current host key.

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

SNMP

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 the InfraStruxure device to receive traps from the Management Card, but Write access is required while you use the interface of the Management Card to set the InfraStruxure device as a trap receiver.

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

SNMPv1

Path: Administration > Network > SNMPv1 > *options*

Option	Description
access	**Enable SNMPv1 Access**: Enables SNMP version 1 as a method of communication with this device.
access control	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. • If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network. • If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device. **Community Name**: The name that 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 `public`, `private`, `public2`, and `private2`. **NMS IP/Host Name**: The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows: • 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment. • 149.225.**255.255**: Access only by an NMS on the 149.225 segment. • 149.**255.255.255**: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. **Access Type**: The actions an NMS can perform through the community. • **Read**: GETS only, at any time • **Write**: GETS at any time, and SETS when no user is logged onto the Web interface or command line interface. • **Write+**: GETS and SETS at any time. • **Disable**: No GETS or SETS at any time.

SNMPv3

Path: Administration > Network > SNMPv3 > *options*

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

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

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

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

Option	Description
access control	You can configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles, but you can edit these settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks. • If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device. • If you configure multiple access entries for one user profile, the limit of four entries requires that one or more of the other user profiles must have no access control entry. If no access control entry is listed for a user profile, no NMS that uses that profile has any access to this device. To edit the access control settings for a user profile, click its user name. **Access**: Mark the **Enable** check box to activate the access control specified by the parameters in this access control entry. **User Name**: From the drop-down list, select the user profile to which this access control entry will apply. The choices available are the four user names that you configure through the **user profiles** option on the left navigation menu. **NMS IP/Host Name**: The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contain 255 restricts access as follows: • 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment. • 149.225.**255.255**: Access only by an NMS on the 149.225 segment. • 149.**255.255.255**: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

Modbus

Path: Administration > Network > Modbus > serial (or TCP)

Enable or disable access to the Modbus serial or TCP interface by selecting or clearing the **Enable** check box.

Set the connection parameters for the Modbus connection - a port number for the TCP connection, or the parameters for the serial connection. The default serial connection settings are 19200 baud, 1 start bit, 8 data bits, even parity, and 1 stop bit.

Note: If you select **None**, the Modbus master should be set to use 2 stop bits. For **Even** or **Odd**, use 1 stop bit.

Set the unique ID for the device by providing a value in the **Target Unique ID** field. The value must be between 1 and 247 (inclusive).

When you are finished making your selections, click **Apply** to save your changes.

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 APC Network Management Card *Utility* CD or from the APC Web site.

Administration: Notification

Event Actions

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

Types of notification

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

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

  You can also log system performance data to use for device monitoring. See "Data log" on page 44 for information on how to configure and use this data logging option.

  – Queries (SNMP GETs)

  For more information, see "SNMP" on page 61. SNMP enables an NMS to perform informational queries. For SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without the risk of allowing remote configuration changes.

Configuring event actions

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

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

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

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

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

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

- "Identifying Syslog Servers" on page 70
- "E-mail recipients" on page 68
- "Trap Receivers" on page 69

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 57.

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

  See “SMTP” on page 67.

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

  See “E-mail recipients” on page 68.

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

SMTP.

Path: Administration > Notification > E-mail > server

Setting	Description
Local SMTP Server	The IP address or DNS name of the local SMTP server. **NOTE:** This definition is required only when **SMTP Server** is set to **Local**. See “E-mail recipients” on page 68.
From Address	The contents of the **From** field in e-mail messages sent by the Management Card: • In the format *user@* [*IP_address*] (if an IP address is specified as **Local SMTP Server**) • In the format *user@domain* (if DNS is configured and the DNS name is specified as **Local SMTP Server**) in the e-mail messages. **NOTE:** The local SMTP server may require that you use a valid user account on the server for this setting. See the server’s documentation.

E-mail recipients.

Path: Administration>Notification>E-mail>recipients

Identify up to four e-mail recipients.

