User Guide

Network Management Card for Easy UPS, 1-Phase & 3-Phase

AP9544, AP9547

990-91545C-001
07/ 2023

Schneider Electric

Schneider Electric Legal Disclaimer

The information presented in this manual is not warranted by Schneider Electric to be authoritative, error free, or complete. This publication is not meant to be a substitute for a detailed operational and site specific development plan. Therefore, Schneider Electric assumes no liability for damages, violations of codes, improper installation, system failures, or any other problems that could arise based on the use of this Publication.

The information contained in this Publication is provided as is and has been prepared solely for the purpose of evaluating data center design and construction. This Publication has been compiled in good faith by Schneider Electric. However, no representation is made or warranty given, either express or implied, as to the completeness or accuracy of the information this Publication contains.

IN NO EVENT SHALL SCHNEIDER ELECTRIC, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF SCHNEIDER ELECTRIC OR THEIR RESPECTIVE OFFICERS, DIRECTORS, OR EMPLOYEES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF SCHNEIDER ELECTRIC HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

Contents

Introduction 1

Product Description 1

Features 1
Supported Devices 2
IPv4 initial setup 2
IPv6 initial setup 2
Network management with Other Applications 3

Internal Management Features 4

Overview 4
Access priority for logging on 4
Types of user accounts 4

How to Reset after a Lost Password 5

Front Panel (AP9544/AP9547) 6

LED Descriptions 7

Status LED 7
Link-RX/TX (10/100/1000) LED 7

Watchdog Features 8

Overview 8
Network interface watchdog mechanism 8
Resetting the network timer 8
Automatic Logout 8

Web User Interface 9

Introduction 9

Overview 9
Supported Web browsers 9

How to Log On 9

Overview 9
URL address formats 10
First log in 10

Home Screen 11
Overview 11
Icons and Links 11

Monitoring the UPS: Status menu 12

UPS on Status menu 12

Overview on Status menu 13

Measurements on Status menu 14

Network on Status menu 15

Maintenance on Status menu 15

Controlling the UPS 17

UPS on Control menu 17

Security on Control menu 18

Network on Control menu 18

Configuring your Settings: 1 19

Power Settings on Configuration menu 19

UPS General screens 20

Self-Test Schedule screen 20

Shutdown on Configuration menu 21
Start of Shutdown 21
Duration of Shutdown 21
PowerChute Shutdown Parameters 22

Shutdown Scheduling 24
For the UPS 24

PowerChute Network Shutdown clients 24

Security menu. 25
Session Management screen 25
Ping Response 25
Local Users 25
Remote Users authentication 26
RADIUS screen. 27
Configuring the RADIUS Server 27
Firewall screens 29
802.1X Security Configuration 31

Configuring your Settings: 2 32

Network on Configuration menu 32
TCP/IP settings for IPv4 screen 32
TCP/IP settings for IPv6 screen 33
DHCP response options 34
Port Speed screen 35
DNS screen. 35
Testing DNS screen 36
Web access screen. 36
Web SSL Certificate screen 37
Console screen 37
SNMP screens 38
Modbus screens 41
BACnet screen 42
FTP Server screen 44
Wi-Fi screen 44

Notification menu 46
Types of notification 46
Configuring event actions 47
E-mail notification screens 48
SNMP Trap Receivers screen 50
SNMP Traps test screen. 51

General menu. 52
Identification screen 52
Date/ Time screen. 52
Creating and Importing settings with the config file 53
Configure Links screen 53

Logs on Configuration menu 54
Identifying Syslog servers 54
Syslog settings 54
Syslog test and format example 55

Tests menu 56
Testing and calibrating 56
Setting the NMC LED lights to blink 56
Logs menus..... 57
Using the Event and Data Logs 57
Event log 57
Data log 58
How to use SCP or FTP to retrieve log files 59
UPS Log 61
Firewall Log. 61
About menu..... 66
About the Network Management Card 66
About the UPS device 66
About the NMC and the firmware modules 66
Support screen 67
Device IP Configuration Wizard 68
Capabilities, Requirements, and Installation. 68
System requirements. 68
Installation 68
How to Export Configuration Settings 69
Retrieving and Exporting the .ini File 69
Summary of the procedure 69
Contents of the .ini file 69
Detailed procedures. 69
The Upload Event and Error Messages 71
The event and its error messages 71
Messages in config.ini 71
Errors generated by overridden values 71
Related Topics 72

File Transfers 73
Upgrading Firmware 73
Firmware File Transfer Methods 73
Using the NMC Firmware Upgrade Utility 73
Use FTP or SCP to upgrade one Network Management Card 74
Use XMODEM to upgrade one NMC 75
Use a USB drive to transfer and upgrade the files 75
Upgrading the firmware on multiple Network Management Cards 76
Verifying Upgrades 77
Verify the success of the transfer 77
Last Transfer Result codes 77
Verify the version numbers of installed firmware 77
Changing UI Language 77
Troubleshooting 78
Network Management Card Access Problems 78
SNMP Issues 79
Modbus Problems 79
APC USB Wi-Fi Device (AP9834) Problems 80
LED Descriptions 80
Two-Year Factory Warranty 82
Terms of warranty 82
Non-transferable warranty 82
Exclusions 82
Warranty claims 83
Copyright Notices 83

Introduction

Product Description

Features

The Schneider Electric Network Management Cards for Easy UPS, 1-Phase & 3-Phase (AP9544 and AP9547) mentioned below are Web-based, IPv6 Ready products. Devices with the Network Management Card (NMC) installed can be managed using multiple open standards such as:

Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)	Secure SHell (SSH)
Secure Copy (SCP)	Secure Boot with Root of Trust for enhanced security
RADIUS	Extensible Authentication Protocol (EAP) over LAN (EAPoL)
Building Automation and Control Networks Protocol (BACnet)	Simple Network Management Protocol versions 1, 2c and 3
Syslog	Telnet
Modbus	Hypertext Transfer Protocol (HTTP)
File Transfer Protocol (FTP)	

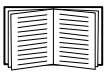
The **AP9544** and **AP9547** Network Management Cards:

- Provide one USB-A host port.
- Provide data and event logs.
- Enable you to set up notifications through event logging, e-mail, Syslog and SNMP traps.
- Provide support for PowerChute® Network Shutdown. **NOTE:** The AP9547 card in 3-Phase Easy UPS devices only support the shut down of the connected servers and applications running on the servers. It is not supported to shut down the UPS device(s).
- Support using a Dynamic Host Configuration Protocol (DHCP) or BOOTstrap
- Protocol (BOOTP) server to provide the network (TCP/IP) values of the NMC.
- Provide 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.
- Provide a selection of security protocols for authentication and encryption.
- Communicate with Data Center Expert, Data Center Operation, or EcoStruxure™ IT.
- Support Modbus TCP/IP.

Supported Devices

The Network Management Card for Easy UPS is compatible with:

- 1-Phase Easy UPS devices (AP9544 only).
- 3-Phase Easy UPS devices (AP9547 only).



Please refer to Knowledge Base article **FA237786** on the **APC website** for a list of UPS devices the Network Management Cards are compatible with.

IPv4 initial setup

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

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

NOTE: If a default gateway is unavailable, use the IP address of a computer that is located on the same subnet as the NMC and that is usually running. The NMC uses the default gateway to test the network when traffic is very light.

NOTE: The Network Management Card has a MAC address prefix of 00:C0:B7 or 28:29:86. To check the MAC address of your NMC, go to **"About > Network"** You can use this MAC address prefix to configure your DHCP service.

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

To configure the TCP/IP settings, see the **Network Management Card for Easy UPS Installation Guide** on the APC website and in printed form.

For detailed information on how to use a DHCP server to configure the TCP/IP settings at an NMC, see “DHCP response options”.

IPv6 initial setup

IPv6 network configuration provides flexibility to accommodate your requirements. IPv6 can be used anywhere an IP address is entered on this interface. You can configure manually, automatically, or using DHCPv6, see the “TCP/IP settings for IPv6 screen”.

Network management with Other Applications

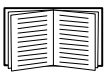
These applications, utilities and resources work with a UPS that connects to the network through an NMC.

- PowerChute Network Shutdown — Provide unattended remote graceful shutdown of computers that are connected to UPS devices.
- APC PowerNet® MIB — Discover how to access UPS devices via SNMP.
- Data Center Expert — Provide enterprise-level power management and management of SNMP agents such as networked UPS devices and environmental sensors.
- EcoStruxure IT — Cloud-based monitoring software with which you can monitor your UPS devices via SNMP and Modbus.
- Device IP Configuration Utility — Configure the basic settings of one or more NMCs over the network, see “Device IP Configuration Wizard”.
- Security Wizard — Assists in creating or importing Transport Layer Security (TLS) server certificates and Secure SHell (SSH) host keys, which help to protect the integrity and confidentiality of communication with the NMC.

Internal Management Features

Overview

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



For more information about the UIs, see “Web User Interface” and the **Network Management Card for Easy UPS CLI Guide** on the APC website. See “SNMP screens” for information about how SNMP access to the NMC is controlled.

Access priority for logging on

You can enable more than one user to log on at the same time, where each user has equal access. See “Session Management screen”.

Types of user accounts

The NMC has various levels of access — Super User, Administrator, Device User, Read-Only User and Network-only User:

- A **Super User** can use all of the menus in the UI and all of the commands in the command line interface. The Super User can also define additional user accounts, and set variables for the additional users. The default user name and password are both `apc` at first log in. You will be prompted to enter a new password after you log in.
  NOTE: The Super User cannot be renamed or deleted, but it can be disabled. It is recommended that the Super User account is disabled once any additional Administrator accounts are created. Make sure that there is at least one Administrator account enabled before the Super User account is disabled.

  An **Administrator** can use all of the menus in the UI and all of the commands in the command line interface. The default user name is `apc`, and a password must be set before the user account can be enabled.
- A **Device User** has read and write access to device-related screens. Administrative functions like session management under the Security menu and Firewall under Logs are greyed out.

  The default user name is `device`, and a password must be set before the user account can be enabled.
- A **Read-Only User** has the access to the same menus as a Device User above, but without the capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled. (The Event and Data Logs display no button for this user to clear the log).

  The default user name is `readonly`, and a password must be set before the user account can be enabled.
- A **Network-only User** can only log on using the Web user interface (UI) and CLI (Telnet/SSH, not serial). There is no default name and password.

The Administrator, Device User, Read-Only User, and Network-only User accounts are disabled by default, and cannot be enabled until the Super User default password (`apc`) is changed.

To set **User Name** and **Password** values for Administrator, Device User and Read-Only account types, see “Local Users”.

How to Reset after a Lost Password

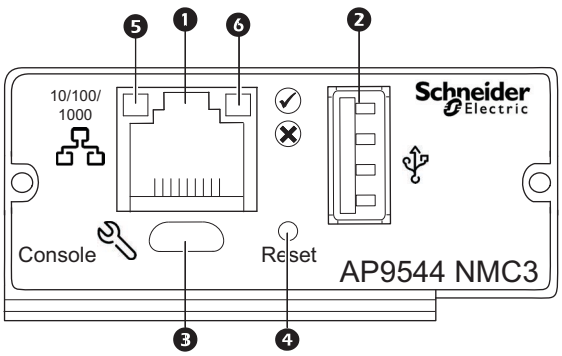
NOTE: Resetting your NMC will reset the card to its default configuration.

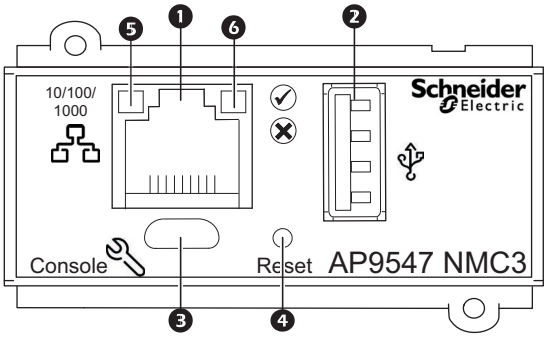
If you forget your password, you must use the **Reset** button on the NMC to wipe all configuration, including the password. Hold down the **Reset** button for 20-25 seconds, ensuring the Status LED is pulsing green during this time. When the Status LED changes to amber or orange, release the **Reset** button to allow the NMC to complete its reboot process.

After the NMC reboots, you must re-configure your NMC. For more information, see the **Network Management Card for Easy UPS Installation Guide** or Knowledge Base article **FA156064** on the APC website.

It is recommended you export the .ini file after configuring your NMC to prevent loss of data in the event of a lost password. See “Retrieving and Exporting the .ini File”.

Front Panel (AP9544/AP9547)





	Item	Description
1	10/100/1000 Base-T connector	Connects the NMC to the Ethernet network.
2	USB port	Support for UPS firmware updates and the optional APC USB Wi-Fi Device (AP9834). See “Update the UPS firmware from a USB drive” and "Wi-Fi screen".
3	USB console port	Connects the NMC to a local computer, via a micro-USB cable (APC part number 960-0603), to configure initial network settings or access the command line interface (CLI).
4	Reset button	Restarts the network management interface. **NOTE:** This does not affect the output power of the device in which the NMC is installed.
5	Link-RX/TX (10/100/1000) LED	See “Link-RX/TX (10/100/1000) LED”.
6	Status LED	An LED (light-emitting diode) is a light source. See “Status LED”.

LED Descriptions

Status LED

This LED (light-emitting diode) indicates the status of the NMC.