Setting	Description
To Address	The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, **myacct100@skytel.com**). The pager gateway will generate the page. To bypass the DNS lookup of the mail server's IP address, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly. **NOTE:** The recipient's pager must be able to use text-based messaging. The MGE Galaxy 300, MGE Galaxy 7000, Symmetra PX 250, and Symmetra PX 500 UPS devices do not support paging.
E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.
SMTP Server	Select one of the following methods for routing e-mail: • **Local**: 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: • 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. • Set up a special e-mail account for the Management Card to forward e-mail to an external mail account. • **Recipient**: 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. When the recipient uses the Management Card's SMTP server, this setting has no effect.
Format	The long format contains Name, Location, Contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.
Language	Chose a language from the drop-down list and any mails will be sent in that language. It is possible to use different languages for different users.
User Name Password Confirm Password	If your mail server requires authentication, type your user name and password here. This performs a simple authentication, not SSI.

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 open the page for configuring a new trap receiver, click **Add Trap Receiver**.
- To modify or delete a trap receiver, first click its IP address or host name to access its settings. (If you delete a trap receiver, all notification settings configured under Event Actions for the deleted trap receiver are set to their default values.)
- To specify the trap type for a trap receiver, select either the SNMPv1 or SNMPv3 radio button. For 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.
Language	Chose a language from the drop-down list. This can differ from the UI and from other trap receivers.

SNMPv1 option.

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

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

See “SNMPv3” on page 62 for information on creating user profiles and selecting authentication and encryption methods.

SNMP Trap Test

Path: Administration > Notification > SNMP Traps > test

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

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

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

Remote Monitoring Service

Path: Administration > Notification > Remote Monitoring

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

To purchase the RMS service, contact your American Power Conversion vendor or see the RMS Web site, **rms.apc.com**.

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

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

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 IPv4/ IPv6 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 **514**, the UDP port assigned to Syslog.
Protocol	Choose between UDP and TCP.
Language	Choose the language for any Syslog messages.

Syslog Settings.

Path: Logs > Syslog > settings

Setting	Definition
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the Management Card's Syslog messages (**User**, by default). **NOTE: User** best defines the Syslog messages sent by the Management Card. **Do not** 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: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** **NOTE:** To disable Syslog messages, see "Configuring event actions" on page 65.

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 and the APC Web site, **www.apc.com**.

The **Name** and **Location** fields also identify the device when you register for the Remote Monitoring Service. See “Remote Monitoring Service” on page 77 for more information.

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.
  - – Select the check box **Apply Local Computer Time** to match the date and time settings of the computer you are using.
- **Synchronize with NTP Server**: Have an NTP Server define the date and time for the 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. *Minimum*: 1; *Maximum*: 8760 (1 year).
Update Using NTP Now	Initiate an immediate update of date and time by the NTP Server.

Daylight saving

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

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

When customizing Daylight Saving Time (DST):

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

Format

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

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

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 (e.g., 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 79.

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 American Power Conversion .ini file utility, available from **www.apc.com/tools/download**.

Event Log, Temperature Units, and Log-In Page

Path: Administration > General > Preferences

Color-code event log text

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

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

Change the default temperature scale

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

Specify the UI language

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

Note: You can also specify different languages for e-mail recipients and SNMP trap receivers. See “E-mail recipients” on page 75 and “Trap Receivers” on page 76.

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[1]	Clear the **Exclude TCP/IP** check box to reset all configuration values; select the **Exclude TCP/IP** check box to reset all values except TCP/IP
Reset Only[1]	**TCP/IP settings**: Set TCP/IP Configuration to **DHCP & BOOTP**, its default setting, requiring that the Management Card receive its TCP/IP settings from a DHCP or BOOTP server. See“TCP/IP and Communication Settings” on page 54.
	Event configuration: Reset all changes to event configuration, by event and by group, to their default settings.
1. Resetting may take up to one 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 American Power Conversion Web-enabled products.
- **Link 3**: The home page of the 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 APC Customer Support for troubleshooting problems with the Management Card. The serial number and MAC address are also available on the Management Card.