Condition	Description
Off	One of the following situations exists: • The NMC is not receiving input power. • The NMC is not operating properly. It may need to be repaired or replaced. Contact Customer Support. See “APC by Schneider Electric Worldwide Customer Support”.
Solid green	The NMC has valid TCP/IP settings.
Solid orange	One of the following situations exists: • A hardware malfunction has been detected in the NMC. Contact Customer Support. See “APC by Schneider Electric Worldwide Customer Support”. • The NMC is in Bootmonitor mode. See "About the NMC and the firmware modules" for more information.
Flashing green	The NMC does not have valid TCP/IP settings.[1]
Flashing orange	The NMC is making BOOTP requests.[1]
Alternately flashing green and orange	If the LED is flashing slowly, the NMC is making DHCP[2] requests.[1] If the LED is flashing rapidly, the NMC is starting up.

1. If you do not use a BOOTP or DHCP server, see the **Network Management Card for Easy UPS Installation Guide** to configure the TCP/IP settings of the NMC.
2. To use a DHCP server, see “DHCP response options”.

NOTE: If the micro-USB cable is connected while the NMC is booting up, the NMC will wait 90 seconds to allow time to access the Boot Monitor. See "Use XMODEM to upgrade one NMC". No LEDs are active during this delay period. It is recommended to disconnect the micro-USB cable if local access to the CLI is not required.

Link-RX/TX (10/100/1000) LED

This LED indicates the network status of the NMC.

Condition	Description
Off	One or more of the following situations exist: • The NMC is not receiving input power. • The cable that connects the NMC to the network is disconnected or not functioning properly. • The device that connects the NMC to the network is turned off or not operating correctly. • The NMC itself is not operating properly. It may need to be repaired or replaced. Contact Customer Support. See “APC by Schneider Electric Worldwide Customer Support”.
Solid yellow	The NMC is connected to a network operating at 10-100 Megabits per second (Mbps).
Solid green	The NMC is connected to a network operating at 1000 Mbps.

Condition	Description
Flashing yellow	The NMC is receiving or transmitting data packets at 10-100 Mbps.
Flashing green	The NMC is receiving or transmitting data packets at 1000 Mbps.

Watchdog Features

Overview

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

Network interface watchdog mechanism

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

Resetting the network timer

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

Automatic Logout

By default, users will be automatically logged out of the NMC Web and CLI interfaces after 3 minutes of inactivity. The default logout time for each user can be adjusted through the web interface:

Configuration > Security > Local Users > Management.

- Click the hyperlink of the user name for the account you want to change.
- Under Session timeout, modify the number of minutes.

Automatic Logout	Duration (min)
Default	3
Minimum	1
Maximum	60 (1hr)

Web User Interface

Introduction

Overview

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

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

Supported Web browsers

The NMC Web UI is compatible with:

- Windows® operating systems:
  - The latest release of Microsoft® Edge®

NOTE: The UPS Firmware Update screen is not compatible with the Edge® browser. See “PowerChute Network Shutdown clients” on page 24.

- All operating systems:
  - The latest releases of Mozilla® Firefox® or Google® Chrome®

Other commonly available browsers might work but have not been fully tested.

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

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

How to Log On

Overview

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

- `apc` for Administrator or Super User
- `device` for a Device User
- `readonly` for a Read-Only User

See also “Types of user accounts”.

You can set your UI language as you log on by choosing a language from the **Language** drop-down box. See “Changing UI Language”.

When HTTPS is enabled, the NMC generates its own certificate. This certificate negotiates encryption methods with your browser. Refer to the **Security Handbook** on the APC website for more details.

URL address formats

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

NOTE: HTTP is disabled by default and HTTPS is enabled by default.

Common browser error messages at log-on.

Error Message	Browser	Cause of the Error
"This page cannot be displayed."	Internet Explorer	Web access is disabled, or the URL was not correct.
"Unable to connect."	Firefox, Chrome	

URL format examples. See also "TCP/IP settings for IPv6 screen".

Example and Access Mode	URL Format
DNS name of `Web1`	
HTTP	`http://Web1`
HTTPS	`https://Web1`
System IP address of `139.225.6.133` and a default Web server port (80)	
HTTP	`http://139.225.6.133`
HTTPS	`https://139.225.6.133`
System IP address of `139.225.6.133` and a non-default Web server port (5000)	
HTTP	`http://139.225.6.133:5000`
HTTPS	`http://139.225.6.133:5000`
System IPv6 address of `2001:db8:1::2c0:b7ff:fe00:1100` and a non-default Web server port (5000)	
HTTP	`http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000`

First log in

When you log in to the NMC for the first time, you will be prompted to change the default Super User account password (`apc`). After you log in, you will be directed to the Configuration Summary Overview screen. This screen is an overview of all system protocols, and their current values (e.g. enabled/disabled). You can access this screen at any time afterwards by following the path: **Configuration > Network > Summary**.

Home Screen

Overview

Path: Home

On the **Home** screen of the interface, you can view active alarms and the most recent events recorded in the Event Log.

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

Symbol	Description
	**No Alarms**: No alarms are present, and the UPS and NMC are operating normally.
	**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.

At the upper right corner of every screen, the same icons report the UPS status. If any **Critical** or **Warning** alarms exist, the number of active alarms also displays.

To view the entire Event Log, click **More Events**.

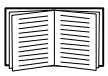
Icons and Links

To make any screen the “home” screen (i.e., the screen that displays first when you log on), go to that screen, and click the  icon at the top right.

Click  to revert to displaying the Home screen when you log on.

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

- Link 1: the **Knowledge Base** page of **www.apc.com** with useful troubleshooting information
- Link 2: the **Product Information** page of **www.apc.com** with background information on your hardware
- Link 3: the **downloads** page of **www.apc.com** with available firmware and software.

 To reconfigure the links, see “Configure Links screen”.

Monitoring the UPS: Status menu

The options below are not available for all UPS devices.

The Status menu options report on the current state of your UPS and network.

You can configure your UPS and network using the Configuration menu options, see “Configuring your Settings: 1” and “Configuring your Settings: 2”.

See the following sections:

- “UPS on Status menu”
- “Overview on Status menu”
- “Measurements on Status menu”
- “Network on Status menu”
- “Maintenance on Status menu”

UPS on Status menu

Path: Status > UPS

The options below are only relevant for supported 1-Phase Easy UPS devices with an AP9544 card installed.

This shows you the UPS load, battery charge, voltage, and other useful information.

Field	Description
UPS Input Measurements	
Voltage	The AC voltage (VAC) being received by the UPS.
Frequency	The frequency, in Hertz, of the input voltage.
Maximum Voltage	The highest input voltage to the UPS during the previous minute of operation.
Minimum Voltage	The lowest input voltage to the UPS during the previous minute of operation.
UPS Output Measurements	
Voltage	The AC voltage (VAC) that the UPS is supplying to its load.
Current	The current, in Amps, applied to the load.
Percentage Active Power	The active power in percentage.
Frequency	The actual value of the frequency of the output voltage, in Hertz.
Percentage Apparent Power	The apparent power in percentage.
UPS Battery Measurements	
Battery Voltage	The DC voltage of the batteries.

Field	Description
Battery Remaining Capacity	The percentage of the UPS battery capacity that is available to support the connected load.
Last Battery Replacement	The latest date a battery was replaced in MM/DD/YY format.
Nominal Battery Voltage	The rated voltage capacity of the UPS batteries; the DC voltage that the batteries are rated to supply when the UPS uses its battery for output power.
Internal Temperature	The temperature inside the UPS.
Runtime Remaining	The length of time, in hours and minutes, that the UPS can support its load while running on battery power.
Battery Current	The current being output from the battery
Battery Capacity	The percentage of the UPS battery capacity that is available to support the attached equipment.
Bypass Frequency Range	
Lower Limit	The bypass frequency range lower limit, in Hertz (Hz).
Upper Limit	The bypass frequency range upper limit, in Hertz (Hz).
Eco Voltage Range	
Lower Limit	The Eco voltage range lower limit.
Upper Limit	The Eco voltage range upper limit.
UPS Battery Pack Status	
Battery Pack N	The status of the UPS device's battery pack. For example, **Installed**, **Not Installed**.
Battery ID	The battery pack's ID.

Overview on Status menu

Path: Status > Overview

The options below are only relevant for supported 3-Phase Easy UPS devices with an AP9547 card installed.

This provides the an overview of the UPS device, including active alarms, battery capacity and other useful information.

Field	Description
Quick Status	
Load	A graph of the load of the attached equipment that the UPS is supporting as a percentage of nominal power.
Battery Capacity	A graph showing the percentage of the total capacity of the UPS battery available to support the attached equipment.
Input Voltage	The AC voltage being received by phase to phase of the UPS.
Output Voltage	The AC voltage that the UPS is providing to the load.

Field	Description
Runtime Remaining	The length of time, in hours and minutes, that the UPS can support its load while running on battery power.
Last Battery Transfer	The reason for the last transfer to battery power at the UPS.
Ambient Temperature	The temperature inside the UPS.
Recent Device Events	
A list of UPS events that recently occurred in reverse chronological order. To view the entire event log, click **More Events**.	

Measurements on Status menu

The options below are only relevant for supported 3-Phase Easy UPS devices with an AP9547 card installed.

Path: Status > Measurements > Input

Field	Description
Frequency	The frequency, in Hertz, of the input voltage.
Voltage	The AC voltage, in Volts, being received by each phase of the UPS.
Current	The current, in Amps, supplied by the input voltage for each phase.

Path: Status > Measurements > Bypass

Field	Description
Frequency	The frequency, in Hertz, of the bypass input voltage.
Voltage	The AC voltage, in Volts, measured between phase to phase of the bypass input. Phase to neutral voltage is not measured.

Path: Status > Measurements > Output

Field	Description
Total Active Power	The load placed on the output of the UPS by the attached equipment, in kW.
Total Apparent Power	The load placed on the output of the UPS by the attached equipment, in kVA.
Total Output Percent Load	The power rate (load) of the attached equipment that the UPS is supporting as a percentage of nominal power.
Frequency	Actual value of the frequency of the output voltage, in Hertz.
Nominal Output Apparent Power	This is the maximum value (in kVA) available for the UPS. If the load is greater than this value, an overload alarm is generated.
Voltage	The AC voltage, in Volts, that each phase of the UPS is supplying to its load.
Current	The current, in Amps, applied to the load by each phase.
Active Power	The load placed on each phase of the UPS by the attached equipment, in kW.
Apparent Power	The load placed on each phase of the UPS by the attached equipment, in kVA.

Path: Status > Measurements > Battery

Field	Description
Runtime Remaining	The length of time, in hours and minutes, that the UPS can support its load while running on battery power.
Battery Remaining Capacity	The present battery charge, as a percentage of full charge capacity.
Battery Running Time	The length of time that the UPS has been running on battery instead of Main AC.
Battery Voltage (+/-)	Actual value of measured battery DC voltage.
Battery Current (+/-)	Actual value of measured battery current.
Battery Temperature	Actual value of battery temperature.
Last Battery Test Result	Result of the automatic battery test.
Last Battery Transfer	The reason for the last transfer to battery power at the UPS.

Path: Status > Measurements > Other Parameters

Field	Description
ECO Mode	Indicates whether ECO mode is enabled or disabled. When the UPS is set to work in Economy mode, when the mains is within tolerance, the UPS works as "Offline", directly on mains (on bypass) and comes back "Online" (on inverter) when mains is no longer within the tolerance.
UPS Type	Indicates how the UPS is configured: Single, 1+1 Redundant, Parallel, or 3:3 Parallel.
Main AC	Indicates whether the main AC is used as the source for the power converter.
UPS Static Bypass Switch State	This switch is internal to the UPS and allows the switchgear to put the UPS into bypass. When the static bypass switch is closed, the source is providing power to the load and the switchgear can put the UPS into bypass. When the static bypass switch is open, the UPS is providing power to the load.

Network on Status menu

Path: Status > Network

The Network screen gives you your IP, domain name, and ethernet port settings. See “Network on Configuration menu”for background details on the fields.

Maintenance on Status menu

Path: Status > Maintenance

The options below are only relevant for supported 3-Phase Easy UPS devices with an AP9547 card installed.

This provides the an overview of the UPS device, including active alarms, battery capacity and other useful information.

Field	Description
Maintenance Cycle	
DC Capacitor	The maintenance cycle of the DC Capacitor.
AC Capacitor	The maintenance cycle of the AC Capacitor.
Auxiliary Power Supply	The maintenance cycle of the auxiliary power supply.
Air Filter	The maintenance cycle of the air filter.
Battery	The maintenance cycle of the battery.
Warranty Cycle	
Warranty	The UPS warranty cycle.
Running Time	
AC Capacitor	The running time of the AC Capacitor since it was last changed.
DC Capacitor	The running time of the DC Capacitor since it was last changed.

Controlling the UPS

The options below are not available for all UPS devices.

The Control menu options enable you to take immediate actions affecting your UPS, and they also have some security and network functions. See the following sections:

- “UPS on Control menu”
- “Security on Control menu”
- “Network on Control menu”

UPS on Control menu

Path: Control > UPS

The options below are only relevant for supported 1-Phase Easy UPS devices with an AP9544 card installed.

When you choose a radio button option and click Next, another screen summarizes the action to take place; click Apply there to continue with the action.

Action	Description
Reboot UPS	Restarts the attached equipment by turning the UPS off and back on. The following parameters control the reboot: • Shutdown Delay • Minimum Battery Capacity • Return Delay
Turn UPS Off	Turns off the output power of the UPS immediately, without a shutdown delay. The UPS remains off until you turn it on again.
Put UPS To Sleep	Puts the UPS into sleep mode by turning off its output power for a period of time defined by the following parameters:. Click Next to see specific details on timing and delays. • The UPS waits the time configured as “Shutdown Delay” before turning off its power. • When input power returns, the UPS turns on output power after two configured periods of time: “Sleep Time” and “Return Delay”.
Put UPS in Bypass/ Return UPS from Bypass	These options control the use of bypass mode, which allows maintenance to be performed at the UPS without turning off power at the UPS.
Signal PowerChute® Server Shutdown	Select this option to notify all servers configured as “PowerChute Network Shutdown clients" that are in communication with this UPS to shut down according to the values configured for “PowerChute Shutdown Parameters". This option will not notify servers when performing any Bypass control actions.

Security on Control menu

Path: Control > Security > Session Management

The screens gives details about users who are logged on, the interface they are using (e.g. the Web user interface, the CLI), their IP address, and how long they have been logged on.

If you have sufficient rights, click on the name to see what means of authentication were used to validate the user. You can then also use the **Terminate Session** button to log off a user.

Network on Control menu

Path: Control > Network > Reset/Reboot

Use these options to reset various Network Management Card options and the UI.

Action	Description
Reboot Management Interface	Restarts the management interface (e.g. the Web user interface, the CLI) by logging you off. The UPS and NMC devices are not rebooted.
Reset All[1]	Caution:This resets all configurable values to their defaults. • If you do not select **Exclude TCP/IP**, all configured values and settings are reset to their default values, including the setting that determines how this device must obtain its TCP/IP configuration values and the EAPoL configuration. The default for TCP/IP configuration settings is DHCP and that for EAPoL access is disabled. • If you select **Exclude TCP/IP**, all configured values and settings except the setting that determines how this device must obtain its TCP/IP and the EAPoL configuration values are reset to their default values.
Reset Only[1]	**TCP/IP**: Resets only the setting that determines how this device must obtain its TCP/IP configuration values including the EAPoL configuration which is reset to disabled. The default for TCP/IP configuration setting is DHCP and that for EAPoL access is disabled.
	Event Configuration: Resets events to their default configuration. Any specifically configured event or group will also revert to the default value. See “Notification menu”
[1]Resetting may take up to a minute. The UPS name you configured will not be reset (see “UPS General screens”).	

Configuring your Settings: 1

The options below are not available for all UPS devices.

With the Configuration menu options, you can set fundamental operational values for your UPS and NMC.

See the sections below and also “Configuring your Settings: 2”.

- “Power Settings on Configuration menu”
- “UPS General screens”
- “Self-Test Schedule screen”
- “Shutdown on Configuration menu”
- “Shutdown Scheduling”
- “PowerChute Network Shutdown clients”
- “Security menu”

NOTE: You can view some of your configuration settings via the Configuration Summary screen (**Configuration > Network > Summary**).

Power Settings on Configuration menu

Path: Configuration > Power Settings

The options below are only relevant for supported 1-Phase Easy UPS devices with an AP9544 card installed.

The **Rated Output Voltage** is the AC voltage the UPS supplies to the load, while the UPS is on battery. You can configure the following types of device-specific items:

- **High** and **Low Transfer Voltage**: The high and low transfer voltage, in VAC.
- **Output Frequency**: The output frequency, in Hertz (Hz).

UPS General screens

Path: Configuration > UPS

Field	Description
UPS Name	A name to identify the UPS.
Last Battery Replacement	Enter the month and year of the most recent UPS battery replacement.
Number of External Batteries	The number of batteries, excluding built-in batteries, that the UPS has. Some devices that have more than 16 batteries must add batteries in quantities of 16 (e.g., 16, 32, 48, etc.), but can then be adjusted to the correct value.

Path: Configuration > UPS > Power

The options below are only relevant for supported 3-Phase Easy UPS devices with an AP9547 card installed.

Alarm thresholds are based on available runtime and redundant power and on UPS load. You can configure the **Alarm if Load Over** threshold which triggers an alarm if the load exceeds from the configured value, in kVA,

Self-Test Schedule screen

Path: UPS > Configuration > Self-Test Schedule

The options below are only relevant for supported 1-Phase Easy UPS devices with an AP9544 card installed.

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

Shutdown on Configuration menu

Path: Configuration > Shutdown

Use this screen to configure the parameters of a UPS shutdown. See the table below and also “Controlled Early Shutdown and End of Shutdown”.

Start of Shutdown

Define the delays and durations that are considered when a UPS shutdown is required.

Field	Description
Low Battery Duration	For a UPS on battery, this defines a runtime remaining threshold, below which a low battery condition is triggered on the UPS. For example, if the Low Battery Duration is set to ten minutes and the UPS predicted runtime remaining reaches ten minutes or below, a low battery condition is triggered. If input power is not restored to the UPS, it will turn off when the battery has exhausted. A low battery condition will trigger a shutdown on all PowerChute Network Shutdown clients associated with the NMC.
Maximum Required Delay	Calculates the delay needed to ensure that each PowerChute client has enough time to shut down gracefully when the UPS or the PowerChute client initiates a graceful shutdown. • It is the longest shutdown delay needed by any server listed as a PowerChute Network Shutdown client. • It is calculated whenever the management interface of the UPS turns on or is reset, or when the *Force Negotiation* option is selected and you click Apply. See “Shutdown delays and PowerChute Network Shutdown”.

Duration of Shutdown

Specify the length of time for which the UPS is powered off.

Field	Description
Sleep Time	Defines how long the UPS keeps its output power turned off when you issue a UPS Sleep command. When the UPS turns off, it will turn back on following the Sleep Time defined here, plus the Return Time. If utility power has not been restored at this point, the UPS will wait until it is restored to turn back on. The Sleep command can be issued via the UPS display, the “UPS on Control menu”, via SNMP command or via PowerChute Business Edition.

PowerChute Shutdown Parameters

Path: Configuration > PowerChute > PowerChute® Configuration

This is the navigation path for 3-Phase Easy UPS devices.

These options are not available for all UPS devices.

Specify the shutdown parameters used by PowerChute Network Shutdown.

Field	Description
Maximum Required Delay - Force Negotiation	Enabling *Force Negotiation* resets the Maximum Required Delay value to match the Low Battery Duration. An updated status packet is sent by the NMC to all of the registered PowerChute agents. PowerChute then compares the Low Battery Duration sent in that packet to its total required shutdown time and increases the Maximum Required Delay accordingly, or the Power Off Delay for the Outlet Group with which it is registered. PowerChute does a runtime remaining verification check every 30 seconds, which compares the PowerChute total shutdown time required to the NMC Low Battery Duration. Selecting Force Negotiation will reset the Power Off Delay for all Outlet Groups to the same value as Low Battery Duration. Force Negotiation can take up to ten minutes to calculate the value required by all of the PowerChute clients registered on the NMC. For more information see “Shutdown delays and PowerChute Network Shutdown” on page 20.
Maximum Negotiated Delay	Maximum Negotiated Delay is the longest shutdown delay needed by any server listed as a PowerChute Network Shutdown client to shutdown safely when the UPS initiates a graceful shutdown. This delay is calculated whenever the management interface of the UPS turns on or is reset.
On-Battery Shutdown Behavior	Define the behavior of the UPS following a shutdown: • Restart when power is restored - When utility power is restored, restart the UPS. • Turn off and stay off - The UPS remains off, even if the utility power is restored.
User Name	Enter the user name to be used for PowerChute.
Authentication Phrase	This phrase is used for authentication between PowerChute and the NMC. The phrase is empty by default, and must be set before you can enable PowerChute.
PCNS Communication Protocols	Select the communication protocol to communicate with PowerChute: HTTPS or HTTP.

Controlled Early Shutdown and End of Shutdown.

These options are not available for all UPS devices.

The Controlled Early Shutdown options enable you to shut down a UPS device on battery when ANY of the conditions that you specify are met:

- When the time on battery exceeds a set number of minutes.
- When the runtime remaining of the UPS is less than a set number of minutes. (Runtime is how long the UPS can use battery power to support its present load).
- When the battery charge is less than a set percentage of its total capacity.
- When the load on the UPS output is less than a set percentage.

With **Stay off after power returns**, you can also decide whether the UPS turns back on, or not, after AC utility power is restored.

The **End of Shutdown** options enable you to set a condition and a delay time for when a UPS can turn back on after AC utility power is restored. Depending on the UPS model, you can specify a **Minimum Battery Capacity** or **"Min Return Runtime"**, before the UPS will turn back on.

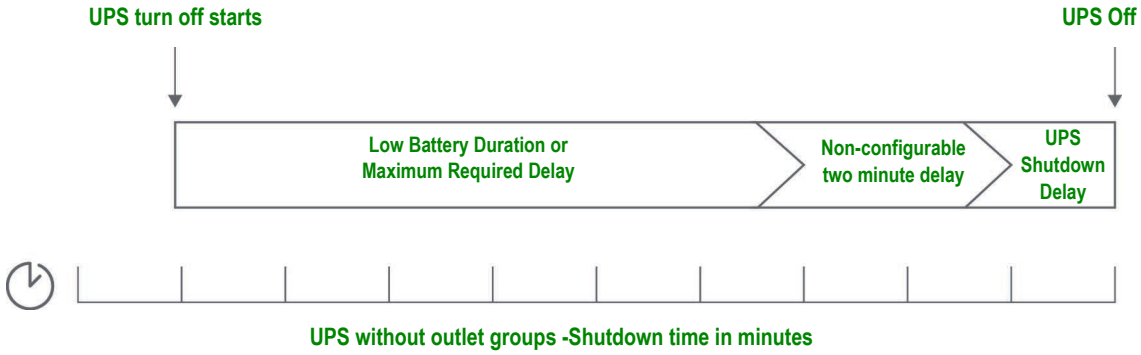
Shutdown delays and PowerChute Network Shutdown.

The following section describes how the Low Battery Duration, Maximum Required Delay and Outlet Group Power Off Delays impact the PowerChute shutdown sequence.

For more information on PowerChute shutdown sequences, see the **User Guide** on the APC website.

For both types of UPS, with and without Outlet Groups, the shutdown time is negotiated by the NMC interacting with PowerChute Network Shutdown, as follows:

UPS without Outlet Groups. For a UPS with NO outlet groups, the UPS shutdown time is the greater of the **Maximum Required Delay** or **Low Battery Duration** values on the NMC **Shutdown** screen, plus a non-configurable 2 minute delay, plus the shutdown delay for the UPS.



Note: If a shutdown has been triggered by a Low Battery condition, the Low Battery Duration value takes precedence over Maximum Required Delay.

Notes:

For more information on PowerChute shutdown sequences, see "*Sample Shutdown Scenarios*" in the PowerChute Network Shutdown **User Guide** on the APC website.

During the comparison of the PowerChute Required Shutdown time and the NMC Maximum Required Delay/Outlet Group Power Off Delay, the largest value is used. For example, if the PowerChute client command line shutdown duration is set to 8 minutes, but the UPS Low Battery Duration is 10 minutes, the NMC will use the larger value of 10 minutes for the Maximum Required Delay.

In Forced Negotiation, the NMC polls the PowerChute Clients to get their required shutdown time. As a result it can take up to ten minutes for the Maximum Required Delay/Outlet Group Power Off delay values to update.

PowerChute never changes the NMC **Low Battery Duration** field value.

With PowerChute Network Shutdown v3.x or higher, the **Maximum Required Delay** value is never used by the NMC for a UPS with outlet groups.

Shutdown Scheduling

Path: Configuration > Scheduling

The options below are only relevant for supported 1-Phase Easy UPS devices with an AP9544 card installed.

NOTE: Do not create shutdown schedules that overlap. An example of an overlapping shutdown schedule is a Weekly Shutdown set from 8pm to 9pm, and a One-time Shutdown set from 8.10pm to 8.30pm. Overlapping shutdown schedules result in unknown and untested behavior.

For the UPS

You can schedule a shutdown for a UPS device under **UPS**.

Any configured shutdown schedules display along the top of the screen when you select **UPS**, with relevant details, including whether they are currently enabled or disabled.

Edit, Enable, Disable, or Delete a Scheduled Shutdown. Click the schedule name in the list of schedules along the top of either the **UPS** screen. This displays the complete details where you can edit the parameters. This includes disabling it temporarily by clearing the **Enable** check box, or deleting it permanently.

Creating a UPS shutdown schedule.

1. Under **Scheduling**, select **UPS.**
2. Use the radio buttons to select the type of shutdown to schedule, **One-time Shutdown**, **Daily Shutdown**, or **Weekly Shutdown**, and click the **Next** button.
3. To disable a schedule temporarily, clear the **Enable** check box.
4. Specify a name, and a schedule date and time.
   For a weekly shutdown, specify the frequency using the drop-down box.
5. Specify whether the device should turn back on after the shutdown:

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

Signal PowerChute Network Shutdown Clients: Specify whether to notify PowerChute clients, see “PowerChute Network Shutdown clients”.

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

PowerChute Network Shutdown clients

Path: UPS > Configuration > PowerChute

The navigation path for 3-Phase Easy UPS devices is **Configuration > PowerChute > PowerChute®**

PowerChute Network Shutdown can shut down your UPS devices remotely.