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

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

Device IP Configuration Wizard

Capabilities, Requirements, and Installation

How to use the Wizard to configure TCP/IP settings

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

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

System requirements

The Wizard runs on Microsoft Windows 2000, Windows Server® 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 **www.apc/tools/download**.
2. Download the Device IP Configuration Wizard.
3. Run the executable file in the folder to which you downloaded it.

Use the Wizard

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

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 or network-enabled devices, obtain the MAC address of each one to identify it when the Wizard discovers it. (The Wizard displays the MAC address on the screen on which you then enter the TCP/IP settings.)
   - For a Management Card that you install, the MAC address is on a label on the bottom of the card.
   - For a network-enabled device (with an embedded Management Card), the MAC address is on a label on the device.
   - You can also obtain the MAC address from the Quality Assurance slip that came with the Management Card or device.

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

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

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

Configure or reconfigure the TCP/IP settings locally

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

How to Export Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

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 American Power Conversion .ini file utility.

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 APC Network Management Card *Utility* CD and at **www.apc.com**.

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

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   - Enclose in quotation marks any values that contain leading or trailing spaces or are already enclosed in quotation marks.
   - To export scheduled events, configure the values directly in the .ini file.
   - To export a system time with the greatest accuracy, if the receiving 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, i.e., FTP, FTP Client, SCP, or TFTP. The following example uses FTP:
  a. From the folder containing the copy of the customized .ini file, use FTP to log in to the 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 American Power Conversion .ini file utility.

  To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* on the APC 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, an additional event text states the error.

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

Messages in config.ini

A device associated with the 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, for another reason, 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 79 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, you can delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Related Topics

On Windows operating systems, instead of transferring .ini files, you can use the 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 76.

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 three modules: An APC 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 APC 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 American Power Conversion file.
- ***`hardware-version`***: `hw0`*`x`* identifies the version of the hardware on which you can use this binary file.
- ***`type`***: Identifies whether the file is for the APC Operating System (AOS) module, the application module, or the boot monitor module for the Management Card.
- ***`firmware-version`*****:** Identifies the version number of the file.
- `bin`: Indicates that this is a binary file.

Obtain the latest firmware version

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

NMC2 Firmware Upgrade Utility for Microsoft Windows systems. The NMC2 Firmware Upgrade Utility automates the transferring of the firmware modules on any supported Windows operating system. Obtain the latest version of the utility at no cost from **www.apcc.com/tools/download**. At this Web page, find the latest firmware release for your American Power Conversion product and, included in it, the automated utility. **Never** use a utility designated for one American Power Conversion product to upgrade the firmware of another American Power Conversion product.

Manual upgrades, primarily for Linux systems. If no computer on your network is running a Microsoft Windows operating system, you must upgrade the firmware of your 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 **www.apcc.com/tools/download**, then extracting the firmware files from the tool.

Note: In manual upgrades, load the boot monitor module first, then the American Power Conversion operating system module, and finally, the application module.

To extract the firmware files:

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

Firmware File Transfer Methods

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 NMC2 Firmware Upgrade Utility downloaded from the APC Web site.

  Note: The utility only works with a Management Card that has an IPv4 address.

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

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

- Use a USB drive to transfer the individual firmware modules from your computer to the NMC.

Use FTP or SCP to upgrade one Management Card

FTP. For you 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 84).

To transfer the files:

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

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

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

   - apc_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 of a space 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 as 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 American Power Conversion 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 APC Network Management Card *Utility* CD.

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

Using the NMC2 Firmware Upgrade Utility for multiple upgrades

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

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

   The new utility works fine with any existing `iplist.txt` file that you have used with the old version of the utility.
3. Select the **Upgrade From Device List** check box to use the `iplist.txt` file. Clear this check box to upgrade the firmware using the IP, user name and password you typed on the dialog box.
4. Choose the **Upgrade Now** button to start the firmware version update(s).