When you install a PowerChute Network Shutdown client on your network, it is added to this list automatically. When you uninstall a PowerChute Network Shutdown client, it is removed automatically.

Click **Add Client** to enter the IP address of a new PowerChute Network Shutdown client. To delete a client, click the IP address of that client in the list, and then click **Delete Client**. The list can contain the IP addresses of up to 50 clients.

With outlet groups, you also have to specify which outlet group is supplying power to the PowerChute client.

NOTE: PowerChute cannot connect to the NMC if HTTP is disabled on the NMC. See “Web access screen” to enable HTTP or HTTPS.

Security menu

Session Management screen

Path: Configuration > Security > Session Management

Enabling **Allow Concurrent Logins** means that two or more users can log on at the same time. Each user has equal access and each interface (HTTP, FTP, telnet console, serial console (CLI), etc.) counts as a logged-in user. **Allow Concurrent Logins** allows a maximum of eight users logged into the web interface, five users logged into the CLI and one user logged into the serial console at the same time.

Remote Authentication Override: The NMC supports Radius storage of passwords on a server. However, if you enable this override, the NMC will allow a local user to log on using the password for the NMC that is stored locally on the NMC. See also “Local Users” and “Remote Users authentication”.

Ping Response

Path: Configuration > Security > Ping Response

Enable the **IPv4 Ping Response** check box to allow the Network Management Card 3 to respond to network pings. This does not apply to IPv6.

Local Users

Use these menu options to view, and to set up access and individual preferences (like displayed date format), to the NMC user interfaces. This applies to users as defined by their logon name.

Path: Configuration > Security > Local Users > Management

Setting user access. With this option an administrator or super user can list and configure the users allowed access to the UI. Click on the name link to view details, and to edit or delete a user.

Click on **Add User** to add a user. On the resulting **User Configuration** screen, you can add a user and withhold access by clearing the **Access** check box. The maximum length for both the name and password is 64 bytes, with less for multi-byte characters. You have to enter a password.

Values greater than 64 bytes in Name and Password might get truncated.
To change an administrator/ super user setting, you must enter all three password fields.

Create a password using a combination of lower and uppercase characters, numbers and special characters. Passwords can be no longer than 64 ASCII characters.

Use **Session Timeout** to configure the time that this UI waits before logging off this user (three minutes by default). If you change this value, you must log off for the change to take effect.

Serial Remote Authentication Override: By selecting this, you can bypass RADIUS by using the serial console (CLI) connection. This screen enables it for the selected user, but it must also be enabled globally to work, through “Session Management screen”.

See also “Configuration > Security > Local Users > Default Settings” below. For background information on accounts see “Types of user accounts”.

User Preferences. 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.
Blue	**Informational**: An alarm to provide information. The Network Management Card and all connected devices are operating normally.

Export Log Format: Exported log files can be formatted using CSV (comma-separate values), or tabs. See “To display the Event Log”.

Select the temperature scale for measurements in this UI. **US Customary** corresponds to Fahrenheit and **Metric** corresponds to Celsius.

You can specify the default language for the UI with the **Language** field. This can be set when you log on also.

You can also specify different languages for e-mail recipients and SNMP trap receivers. See “E-mail recipients” and “Trap Receivers”.

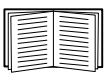
Path: Configuration > Security > Local Users > Default Settings

Setting up defaults can make adding users quicker. Use this option to set defaults for the many options on the Management screen, see “Configuration > Security > Local Users > Management” above.

Remote Users authentication

Path: Configuration > Security > Remote Users > authentication

Authentication. Specify how you want users to be authenticated at logon.



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

The following authentication and authorization functions of RADIUS (Remote Authentication Dial-In User Service) are supported:

- When a user accesses the NMC 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 are limited to 32 characters with the NMC.

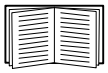
Select one of the following:

- **Local Authentication Only**: RADIUS is disabled. See “Local Users”.
- **RADIUS, then Local Authentication**: Both are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server does not respond, local authentication is used.
- **RADIUS Only**: There is no local authentication.

If **RADIUS Only** is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, remote access is unavailable to all users. To regain access, you must use a serial connection to the command line interface and change the **access** setting to **local** or **radiusLocal**.

For example, the command to change the access setting to **local** would be:

```
radius -a local
```



See also “RADIUS screen” below and “Configuring the RADIUS Server”.

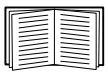
RADIUS screen

Path: Configuration > Security > Remote Users > RADIUS

You can use a RADIUS server to authenticate remote users.Use this option to do the following:

- List the RADIUS servers (a maximum of two) available to the NMC and the time-out period for each.
- Configure the authentication parameters for a new or existing RADIUS server by clicking on a **Radius Server** link.

RADIUS Setting	Description
RADIUS Server	The server name or IP address (IPv4 or IPv6). **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. The NMC supports ports 1812, 5000 to 32768.
Secret	The shared secret between the RADIUS server and the NMC.
Reply Timeout	The time in seconds that the NMC waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password in order to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path.

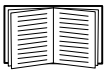


See also “Remote Users authentication” above and “Configuring the RADIUS Server” below.

Configuring the RADIUS Server

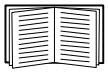
Summary of the configuration procedure.

You must configure your RADIUS server to work with the NMC, see the steps below.



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** on the APC website.

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



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

1. VSAs can be used instead of the Service-Type attributes provided by the RADIUS server.
   VSAs require a dictionary entry and a RADIUS user's 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 not work. VSAs take precedence over standard RADIUS attributes.

Configuring a RADIUS server on UNIX® with shadow passwords.

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

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

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

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

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

Supported RADIUS servers.

FreeRADIUS v1.x and v2.x, and Microsoft Server 2008 and 2012 Network policy Server (NPS) are supported. Other commonly available RADIUS applications may work, but may not have been fully tested.

Firewall screens

Path: Configuration > Security > Firewall > Configuration

Enable or disable the firewall functionality. The configured policy is listed by default. Select the **Enable** check box to enable the firewall. The check box is un-checked by default.

- Click **Apply** to confirm a firewall policy you have selected to enable. The **Firewall Confirmation** page will open.
  - The Confirmation page contains a recommendation to test the firewall before enabling. It is not mandatory.
  - The first hyperlink goes to the Firewall Policy page.
  - The second hyperlink goes to the Firewall Test page.
  - Click on **Apply** to enable the firewall and return to the Configuration page.
  - Click on **Cancel** to return to the Configuration page without enabling the Firewall.
- Click **Cancel**: No new selection will be enabled. You stay on the Configuration page.

Path: Configuration > Security > Firewall > Active Policy

Select an active policy from the Available Policies drop-down list, and view the validity of that policy. The current active policy is displayed by default; you can select another from the list.

- Click **Apply** to enable your changes. If a different firewall was selected and enabled, the change is effective immediately. If a newly configured firewall policy has been selected, it is recommended that you test the new firewall before enabling it. (See Configuration above.)
- Click **Cancel** to restore the original active policy and stay on the Active Policy page.

Path: Configuration > Security > Firewall > Active Rules

When a firewall is enabled, this read-only page lists the individual rules that are being enforced by a current active policy. See the **Create/Edit Policy** section for descriptions of the fields (Priority, Destination, Source, Protocol, Action, and Log).

Path: Configuration > Security > Firewall > Create/Edit Policy

Create a new policy; delete or edit an existing policy:

NOTE: While deleting an active enabled firewall policy cannot be done, editing a running policy can be done but is not recommended as changes are applied immediately. Instead, disable the firewall, edit the policy, test it, and then re-enable the policy.

Create a new policy: Click **Add Policy**, and type in the file name for the new firewall file. The filename should have a .fwl file extension. If left without a file extension, .fwl will be appended to the name automatically.

- Click **Apply**: If the filename is legal, the empty file firewall policy file will be created. It will be located in the /fwl folder with the other policies on the system.
- Click **Cancel** to return to the previous page without creating a new firewall file.

Edit an existing policy:

Select **Edit Policy** to go to the edit page. You can edit an firewall policy which is not active.

Warning page: If you attempt to edit the active enabled policy, a warning page will open: **“Editing the active firewall policy will cause all changes made to be applied immediately. It is recommended to disable the firewall and test the policy before enabling it.”**

- Click **Apply** to leave the Warning page and return to the Edit Policy page.
- Click **Cancel** to leave the Warning page and return to the Create/Edit Policy page.

1. Select the policy you want to edit from the **Policy Name** drop-down list, and click **Edit Policy**.
2. Click **Add Rule** or select the **Priority** of an existing rule to go to the **Edit Rule** page. From this page, you can change the rule settings or delete the selected rule.

Setting	Description
Priority	If 2 rules conflict, the rule with the higher priority will determine what happens. The highest priority is 1; the lowest is 250.
Type	**host**: In the IP/any field, you will enter a single IP address. **subnet**: In the IP/any field, you will enter a subnet address. **range**: In the IP/any field, you will enter a range of IP addresses.
IP/any	Specify the IP address or range of addresses this rule applies to, or select one of the following: • **any**: The rule applies regardless of the IP address. • **anyipv4**:The rule applies for any IPv4 address. • **anyipv6**:The rule applies for any IPv6 address.
Port	Specify a port the rule will apply to. • **None**: The rule will apply to any port. • **Common Configured ports**: Select a standard port. • **Other**: Specify a non-standard port number.
Protocol	Specify which protocol the rule applies to. • **any**: any protocol. • **tcp**: used for reliable information transfer between applications. • **udp**: alternative to TCP using for faster, lower bandwidth information transfer. Though it has fewer delays, UDP is less reliable than TCP. • **icmp**: used to report errors for troubleshooting. • **icmpv6**: used to report errors for troubleshooting on applications using IPv6.
Action	**allow**: Allow the packet that matches this rule. **discard**: Discard the packet that matches this rule.
Log	If this rule applied to a packet, regardless of whether the packet is blocked or allowed, this will add an entry to the Firewall Log. See “Firewall Log”.

It is recommended that you add one of the following as the lowest priority rule in your firewall policy:

- To use the firewall as an allowlist, add
  `250 Dest any / Source any / protocol any / discard`
- To use the firewall as a blocklist, add
  `250 Dest any / Source any / protocol any / allow`

Delete a policy:

Select **Delete Policy** to open the Confirm Deletion page.

Click **Apply** to confirm, and the selected firewall file is removed from the file system.

Path: Configuration > Security > Firewall > Load Policy

Upload a policy (with the .fwl suffix) from a source external to this device.

Path: Configuration > Security > Firewall > Test

Temporarily enforce the rules of a chosen policy for a time that you specify.

802.1X Security Configuration

Path: Configuration > Security > 802.1X Security

The NMC takes the role of a supplicant in an EAPoL (Extensible Authentication Protocol over LAN) architecture used in IEEE 802.1X port-based network access control. The NMC supports EAP-TLS as an authentication method which requires you to upload 3 client-side certificates. The private key is stored in an encrypted format. You need to provide a valid passphrase to be able to enable 802.1X security access.

NOTE: The NMC supports only EAP-TLS authentication method.

The Web UI offers the following options for EAPoL configuration:

Setting	Description
EAPoL Access	Used to enable or disable 802.1X security access. **NOTE:** 802.1X security access is disabled by default. You can only enable access when valid certificates and a valid passphrase for the private key are provided.
Supplicant Identifier	Allows you to set your own supplicant identifier (up to 32 characters including whitespace). **NOTE:** By default, the supplicant identifier is set to “NMC-Supplicant-xx:xx:xx:xx:xx:xx” where six octets of “xx” are the MAC ID of the NMC.
CA Certificate	Upload/replace or remove a CA root certificate. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extension .pem, .PEM, .der, or .DER.
Private Key Certificate	Upload/replace or remove an encrypted private key. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extensions .key or .KEY. **NOTE:** Unencrypted private keys are not accepted.
Private Key Passphrase	Provide the passphrase to decrypt the encrypted private key. Allows up to 64 characters including whitespace.
User/Public Certificate	Upload/replace or remove a user/public certificate. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extensions .pem, .PEM, .der, or .DER.

Configuring your Settings: 2

With the Configuration menu options, you can set fundamental operational values for your UPS and NMC.

See the sections below and also “Configuring your Settings: 1”.

- “Network on Configuration menu”
- “Notification menu”
- “General menu”
- “Logs on Configuration menu”

NOTE: You can view some of your configuration settings via the Configuration Summary screen (**Configuration > Network > Summary**).

Network on Configuration menu

TCP/IP settings for IPv4 screen

Path: Configuration > Network > TCP/IP > IPv4 Settings

This option displays any current IPv4 address, subnet mask, default gateway, MAC address, and boot mode of the Network Management Card (NMC). Use the lower part of the screen to configure those settings, including disabling IPv4.

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

Option	Description
Manual	Specify your IPv4 address, subnet mask, default gateway here.
BOOTP*	At 32-second intervals, the device requests network assignment from any BOOTP server: • If it receives a valid response, it starts the network services. • If previously configured network settings exist, and it receives no valid response to five requests (the original and four retries), by default it uses those previously configured settings. This ensure that it remains accessible if a BOOTP server is no longer available. • If it finds a BOOTP server, but the request to that server does not work or times out, the device stops requesting network settings until it is restarted.
DHCP*	At 32-second intervals, the device requests network assignment from any DHCP server: • If a DHCP server is found, but the request to that server does not work or times out, it stops requesting network settings until it is restarted. • Optionally, you can set up the device with **Require vendor specific cookie to accept DHCP Address** in order to accept the lease and start the network services. See “DHCP response options”.

*Vendor Class: APC
Client ID: The MAC address of the device. If you change this value, the new value must be unique on the LAN.
User Class: The name of the application firmware module, see “File Transfers”.

TCP/IP settings for IPv6 screen

Path: Configuration > Network > TCP/IP > IPv6 Settings

This option displays any current IPv6 settings of the Network Management Card (NMC). Use the lower part of the screen to configure those settings, including disabling IPv6.

You have a choice of using manual or automated IP addressing. It is possible to use them both concurrently. For **Manual**, select the check box and then enter the **System IP** v6 address and the **Default Gateway**.

Select the **Auto Configuration** check box to enable the system to obtain addressing prefixes from the router (if available). It will use those prefixes to automatically configure IPv6 addresses.

IPv6 Possible Formats	Description
fe80:0000:0000:0000:0204:61ff:fe9d:f156	full form of IPv6
fe80:0:0:0:204:61ff:fe9d:f156	drop leading zeroes
fe80::204:61ff:fe9d:f156	collapse multiple zeroes to :: in the IPv6 address
fe80:0000:0000:0000:0204:61ff:254.157.241.86	IPv4 dotted quad at the end
fe80:0:0:0:0204:61ff:254.157.241.86	drop leading zeroes, IPv4 dotted quad at the end
fe80::204:61ff:254.157.241.86	dotted quad at the end, multiple zeroes collapsed
::1	localhost
fe80::	link-local prefix
2001::	global unicast prefix

For **DHCPv6 Mode**, see the table below.

DHCPv6 Mode for IPv6 Configuration	
Option	**Description**
Router Controlled	When this radio box is selected, DHCPv6 is controlled by the **M** (Managed Address Configuration Flag) and **O** (Other Stateful Configuration Flag) flags received in IPv6 Router Advertisements. When a router advertisement is received, the NMC checks whether the M and O flags are set. The NMC interprets them as follows: • **Neither is set**: Indicates that the local network has no DHCPv6 infrastructure. The NMC uses Router Advertisements and manual configuration to get non-link-local addresses 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, even if subsequent Router Advertisement packets are received in which the M flag is not set. If an O flag is received first, then an M flag is received subsequently, the NMC performs full address configuration upon receipt of the M flag. • **Only O is set**: In this situation, the NMC sends a DHCPv6 Info-Request packet. DHCPv6 is used to configure “other” settings (such as location of DNS servers), but NOT to provide addresses. This is known as “DHCPv6 stateless”.

DHCPv6 Mode for IPv6 Configuration	
Option	**Description**
Address and Other Information	DHCPv6 is used to obtain addresses AND other configuration settings. This is known as “DHCPv6 stateful”.
Non-Address Information Only	DHCPv6 is used to configure “other” settings (such as location of DNS servers), but NOT to provide addresses. This is known as “DHCPv6 stateless”.
Never	DHCPv6 is NOT used for any configuration settings.

DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings that the NMC needs in order to operate on a network. Each response also has other information that affects the operation of the NMC. See also Knowledge Base article **FA156110**.

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

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

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

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

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

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

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

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

- **Network Time Protocol Servers** (option 42): Up to two NTP servers (primary and secondary) that the NMC can use.
- **Time Offset** (option 2): The offset of the NMC's subnet, in seconds, from Coordinated Universal Time (UTC).
- **Domain Name Server** (option 6): Up to two Domain Name System (DNS) servers (primary and secondary) that the NMC can use.
- **Host Name** (option 12): The host name that the NMC will use (32-character maximum length).

- **Domain Name** (option 15): The domain name that the NMC will use (64-character maximum length).
- **Boot File Name** (from the **file** field of the DHCP response, described in **RFC2131**): The fully qualified directory-path to a user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the NMC will download the .ini file. After the download, the NMC uses the .ini file as a boot file to reconfigure its settings.
- **Fully Qualified Domain Name** (FQDN, option 81): The fully qualified domain name of the NMC.

Port Speed screen

Path: Configuration > Network > Port Speed

The Port Speed setting defines the communication speed of the Ethernet network port. Your current setting is displayed in **Current Speed**.

You can change the setting by choosing a radio button under **Port Speed**:

- For **Auto-negotiation** (the default), network devices negotiate to transmit at the highest possible speed, but if the supported speeds of two devices are not matched, 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).

NOTE: You can only change the Port Speed to 1000 Mbps by choosing the **Auto-negotiation** radio button.

DNS screen

Path: Configuration > Network > DNS > Configuration

The values under **Domain Name System Status** list your current status and setup.

Use the options under **Manual Domain Name System Settings** to configure he Domain Name System (DNS):

- Enabling the **Override Manual DNS Settings** means that configuration data from other sources like DHCP take precedence over the manual configurations here.
- Specify the **Primary DNS Server** and, optionally, the **Secondary DNS Server** with IPv4 or IPv6 addresses. For the NMC to send e-mail, you must at least define the IP address of the primary DNS server.
  - The NMC waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server. If the NMC does not receive a response within that time, e-mail cannot be sent. Use DNS servers on the same segment as the NMC or on a nearby segment, but not across a wide-area network (WAN).
  - After you define the IP addresses of the DNS servers, test it, see “Testing DNS screen”.
- **System Name Synchronization**: Enabling this synchronizes the DNS hostname with the NMC System Name. Click on the System Name link to define it.

  If the DNS hostname and the NMC System Name are synchronized, the System Name is limited to a certain number of characters, based on DNS RFC. If they are not synchronized, the system name is limited to 255 characters.

- **Host Name**: After you configure a host name here and a domain name in the **Domain Name** field, users can enter a host name in any field in the NMC interface (except e-mail addresses) that accepts a domain name.

- **Domain Name (IPv4/IPv6)**: For the NMC interface, you only need to configure the domain name here. In all other fields in this UI — except e-mail addresses — that accept domain names, the NMC defaults to adding this domain name when only a host name is entered.
  - To override the expansion of a specified host name by the addition of a domain name, set this domain name field to its default, `somedomain.com` or to `0.0.0.0`.
  - To override the expansion of a *specific* host name entry (for example, when defining a trap receiver), include a trailing period. The NMC recognizes a host name with a trailing period (such as `mySnmpServer.`) as if it were a fully-qualified domain name and does not append the domain name.
- **Domain Name (IPv6)**: Specify the IPv6 domain name here.

Testing DNS screen

Path: Configuration > Network > DNS > Test

Use this option to send a DNS query that tests the setup of your DNS servers by looking up the IP address. See “DNS screen” above on how to set up your servers.

View the result of a test in the **Last Query Response** field.

- At **Query Type**, select the method to use for the DNS query, see table below.
- At **Query Question**, specify the value to be used for the selected query type as explained in the table.

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

Web access screen

Path: Configuration > Network > Web > Access

Use this option to configure the access method for the Web interface. (In order to activate any changes here, you must reboot the NMC. See “Network on Control menu” on page 18).

You can enable access to this UI through either **HTTP** or **HTTPS** or through both, by using the Enable check boxes. HTTP is disabled by default, and HTTPS is enabled by default. HTTPS encrypts user names, passwords, and data during transmission; HTTP does not.

HTTPS also authenticates the NMC by digital certificate. See “Creating and Installing Digital Certificates” in the **Security Handbook** on the APC website to see how to use digital certificates.