Choose **View Log** to verify any upgrade.

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 84).

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 83.

Use a USB drive to transfer the files

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

1. Download the update files and unzip them.
2. Create a folder named `apcfirm` on the USB drive.
3. Place the extracted files in the `apcfirm` directory.
4. Insert the USB drive into any USB port on the Network Management Card 2.
5. Reset the Network Management Card 2 and wait for the card to reboot fully.
6. Check that the upgrade was completed successfully using the procedures in “Verifying Upgrades and Updates” on page 87.

Verifying Upgrades and Updates

Verify the success or failure of the transfer

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

Last Transfer Result codes

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

Verify the version numbers of installed firmware.

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

Adding and Changing Language Packs

Note: Language packs are not available for the MGE Galaxy 300 or MGE Galaxy 7000. The Symmetra PX 250 and Symmetra PX 500 do not support Italian or Japanese as options for the language packs.

The Network Management Card 2 language pack files contain the information required to display the user interface in languages other than English. Each language pack can contain up to five languages (this is why the **Language** drop-down box has up to five languages to choose from when you log on).

The full list of available languages is French, Italian, German, Spanish, Brazilian Portuguese, Russian, Korean, Japanese, and Simplified Chinese. The language pack files are available for distribution through your Field Service Engineer. The labelling tells you the languages in each pack and the product line, e.g. Symmetra, Symmetra 3-Phase, and Smart-UPS.

To use a language that is not currently available on your user interface, download the language pack from the website, and follow these steps:

1. Connect to the Management Card using FTP.
2. Transfer the required language pack to the Management Card. For example, type:
   ```
   put <full path/language pack name>.lpk
   ```
3. When the file finishes the transfer, log off FTP and the Management Card will reboot.
4. When the reboot is complete, the new language pack is ready for use.

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

Troubleshooting

Management Card Access Problems

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

If the problem still persists, see “APC Worldwide Customer Support” on page 96.

Problem	**Solution**
Unable to ping the Management Card	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: • Verify that the Management Card is properly seated in the UPS. • Verify all network connections. • Verify the IP addresses of the Management Card and the NMS. • 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). • Verify the number of subnet bits for the Management Card’s subnet mask.
Cannot allocate the communications port through a terminal program	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.
Cannot access the command line interface through a serial connection	Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.
Cannot access the command line interface remotely	• Make sure you are using the correct access method, Telnet or Secure SHell (SSH). An Administrator can enable these access methods. By default, Telnet is enabled. Enabling SSH automatically disables Telnet. • For SSH, the 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.
Cannot access the Web interface	• Verify that HTTP or HTTPS access is enabled. • Make sure you are specifying the correct URL — one that is consistent with the security system used by the Management Card. SSL requires **https**, not **http**, at the beginning of the URL. • Verify that you can ping the Management Card. • Verify that you are using a Web browser supported for the Management Card. See “Supported Web browsers” on page 28. • 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.

SNMP Issues

Problem	Solution
Unable to perform a GET	• Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3). • Use the command line interface or Web interface to ensure that the NMS has access. See “SNMP” on page 61.
Unable to perform a SET	• Verify the read/write (SET) community name(SNMPv1) or the user profile configuration (SNMPv3). • Use the command line interface or Web interface to ensure that the NMS has write (SET) access (SNMPv1) or is granted access to the target IP address through the access control list (SNMPv3). See “SNMP” on page 61.
Unable to receive traps at the NMS	• Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the NMS as a trap receiver. • For SNMP v1, query the **mconfigTrapReceiverTable** APC MIB OID to verify that the NMS IP address is listed correctly and that the community name defined for the NMS matches the community name in the table. If either is not correct, use SETs to the **mconfigTrapReceiverTable** OIDs, or use the command line interface or Web interface to correct the trap receiver definition. • For SNMPv3, check the user profile configuration for the NMS, and run a trap test. See “SNMP” on page 61, “Trap Receivers” on page 69, and “SNMP Trap Test” on page 69.
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.