For the **ports**, you can change the setting to any unused port for additional security; the range is 5000–32768. You 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(s)://152.214.12.114:5000
```

Web SSL Certificate screen

Path: Configuration > Network > Web > SSL Certificate

Add, replace, or remove a security certificate. SSL (Secure Socket Layer) is a protocol used to encrypt data between your browser and the web server.

The **Status** can be:

- **Valid certificate**: A valid certificate was installed or was generated by the NMC. Click on this link to view the contents of the certificate.
- **Certificate 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 NMC.
- **Generating**: The NMC is generating a certificate because no valid certificate was found.
- **Loading**: A certificate is being activated on the NMC.

If you install an invalid certificate, or if no certificate is loaded while SSL is enabled, the NMC generates a default certificate, a process which delays access to the interface for up to one minute. You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on.

Add or Replace Certificate File: Browse to the certificate file created with the Security Wizard. See “Creating and Installing Digital Certificates” in the **Security Handbook** on the APC website to see how to use digital certificates created by the Security Wizard or generated by the NMC.

Remove: Delete the certificate. See screen text also.

Console screen

Path: Configuration > Network > Console > Access

Path: Configuration > Network > Console > SSH Host Key

Console access. You need to enable console access in order to update your UPS firmware. Console access enables use of the command line interface (CLI).

You can enable access to the CLI through either **Telnet** or **SSH** or through both, by using the Enable check boxes. Telnet is disabled by default, and SSH is enabled by default. Telnet does not encrypt user names, passwords, and data during transmission whereas SSH does.

NOTE: If you enable SSH, SCP (SeCure CoPy) is also enabled, for secure file transfer. See “File Transfers” for more information on the use of SCP.

For the **ports** to be used to communicate with the NMC, you can change the setting to any unused port from 5000 to 32768 for additional security.

- **Telnet Port**: This is 23 by default. You must then use a colon (:) or a space to specify the non-default port, as required by your Telnet client program.

  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` *or* `telnet 152.214.12.114 5000`

- **SSH Port**: This is 22 by default. See the documentation for your SSH client for the command line format required to specify a non-default port. See also “SSH Host Key” below.

SSH Host Key. If you’re using SSH (Secure Shell Protocol) for console (CLI) access, you can add, replace, or remove the host key on the SSL Host Key screen.

Status indicates whether the host key (private key) is valid. The Status can be:

- **SSH Disabled:** No host key in use.
- **Generating**: The NMC is creating a host key because no valid host key was found.
- **Loading**: A host key is being activated on the NMC.
- **Valid**: One of the following valid host keys is in the **/ssh** directory (the required location on the Network Management Card):
  - 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 Host Key: Upload a host key file created by the Security Wizard. To use the Security Wizard, see the **Security Handbook** on the APC website. To use an externally created host key, load the host key before you enable SSH (with “Console access” above).

NOTE: To reduce the time required to enable SSH, create and upload a host key in advance. *If you enable SSH with no host key loaded, the NMC takes up to one minute to create a host key, and the SSH server is not accessible during that time.*

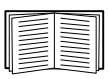
Remove: Delete the host key. See screen text also.

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 (except Windows 10). Clients for Windows are available from various vendors, such as PuTTY which is available from **www.putty.org**.

SNMP screens

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 **Data Center Expert** to manage a UPS on the public network of a system, you *must* have SNMPv1 or SNMPv3 enabled in the NMC interface. Read access will allow the device to receive traps from the NMC, but Write access is required while you use the NMC user interface to set the device as a trap receiver.



For detailed information on enhancing and managing the security of your system, see the **Security Handbook** on the APC website.

SNMPv1.

Path: Configuration > Network > SNMPv1 > Access and **Access control**

Use **Access** to enable or disable SNMP version 1 as a method of communication with the NMC.

SNMPv1 is disabled by default. The **Community Name** must be set before SNMPv1 communications can be established.

Use of SNMPv2c is supported by the SNMPv1 options.

Access Control. You can configure up to four access control entries to specify which Network Management Systems (NMSs) have access to the NMC. To edit, click a community name.

By default one entry is assigned to each of the four available SNMPv1 communities. You can edit these settings to apply *more than one entry to any one community* to grant access by several specific IPv4 and IPv6 addresses, host names, or IP address masks.

- By default, a community has access to the NMC from any location on the network.
- If you configure multiple access control entries for any one community name, it means that one or more of the other communities have no access to the device.

Community Name: The name that a Network Management Station (NMS) must use to access the community. The maximum length is 16 ASCII characters.

NMS IP/Host Name: The IPv4 or IPv6 address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (for example, 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 UI or command line interface.
- **Write+**: GETS and SETS at any time.
- **Disable**: No GETS or SETS at any time.

SNMPv3.

Path: Configuration > Network > SNMPv3 > Access, User Profiles, and Access Control

For 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, to browse the MIB, and to receive traps.

SNMPv3 is disabled by default. A valid user profile must be enabled with passphrases (**Authentication Passphrase**, **Privacy Passphrase**) set before SNMPv3 communications can be estiablished

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

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

Enable SNMPv3 access under access enables this 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**, with 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 that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be.
  It also verifies that the message has not been changed during transmission, and that the message was communicated in a timely manner. This indicates 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 that ensures the privacy of the data that an NMS is sending to or receiving from this device through SNMPv3, by using encryption.
- **Authentication Protocol:** The implementation of SNMPv3 supports SHA and MD5 authentication. One of these must be selected.
- **Privacy Protocol:** The implementation of SNMPv3 supports AES and DES as the protocols for encrypting and decrypting data. You must use both a privacy protocol and a privacy password, otherwise the SNMP request is not encrypted.

  In turn, you cannot select the privacy protocol if no authentication protocol is selected.

Access Control. You can configure up to four access control entries to specify which Network Management Systems (NMSs) have access to the NMC. To edit, click a user name.

By default one entry is assigned to each of the four user profiles. You can edit these settings to apply *more than one entry to any one user profile* to grant access by several specific IP addresses, host names, or IP address masks.

- By default, all NMSs that use that profile have access to this device.
- If you configure multiple access control entries for one user profile, it means that one or more of the other user profiles must have no access to this device.

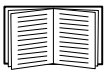
User Name: From the drop-down list, select the user profile to which this access control entry will apply. The choices available are the four user names that you configure through the “User Profiles” option.

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 (for example, 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows:

- 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment.
- 149.225.**255.255**: Access only by an NMS on the 149.225 segment.
- 149.**255.255.255**: Access only by an NMS on the 149 segment.
- 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

Modbus screens

Use the Modbus options to configure your NMC to use the Modbus protocol, to connect to a Building Management System (BMS).



For more information on the Modbus implementation on your UPS, see the **Modbus Documentation Addendum** and *Modbus Register Maps* available on the **APC website**.

NOTE: The NMC supports 5 simultaneous Modbus TCP connections.

Modbus TCP.

Path: Configuration > Network > Modbus > TCP

1. Use **Access** to enable or disable Modbus TCP as a method of communication with the NMC.
2. Set the **Port** number for the TCP connection. It can be set to 502 (default) or to a value between 5000 and 32768.
3. Click Apply to save your changes.

BACnet screen

BACnet is not supported on the AP9544 card.

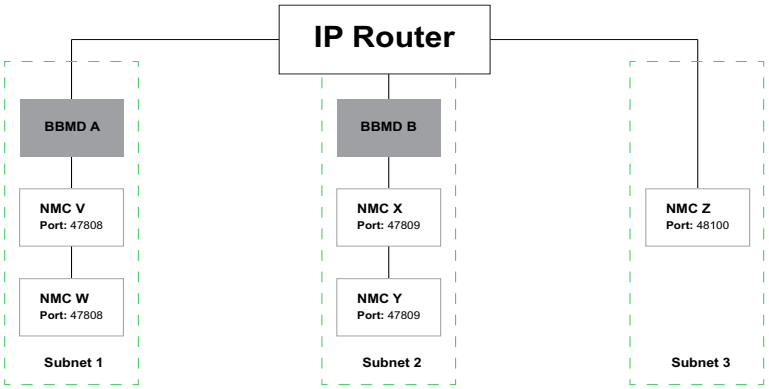
Use the BACnet options to configure your NMC to use the BACnet protocol, and to make UPS data available to building automation and control networks.

For more information on the UPS data points made available via BACnet, see the BACnet Application Maps available on the **APC website**.

BACnet Configuration

Option	Description
Access	Select the check box to enable BACnet. If this is not enabled, the NMC cannot be accessed via BACnet. BACnet is disabled by default. **NOTE:** BACnet cannot be enabled until the **Device Communication Control Password** is set.
Device ID	A unique identifier for this BACnet device, used for addressing the device. Acceptable range: 0–4194303.
Device Name	A name for this BACnet device, which must be unique on the BACnet network. The default device name is “BACn”+ the last eight digits of the NMC MAC address. The minimum length is 1, the maximum length is 150 characters, and special characters are permitted.
Network Protocol	Select the protocol to be used: • BACnet/IP
APDU Timeout	The number of milliseconds the NMC will wait for a response to a BACnet request. Acceptable range: 1000-30000. The default value is 6000.
APDU Retries	The number of BACnet requests attempts that the NMC will make before aborting the request. Acceptable range: 1–10. The default value is 3.
Device Communication Control Password	The Device Communication Control service is used by a BACnet client to instruct a remote device (e.g. a BACnet-enabled NMC) to stop initiating, or stop responding to all APDUs (except the Device Communication Control service) for a specified duration of time. This service can be used for diagnostic purposes. Specify the Device Communication Control password to ensure that a BACnet client cannot control the BACnet communication of an NMC without first providing the password set here. The password is required to be between 8 and 20 characters, and must contain: • A number. • An uppercase character. • A lowercase character. • A special character. It is recommended to update the password when you first enable BACnet. You do not need to know the current password to update the password.

BACnet/IP

Option	Description
Local Port	The UDP/IP port the NMC uses to send and receive BACnet/IP messages. Acceptable range: 5000–65535. Default: 47808. **NOTE:** The address of a BACnet/IP-enabled NMC is defined as the IP address of the NMC and the local port.
Enable foreign device registration	Select the check box to register the NMC with a BACnet broadcast management device (BBMD). **NOTE:** You need to register your NMC as a foreign device with a BBMD if there is no BBMD currently on the subnet of the NMC, or if the NMC uses a different local port to the BBMD.  In the above example: • BBMD A manages the broadcast messages to NMCs V and W. • BBMD B manages the broadcast messages to NMCs X and Y. • Only NMC Z needs to register with a BBMD A or B as a foreign device, as there is no BBMD present on its subnet. • Once registered, NMC Z can receive broadcast messages from the BBMD with which it is registered, and can send messages to the BBMD, which broadcasts them to all devices on its subnet, and to the other BBMDs on the network via the IP router.
Status	The status of the foreign device registration (FDR): • **Foreign device registration inactive** FDR will be inactive if: – FDR is enabled and BACnet is disabled – FDR is disabled and BACnet is enabled – FDR is disabled and BACnet is disabled • **Registration successful** FDR has completed successfully. • **Registration rejected** FDR has not completed successfully. The NMC will retry registration automatically, but you can also toggle the **Enable foreign device registration** check box to prompt the NMC to retry registration. • **Registration sent** The FDR request has been sent, but it has not yet completed.

Option	Description
BACnet/IP Broadcast Management Device	The IP address or fully qualified domain name (FQDN) of the BACnet broadcast management device with which this NMC card will be registered.
Port	The port of the BBMD with which this NMC card will be registered.
TTL	The number of seconds (Time To Live) that the BBMD will maintain the NMC as a registered device. If the NMC does not re-register before this time expires, the BBMD will delete it from its foreign-device table, and the NMC will no longer be able to send and receive broadcast messages via the BBMD. The TTL controls how frequently the NMC registers with the BBMD, as the NMC will attempt to re-register before this time expires.

FTP Server screen

Path: Configuration > Network > FTP Server

Use this screen to enable access to an FTP server and to specify a port.

Option	Description
Access	FTP transmits files without encrypting them. By default, FTP is disabled. For encrypted file transfer, use Secure CoPy (SCP). SCP (via SSH) is enabled by default. However, it will not allow a file transfer until the Super User default password (`apc`) is changed. **NOTE**: At any time that you want a device to be accessible for management by Data Center Expert or Operation, FTP Server must be enabled in the Network Management Card interface of that UPS. For detailed information on enhancing and managing the security of your system, see the **Security Handbook** on the APC website.
Port	The TCP/IP port of the FTP server (21 by default). The FTP server uses both the specified port and the port one number lower. The allowed non-default port numbers are indicated on the screen: 21, and 5001–32768. **NOTE**: Configuring the FTP server to use a non-default port enhances security by requiring users to append the port name to the IP address in an FTP command line. The appended port name must be preceded by a space or colon depending on the FTP client used.

Wi-Fi screen

Path: Configuration > Network > Wi-Fi

NOTE: This screen is relevant when the optional APC USB Wi-Fi Device (AP9834) is inserted in a USB port of an AP9544/AP9547 card.

IMPORTANT: It is recommended that you do not download a config.ini file from a wired device and upload the entire file to a Wi-Fi-enabled device. It is also not recommended to download a config.ini file from a Wi-Fi-enabled device and push the entire file to a wired device unless the entire `[NetworkWiFi]` section is removed or commented out using semicolons (for example `;WiFi=enabled`).
The `[NetworkWiFi]` section contains device settings specific to Wi-Fi use. These settings should not be uploaded to a wired device.

Use this screen to view the current status of the Wi-Fi network, enable/disable Wi-Fi, and configure the Wi-Fi network's settings.

NOTE: Enabling/disabling Wi-Fi will disable/enable the wired LAN connection. The NMC will reboot when the Wi-Fi settings are configured. After the reboot, the wired network will be disabled and the NMC will attempt to connect to the given **Network Name (SSID)**.

Network Name (SSID): Specify the network name (SSID) of the Wi-Fi network. The maximum length is 32 characters.

Security Type: Specify the security type of the Wi-Fi network and provide the authentication details:

Option	Description
WPA	**Wi-Fi Password:** Specify a password for the Wi-Fi network. The maximum length is 64 characters.
WPA2-AES	
WPA2-Mixed	
WPA2-TKIP	
WPA2-Enterprise	• **User Name:** The user name for WPA2-Enterprise authentication. The maximum length is 32 characters. • **Password:** The password for WPA2-Enterprise authentication. The maximum length is 32 characters. • **Outer Identity:** Specify the WPA-2-Enterprise outer identity. This is an optional unencrypted identification used by the WPA-2-Enterprise server. For example: user@example.com or anonymous. The maximum length is 32 characters.

For information on how to upgrade the APC USB Wi-Fi Device's (AP9834) firmware, see the `wifi` command in the **Network Management Card for Easy UPS CLI Guide**.

To troubleshoot the connection to the APC USB Wi-Fi Device (AP9834), and the Device's LED descriptions, see "APC USB Wi-Fi Device (AP9834) Problems".

Notification menu

See these sections:

- “Types of notification”
- “Configuring event actions”
- “E-mail notification screens”
- “SNMP Traps test screen”
- “SNMP Trap Receivers screen”

Types of notification

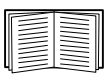
You can configure notification actions to occur in response to an event. You can notify users of an event in any of several ways:

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

  - Queries (SNMP GETs)

    For more information, see “SNMP Trap Receivers screen” and “SNMP Traps test screen”. 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.

The NMC supports the use of the **RFC1628 MIB** (Management Information Base). See “SNMP Trap Receivers screen” for information on how you can set up a trap receiver. The **1628 MIB** group of three events only work with that MIB, not the alternative Powernet MIB. They can be configured like any event (see “Configuring event actions” below).

Configuring event actions

Configuring by event.

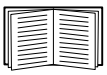
Path: Configuration > Notification > Event Actions > By Event

By default, logging an event is selected for all events. To define event actions for an individual event:

1. Select the **Configuration** menu, then **Notification**, **Event Actions**, and **By Event**.
2. To find an event, click on a column heading to see the lists under the **Power Events**, **Environment Events**, or **System Events** categories.

   Or you can click on a sub-category under these headings like **Input Line Status** or **Temperature**.
3. Click on the event name to view or change the current configuration, such as recipients to be notified by e-mail, or Network Management Systems (NMSs) to be notified by SNMP traps. See “Notification parameters”. Click on the **Event Log** check box to enable or disable an event log entry for this event.

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



When viewing details of an event’s configuration, you can 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”
- “E-mail recipients”
- “Trap Receivers”

Configuring by groups of events.

Path: Configuration > Notification > Event Actions > By Group

To configure a group of events simultaneously:

1. Select the **Configuration** menu, then **Notification**, **Event Actions**, and **By Group**.
2. Choose how to group events for configuration:
   - Choose **Grouped by severity**, and then select 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 screen to screen 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 screen. (See “Logs on Configuration menu”).
   b. Select whether to leave the newly configured event action enabled for this group of events or to disable the action.

   See “Notification parameters” directly below.

Notification parameters. These configuration fields define the parameters for sending notifications of events. See “Configuring by event” and “Configuring by groups of events”.

They are usually accessed by clicking the receiver or recipient name.

Field	Description
Notification Delay	If the event persists for the specified time, the notification is sent. If the condition clears before the time expires, no notification is sent.
Repeat Interval	The notification is sent repeatedly at the specified interval (the default is every 2 minutes until the condition clears).
Number of Notifications After Initial	During an active event, the notification repeats for this number of times.
or	
Notify Until Condition Is Cleared	The notification is sent repeatedly until the condition clears or is resolved.

For events that have an associated clearing event, you can also set these parameters. (An example of an event with its clearing event is `UPS: Lost communication with the battery packs` and `UPS: Restored communication with the battery packs`).

E-mail notification screens

Overview of setup. Use 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 screen”)
- The IP address or DNS name for the **SMTP Server** and **From Address**. (See “SMTP Server” below)
- The e-mail addresses for a maximum of four recipients. (See “E-mail recipients”)

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

SMTP Server.

Path: Configuration > Notification > E-mail > Server

This screen lists your primary and secondary DNS server (see “DNS screen”) and then these fields:

Field	Description
Outgoing Mail Configuration	
From Address	The contents of the **From** field in e-mail messages sent by the NMC: • 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.
SMTP Server	The IPv4/ IPv6 address or DNS name of the local SMTP server. **NOTE:** This definition is required only when **SMTP Server** is set to **Local**. See “E-mail recipients”
Authentication	Enable this if the SMTP server requires authentication.
Port	The SMTP default port is 25. Alternative ports: 465, 587, 2525, 5000 to 32768.

Field	Description
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.
Advanced	
Use SSL/TLS	• **Never**: The SMTP server does not require nor support encryption. • **If Supported**: The SMTP server advertises support for STARTTLS but *doesn't* require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given. • **Always**: The SMTP server requires the STARTTLS command to be sent on connection to it. • **Implicitly**: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.
Require CA Root Certificate	This should only be enabled if the security policy of your organization does not allow for implicit trust of SSL connections. If this is enabled, a valid root CA certificate must be loaded onto the NMC for encrypted e-mails to be sent.
File Name	This field is dependent on the root CA certificates installed on the NMC and whether or not a root CA certificate is required.

E-mail recipients.

Path: Configuration > Notification > E-mail > Recipients

Specify up to four e-mail recipients. Click on a name to configure the settings. See also “SMTP Server” above.

Field	Description
E-mail Generation	Enables (default) or disables sending e-mail to the recipient.
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.
Format	The long format contains name, location, contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.
Language	Chose a language from the drop-down list and any mails will be sent in that language. It is possible to use different languages for different users. See “Changing UI Language”.

Field	Description
Server	Select one of the following methods for routing e-mail: • **Local**: Through the site-local SMTP server. This recommended setting ensures that the e-mail is sent using the site-local SMTP server. Choosing this setting limits delays and network outages and retries sending e-mail for many hours. When choosing the Local setting you must also enable forwarding at the SMTP server of your device and set up a special external e-mail account to receive the forwarded e-mail. Check with your SMTP server administrator before making these changes. • **Recipient**: Through the recipient's SMTP server. The NMC performs an MX record look-up on the recipients e-mail address and uses that as its SMTP server. The e-mail is only sent once so it could easily be lost. • **Custom**: This setting enables each e-mail recipient to have its own server settings. These settings are independent of the settings given under “SMTP Server” above.

E-mail SSL Certificates.

Path: Configuration > Notification > E-mail > SSL Certificates

Load a mail SSL certificate on the NMC for greater security. The file must have an extension of `.crt` or `.cer`. Up to five files can be loaded at any given time.

When installed, the certificate details also display here. An invalid certificate will display “n/a” for all fields except File Name.

Certificates can be deleted from this screen. Any e-mail recipients using the certificate should be manually modified to remove reference to this certificate.

E-mail test.

Path: Configuration > Notification > E-mail > Test

Send a test message to a configured recipient.

SNMP Trap Receivers screen

Trap Receivers.

Path: Configuration > Notification > SNMP Traps > Trap Receivers

With Simple Network Management Protocol (SNMP) traps, you can get automatically notified of significant UPS events. They are a useful tool for monitoring devices on your network.

The trap receivers are displayed by **NMS IP/Host Name**, where NMS stands for Network Management System. You can configure up to six trap receivers.

To configure a new trap receiver, click **Add Trap Receiver**. To edit (or delete) one, click its IP address/ host name.

If you delete a trap receiver, all notification settings configured under “Configuring event actions” for the deleted trap receiver are set to their default values.

Select either the **SNMPv1** or **SNMPv3** radio button to specify the trap type. For an NMS to receive *both* types of traps, you must separately configure two trap receivers for that NMS, one for each trap type.

Field	Description
Trap Generation	Enable (the default) or disable trap generation for this trap receiver.

Field	Description
Powernet MIB Trap Generation/ RFC1628	Choose between these two MIB trap generation types for each trap created. The Powernet option is customized for Schneider Electric and contains many additional variables relevant to the company's products. The RFC1628 is the generic, standard Management Information Base (MIB) for UPS devices. If you use the RFC1628 MIB, you can also use the three RFC1628 event notifications (see "Configuring event actions"). They can be used to avoid having to configure notification events outside the NMC environment, see **RFC1628 MIB**.
NMS IP/Host Name	The IPv4/ IPv6 address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.
Language	Chose a language from the drop-down list. This can differ from the UI and from other trap receivers.
SNMPv1	Community Name: The name 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).
SNMPv3	User Name: Select the identifier of the user profile for this trap receiver. See also "User Profiles" under "SNMP screens".

SNMP Traps test screen

Path: Configuration > 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 itself 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 screen is displayed. See "SNMP Trap Receivers screen" above.

General menu

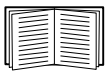
This menu deals with miscellaneous configuration items including device identification, date and time, exporting and importing your NMC configuration options, the three links at the bottom left of the screen, and consolidating data for troubleshooting purposes.

Identification screen

Path: Configuration > General > Identification

Define the **Name** (the NMC System Name, see “DNS screen”), the **Location** (the physical location), and the **Contact** (the person responsible for the device) used by:

- the SNMP agent of the NMC
- Data Center Expert



Specifically, the name field is used by the **sysName**, **sysContact**, and **sysLocation** object identifiers (OIDs) in the NMC’s SNMP agent. For more information about MIB-II OIDs, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide,* available on the **APC website**.

Date/ Time screen

Mode.

Path: Configuration > General > Date/Time > Mode

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

With both, you select the **Time Zone**. This is your local time difference with Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT).

- **Manual Mode**: Do one of the following:
  - Enter the date and time for the NMC or
  - mark the check box **Apply Local Computer Time** to read the date and time settings of the computer you are using and apply those here.
- **Synchronize with NTP Server**: Have an NTP (Network Time Protocol) Server define the date and time for the NMC.

By default, any NMC on the private side of Data Center Expert obtains its time settings by using Data Center Expert as an NTP server.

Field	Description
Override Manual NTP Settings	If you select this, data from other sources (typically DHCP) take precedence over the NTP configurations you set here.
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.
Update Interval	Define, in hours, how often the NMC accesses the NTP Server for an update. *Minimum*: 1; *Maximum*: 8760 (1 year).

Field	Description
Update Using NTP Now	Initiate an immediate update of the date and time by the NTP Server.

Daylight saving.

Path: Configuration > General > Date /Time > Daylight Savings

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

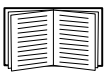
When customizing DST, the system puts the clock forward by an hour when the time and date you specify under **Start** is reached and puts the clock back an hour when the time and date you specify under **End** is reached.

- If your 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, you should still choose **Fourth/Last**.
- If your 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**.

Creating and Importing settings with the config file

Path: Configuration > General > User Config File

You can speed up and simplify the configuration of new devices by re-using the existing configuration settings with this option. Use **Upload** to transfer configuration data to this interface and **Download** to transfer from this interface (and then use the file to configure another interface). The default name of the file is **config.ini**.



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

Configure Links screen

Path: Configuration > General > Quick Links

Use this option to view and change the URL links displayed at the bottom left of each screen of the interface.

To reconfigure a link, click the link name in the **Name** column. You can reset the links to their defaults at any time by clicking on **Reset to Defaults** there.

Logs on Configuration menu

Path: Configuration > Logs > Syslog > *options*

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

This User Guide does not describe Syslog or its configuration values in detail. See **RFC3164** for more information about Syslog.

Identifying Syslog servers

Path: Configuration > Logs > Syslog > Servers

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

Syslog settings

Path: Configuration > Logs > Syslog > Settings

Field	Description
Message Generation	Enable the generation and the logging of Syslog messages for events that have Syslog configured as a notification method. See “Configuring event actions”.
Facility Code	Selects the facility code assigned to the NMC’s Syslog messages (**User**, by default). **NOTE: User** best defines the Syslog messages sent by the NMC. *Do not* change this selection unless advised to do so by the Syslog network or system administrator.

Field	Description
Severity Mapping	Maps each severity level of NMC or Environment events to available Syslog priorities. The local options are Critical, Warning, and Informational. 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”.

Syslog test and format example

Path: Logs > Syslog > Test

Send a test message to the Syslog servers (configured through the “Identifying Syslog servers” option above). The result will be sent to all configured Syslog servers.

Select a severity to assign to the test message and then define the 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.

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

  Example: `APC: Test Syslog is valid.`

Tests menu

Testing and calibrating

Path: Tests > UPS

The options below are only relevant for supported single-phase Easy UPS devices with an AP9544 card installed.

With some UPS devices, you can run a self-test, an alarm test, or a runtime calibration for your UPS. The **Self-Test** and **Calibration** fields display the results of the most recent test and calibration.

A runtime calibration causes the UPS to recalculate its available runtime capacity based on its current load. This ensures that the runtime reported is more accurate. Because a calibration temporarily depletes the UPS batteries, you can perform a calibration only if battery capacity is at 100%. The load on your UPS must be at least 15% without fluctuating to guarantee that a calibration will be accepted.

Caution - Runtime calibrations deeply discharge UPS batteries, which can leave a UPS temporarily unable to support its attached load if a power outage occurs.

Frequent calibrations reduce the life of batteries.

Perform a calibration whenever you significantly increase the load that the UPS is supporting.

The alarm test for a UPS is device-specific and might not be available for your UPS. To enable the alarm, see “UPS General screens”.

- When you select **UPS Alarm Test**, the UPS beeps for four seconds and the LEDs illuminate.
- When you select **UPS Alarm Test - Continuous**, the UPS beeps and illuminates the LEDs until you cancel the test. A separate bullet displays on this screen, **Cancel Continuous Alarm Test**. To cancel the test, select this and click Apply. Alternatively you press any key on the LED display interface of the UPS. This test is useful for locating a UPS.

Setting the NMC LED lights to blink

Path: Tests > Network > LED Blink

If you are having trouble finding your UPS device, enter a number of minutes in the **LED Blink Duration** field, click Apply, and your NMC LED lights will start flashing. This can assist in locating the physical device.

Logs menus

Using the Event and Data Logs

The Event Log records individual occurrences. The Data Log, by contrast, provides you with a snapshot of your system by recording values at regular time intervals.

Event log

Path: Logs > Events > *available options*

With Basic functionality, only the last 25 events are stored in the Event Log.

By default, the log displays all events recorded during the last two days, starting with the latest events. See “Configuring by event”.

In addition, the log records: i) Any event that sends an SNMP trap, except unsuccessful SNMP authentication attempts. ii) Abnormal internal system events.

You can enable event color coding for through “Local Users” on the Configuration menu.

To display the Event Log.

Path: Logs > Events > Log

By default, the Event Log displays the most recent events first. To see the events listed together on a Web page, click the **Launch Log in New Window** button. JavaScript must be enabled in your browser to do this.

To open the log in a text file or to save the log to disk, click on the floppy disk icon,  , in the same line as the **Event Log** heading.

You can also use Secure CoPy (SCP) or FTP to view the Event Log. See “How to use SCP or FTP to retrieve log files”.

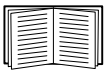
To filter the Event Log. Use filtering to omit information you don’t want to display.

Filtering the log by date or time	Use the **Last** or **From** radio buttons. (The filter configuration is saved until the NMC restarts).
Filtering the log by event severity or category	Click **Filter Log**. Clear a check box to remove it from view. After you click **Apply** text at the upper right corner of the Event Log page indicates that a filter is active. The filter is active until you clear it or until the NMC restarts. To remove an active filter, click **Filter Log**, then **Clear Filter (Show All)**. As Administrator, click **Save As Default** to save this filter as the new default log view for all users.

Important points on filtering:

- Events are processed through the filter using OR logic. If you apply a filter, it works regardless of the other filters.
- Events that you cleared in the **Filter By Severity** list never display in the filtered Event Log, even if selected in the **Filter by Category** list.
- Similarly, events that you clear in the **Filter by Category** list never display in the filtered Event Log.

To delete the Event Log. To delete all events, click **Clear 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 groups of events”.

To configure reverse lookup:

Path: Logs > Events > Reverse Lookup

With reverse lookup enabled, when a network-related event occurs, both the IP address *and* the domain name for the networked device 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.

Reverse lookup is disabled by default. You should not need to enable it if you have no DNS server configured or have poor network performance because of heavy network traffic.

To resize the Event Log.

Path: Logs > Events > Size

Use Event Log Size to specify the maximum number of log entries.

Caution: When you resize the Event Log in order to specify a maximum size, *all existing log entries are deleted*. To avoid losing log data, use SCP or FTP to retrieve the log first, see “How to use SCP or FTP to retrieve log files”. When the log subsequently reaches the maximum size, the older entries are deleted.

Data log

Path: Logs > Data > *options*

Use the Data Log to display measurements about the UPS, the power input to the UPS, and the ambient temperature of the UPS and batteries.

The steps to display and resize the Data Log are the same as for the Event Log, except that you use menu options under **Data** instead of **Events**. See “To display the Event Log” and “To resize the Event Log”.

To filter the Data Log by date or time, use the **Last** or **From** radio buttons. (The filter configuration is saved until the NMC restarts). To delete all data recorded in the Data Log, click **Clear Data Log**. Deleted data cannot be retrieved.

To set the data collection interval (Logs > Data > Interval): Define, in the **Log Interval** setting, how frequently data is searched for and stored in the Data Log. When you click Apply, the number of possible storage days is recalculated and display at the top of the screen.

When the log is full, the oldest entries are deleted. To avoid automatic deletion of older data, see “To configure Data Log rotation (Logs > Data > Rotation):” directly below.

NOTE: Because the interval specifies how often the data is recorded, the *smaller the interval*, the more times the data is recorded and the larger the log file.

To configure Data Log rotation (Logs > Data > Rotation): Rotation causes the contents of the Data Log to be appended to the file you specify by name and location. This means you can store the data before it is deleted, see “To set the data collection interval (Logs > Data > Interval):” directly above.

Use this option to set up password-protection and other parameters.

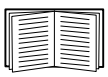
Field	Description
FTP Server	The IP address or host name of the server where the file will reside.
User Name **Password**	The user name with password required to send data to the repository file. This user must also be configured to have read and write access to the data repository file and the directory (folder) in which it is stored.
File Path	The path to the repository file.
Filename	The name of the repository file (an ASCII text file), e.g. `datalog.txt`. Any new data is appended to this file, it does not overwrite it.
Unique Filename	Select this check box to save the log as `mmddyyyy_<filename>.txt`, where filename is what you specified in the **Filename** field above. Any new data is appended to the file but each day has its own file.
Delay *n* hours between uploads.	The number of hours between uploads of data to the file (max. 24 hours).
Upon failure, try uploading every *n* minutes	The number of minutes between attempts to upload data to the file after an upload does not work.
up to *n* times	The maximum number of times the upload will be attempted after it does not work initially.
until upload succeeds	Attempt to upload the file until the transfer is completed.

How to use SCP or FTP to retrieve log files

An Administrator or Device User can use SCP or FTP to retrieve a tab-delineated Event Log file (*event.txt*) or Data Log file (*data.txt*) and import it into a spreadsheet. Both reside on the NMC.

- The file reports all events or data recorded since the log was last deleted, or truncated because it reached maximum size.
- The file includes information that the Event Log or Data Log does not display.
  - The Application version
  - The date and time the file was retrieved
  - The **Name**, **Contact**, and **Location** values and IP address of the NMC
  - The name of the UPS Model (*data.txt* file only)
  - The unique **Event Code** for each recorded event (*event.txt* file only)
  - The NMC uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits.

If you are using the encryption-based security protocols, see “To use SCP to retrieve the files”. If you are using unencrypted authentication methods for security, see “To use FTP to retrieve the files”.



See the **Security Handbook** on the APC website for information on available protocols and methods for setting up the type of security you need.

To use SCP to retrieve the files. Enable SSH on the NMC, see “Console access”. **NOTE:** The below commands are examples only.

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