Appendix A: List of Supported Commands

```
?

about

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

boot
[-b <dhcp | bootp | manual>]
[-c <dhcp cookie> [enable | disable]]
[-v <vendor class>]
[-i <client id>]
[-u <user class>]

cd

console
[-S <disable | telnet | ssh>]
[-pt <telnet port #>]
[-ps <ssh port #>]
[-b <baud rate> [2400 | 9600 | 19200 | 38400]]

date
[-d <"datestring">]
[-t <00:00:00>]
[-f [mm/dd/yy | dd.mm.yyyy | mmm-dd-yy |
dd-mmm-yy | yyyy-mm-dd]]
[-z <time zone offset>]

delete

dir

dns
[-OM [enable | disable]]
[-p <primary DNS server>]
[-s <secondary DNS server>]
[-d <domain name>]
[-n <domain name IPv6>]
[-h <host name>]

eventlog

exit

format

ftp
[-p <port number>]
[-S <enable | disable>]

help

modbus
[-p]
[-a [enable | disable]]
[-br [9600 | 19200]]
[-pr [even | odd | none]]
[-s <slave # in hex>]
[-o [master | slave]]
[-rt <timeout in mSec>]
[-sr <scan rate in mSec>]
[-rep <# of repetitions>]
[-ResetToDef]

netstat

ntp
[-OM [enable | disable]]
[-p <primary NTP server>]
[-s <secondary NTP server>]

ping
[<IP address or DNS name>]

portspeed
[-s [auto | 10H | 10F | 100H | 100F]]

prompt
[-s [long | short]]

quit

radius
[-a <access> [local | radiusLocal | radius]]
[-p# <server IP>]
[-s# <server secret>]
[-t# <server timeout>]

reboot

resetToDef
[-p [all | keepip]]

snmp
[-S [enable|disable]]

snmp3
[-S [enable|disable]]

system
[-n <system name>]
[-c <system contact>]
[-l <system location>]
```

```
tcpip
[-S [enable | disable]]
[-i <IP address>]
[-s <subnet mask>]
[-g <gateway>]
[-d <domain name>]
[-h <host name>]

tcpip6
[-S [enable | disable]]
[-man [enable | disable]]
[-auto [enable | disable]]
[-i <IPv6 address>]
[-g <IPv6 gateway>]
[-d6 [router | stateful | stateless | never]]
tls
[-p]
[-a [enable | disable]]
[-m <slave # in hex> <call cause mask in hex>]
[-t [primary | secondary] <telephone #>]
[-si <# of connected UPS><slaveID1 in hex>...]
[-id <slave ID in hex> <id>]
[-d <delay in seconds>]
[-test [appearance | disappearance] <bit position>]
[-initstr [apc | mge | <any other string>]]
[-dialstr [apc | mge | <any other string>]]
[-resettodef]

uio
[-rc <dI> [open | close]
[-st <port # | port #]]
[-disc <port # | port #]]

ups
[-input [<phase#> | all] [voltage | current | frequency | all]]
[-bypass [<phase#> | all] [voltage | current | frequency | all]]
[-output [<phase#> | all] [voltage | current | load | percload | pf | frequency | all]]
[-batt]
[-about]
[-al [c | w]]

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

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

xferINI

xferStatus
```

Two-Year Factory Warranty

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

Terms of warranty

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

Non-transferable warranty

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

Exclusions

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

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

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

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

Warranty claims

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

APC Worldwide Customer Support

Customer support for this or any other APC product is available at no charge in any of the following ways:

- Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
  - **www.apc.com** (Corporate Headquarters)
    Connect to localized APC Web sites for specific countries, each of which provides customer support information.
  - **www.apc.com/support/**
    Global support searching APC Knowledge Base and using e-support.
- Contact the APC Customer Support Center by telephone or e-mail.
  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

For information on how to obtain local customer support, contact the APC representative or other distributors from whom you purchased your APC product.