```
scp <username@hostname> or <ip_address>:event.txt ./event.txt
```

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

```
scp <username@hostname> or <ip_address>:data.txt ./data.txt
```

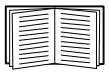
To use FTP to retrieve the files. To use FTP to retrieve the *event.txt* or *data.txt* file:

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

   If the **Port** setting for the **FTP Server** option (see “FTP Server”) has been changed from its default (`21`), you must use the non-default value in the FTP command.

   For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

   ```
   ftp>open ip_address port_number
   ```

   To set a non-default port value to enhance security for the FTP Server, see “FTP Server”. 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 user name. For the Device User, the default user name is `device`.
3. To set the file transfer mode to binary, type:

   ```
   ftp>bin
   ```

   To show a progress bar during file transfer, type:

   ```
   ftp>hash
   ```

4. Use the `get` command to transmit the text of a log to your local drive.

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

   or

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

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

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

   or

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

   You will not be asked to confirm the deletion.

   – If you clear the Data Log, the Event Log records a deleted-log event.
   – If you clear the Event Log, a new *event.txt* file records the event.

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

UPS Log

Path: Logs > UPS

This menu option is not available for all UPS devices.

This information is derived from your UPS device and is separate from your NMC logs. (It is not directly related to or a subset of the NMC “Event log”).

The information can be useful to help the technical support team solve problems.

UPS Transfer Logs Displays a table of the UPS stored transfer events, including transfers to battery and transfers to bypass.

UPS Fault Logs Displays a table of the UPS stored faults.

Firewall Log

Path: Logs > Firewall

If you create a firewall policy, firewall events will be logged here. For more information on implementing a policy, see “Firewall screens”.

The information can be useful to help the technical support team solve problems.

Log entries contain information about the traffic and the rules action (allowed, discarded). When logged here, these events are not logged in the main Event Log. See “Event log”.

A firewall log contains up to 50 of the most recent events. The firewall log is cleared when the NMC reboots.

About menu

About the Network Management Card

About the UPS device

Path: About > UPS

The information displayed under UPS varies according to the device used.

Field	Description
Product Name	The name of the UPS product line.
Model	This field identifies your UPS device.
Manufacture Date	The date your UPS was manufactured.
Serial Number	The unique identification number of the UPS. The serial number is also on the outside of the UPS.
Manufacture Date	The date your UPS was manufactured.
Firmware Version	The version numbers of the firmware modules currently installed on the UPS
Manufacturer Name	The UPS manufacturer.
Rated VA	The rated apparent power of the UPS in VA.
Rated Input Voltage	The rated input voltage of the UPS in VAC.
Rated Output Voltage	The rated output voltage of the UPS in VAC
Rated Output Frequency	The rated frequency of the output voltage of the UPS in Hz.
Rated Output Current	The rated output current of the UPS in A.
Rated Battery Voltage	The rated voltage of the UPS battery in VDC.
Input Phases	The number of input phases of the UPS.
Output Phases	The number of output phases of the UPS.

The **About UPS Battery Packs** table displays the firmware version, model, serial number, and manufacture date of the UPS battery packs.

About the NMC and the firmware modules

Path: About > Network

Hardware Factory: This hardware information is useful for troubleshooting problems with your NMC device. **Management Uptime** refers to the length of time this management interface has been running continuously; that is, the length of time since the NMC has been warm or cold started.

Application Module, **APC OS (AOS)**, and **Boot Monitor**: This information is useful for troubleshooting, and for determining if updated firmware is available, **www.apc.com/shop/us/en/tools/software-firmware**.

Field Label	Description
Name	The name of the firmware module. The **Application Module** name differs according to the UPS device type. The **APC AOS module** is always named **aos**, and the **boot monitor module** is always named **boot**.
Version	The version number of the firmware module. Version numbers of the modules may differ, but compatible modules are released together. See “Upgrading Firmware”.
Date/ Time	The date and time at which the firmware module was loaded.

See also “Verify the version numbers of installed firmware”.

Support screen

Path: About > Support

With this option, you can consolidate various data in this interface into a single zipped file for troubleshooting purposes and customer support. The data includes the event and data logs, the configuration file (see “Creating and Importing settings with the config file”) and complex debugging information.

Click **Generate Logs** to create the file and then **Download**. You are asked whether you want to view or save the zipped file.

Device IP Configuration Wizard

Capabilities, Requirements, and Installation

The Device IP Configuration Wizard can discover Network Management Cards (NMC) that do not have an IP address assigned. Once discovered, you can configure the IP address settings for the cards.

You can also search for devices already on the network by entering an IP range to define the search. The Wizard scans the IP addresses in the defined range and discovers cards that already have a DHCP-assigned IP address.

NOTES:

• You cannot search for assigned devices already on the network using an IP range unless you enable SNMPv1 on the NMC and set the **Community Name** to “public”. For more information, see "SNMP screens".

• When the NMC IP address is configured, to access the NMC Web UI in a browser, you must update the URL from `http` to `https`.

For detailed information on the Wizard, see Knowledge Base article **FA156064** on the **APC website**.

Knowledge Base article FA156064 also details the use of DHCP Option 12.

System requirements

The Wizard runs on Windows Server® 2012, Windows Server 2016, Windows Server 2019 and on both 32- and 64-bit versions of Windows 8.1 and Windows 10 operating systems.

The Wizard is for IPv4 only.

Installation

To install the Wizard from a downloaded executable file:

1. Go to **www.apc.com/shop/tools/software-firmware**.
2. Filter by Software / Firmware > Wizards and Configurators.
3. Download the Device IP Configuration Wizard.
4. Run the executable file in the folder to which you downloaded it.

When installed, the Wizard is available through the Windows menu options.

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 (NMC) and export it to another NMC or to multiple NMCs. The steps are below, see details in the sections following.

1. Configure an NMC with the desired settings and export them, see “Creating and Importing settings with the config file”.
2. Retrieve the .ini file from that NMC.
3. Customize the file to change the TCP/IP settings at least.
4. Use a file transfer protocol supported by the NMC to transfer a copy to one or more other NMCs. For a transfer to multiple NMCs, use an FTP or SCP script or the .ini file utility.

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

Contents of the .ini file

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

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

Detailed procedures

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

1. If possible, use the interface of an NMC to configure it with the settings to export. (Directly editing the .ini file risks introducing errors).
2. The example below shows how to use FTP to retrieve config.ini from the configured NMC using a command prompt type client:
   a. Open a connection to the NMC, using its IP address:

      ```
      ftp> ip_address
      ```

   b. Log on using the Administrator user name and password.
   c. To set the file transfer mode to binary, type:

      ```
      ftp> bin
      ```

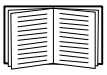
      To show a progress bar during file transfer, type:

      ```
      ftp> hash
      ```

   d. Retrieve the config.ini file containing the NMC’s settings:

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

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



To retrieve configuration settings from multiple NMCs and export them to other NMCs, see *Release Notes: ini File Utility,* available on the **APC website**. Or see Knowledge Base article **FA156117** at **http://www.apc.com/support**.

Customizing. You must customize the file before you transfer it to another NMC.

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

     ```
     NTPEnable=enabled
     ```

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

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

- From the user interface of the receiving NMC, select **Configuration** - **General** - **User Config File**. Enter the full path of the file, or use **Browse** on your local PC.
- Use any file transfer protocol supported by Network Management Cards, i.e., FTP, FTP Client, SCP, or TFTP. The following example uses FTP:
  a. From the folder containing the copy of the customized .ini file, use FTP to log in to the NMC to which you are exporting the .ini file:

     ```
     ftp> open ip_address
     ```

  b. To set the file transfer mode to binary, type:

     ```
     ftp> bin
     ```

     To show a progress bar during file transfer, type:

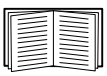
     ```
     ftp> hash
     ```

  c. Export the copy of the customized .ini file to the root directory of the receiving NMC:

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

Transferring the file to multiple NMCs. Follow these steps:

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



To create the batch file and use the utility, see *Release Notes: ini File Utility,* available on the **APC website**. Or see Knowledge Base article **FA156117** at **http://www.apc.com/support**.

The Upload Event and Error Messages

The event and its error messages

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

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

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

Event text	Description
Configuration file warning: Invalid keyword on line *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

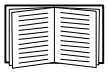
A device associated with the NMC from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the device (such as a UPS) is not present or is not discovered, the config.ini file contains a message under the appropriate section name, instead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

```
UPS not discovered
```

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.

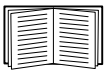


See “Contents of the .ini file” for information about which values are overridden.

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

Related Topics

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



See “Device IP Configuration Wizard”.

File Transfers

Upgrading Firmware

When you upgrade the firmware on the Network Management Card (NMC), you obtain the latest new features, security and performance improvements, and bug fixes.

Upgrading here means simply placing the `.nmc3` file on the NMC, there is no installation as such. Check regularly on **www.apc.com/shop/tools/software-firmware** for any new upgrades.

The `.nmc3` file name has the following format:

`apc_hardware-version_type_firmware-version.nmc3`

- `apc`: Indicates the context.
- `hardware-version: hw0n` where n identifies the hardware version on which you can use this file.
- `type`: Identifies which module.
- `version`: The version number of the file.

Firmware File Transfer Methods

Obtain the free, latest firmware version from **www.apc.com/shop/tools/software-firmware**. To upgrade the firmware of one or more NMCs, use one of these four methods:

- On a Windows operating system, use the **Firmware Upgrade Utility** downloaded from the **APC website**. See “Using the NMC Firmware Upgrade Utility”.
- On any supported operating system, use **FTP or SCP** to transfer the `.nmc3` file. See “Use FTP or SCP to upgrade one Network Management Card”.
- For a Network Management Card that is NOT on your network, use **XMODEM** through a USB virtual communication port via the boot loader to transfer the `.nmc3` file from your computer to the NMC. See “Use XMODEM to upgrade one NMC”.
- Use a **USB drive** to transfer the firmware file from your computer. See “Use a USB drive to transfer and upgrade the files”.
- For upgrades to **multiple NMCs**, see “Upgrading the firmware on multiple Network Management Cards” and “Using the NMC Firmware Upgrade Utility for multiple upgrades on Windows”.

Using the NMC Firmware Upgrade Utility

This Firmware Upgrade Utility is part of the firmware upgrade package available on the **APC website**. (*Never* use an Upgrade Utility designated for one product to upgrade the firmware of another product).

Using the Utility for upgrades on Windows systems. On any supported Windows operating system, the NMC Firmware Upgrade Utility automates the transferring of the `.nmc3` file.

Unzip the downloaded firmware upgrade file and double-click the .exe file. Enter the Host IP address, the user name, and the password in the dialog fields. You must also select either FTP or SCP and its associated port. **NOTE:** The chosen protocol must be enabled on the NMC device for the firmware upgrade to complete. See also “Using the NMC Firmware Upgrade Utility for multiple upgrades on Windows”.

Use FTP or SCP to upgrade one Network Management Card

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

- The NMC must be on the network, with its system IP, subnet mask, and default gateway configured.
- The FTP server must be enabled at the NMC, see “FTP Server”.

To transfer the file, perform these steps:

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

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

   For file information, see “About the NMC and the firmware modules”.

2. Open an FTP client session:

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

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

   - For Windows FTP clients, separate a non-default port number from the IP address by a space. For example (showing a space before 21000):
     `ftp> open 150.250.6.10 21000`
   - Some FTP clients require a colon instead before the port number.

4. Log on as Administrator.
5. Upgrade the firmware.

   `ftp> bin`
   `ftp> put apc_hw21_AA_v-v-v-v.nmc3` (where AA is the application, e.g. eu3p, and v-v-v-v is the firmware version number)

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

SCP. To use Secure CoPy (SCP) to upgrade firmware for the NMC, follow these steps:

1. Use an SCP command line to transfer the `.nmc3` file to the NMC. The following example uses *v-v-v-v* to represent the version number of the application module:

   ```
   scp apc_hw21_eu3p_v-v-v-v.nmc3 apc@158.205.6.185:apc_hw21_eu3p_v-v-v-v.nmc3
   ```

NOTE: To use SCP, SSH must be enabled. See “Console screen” to enable SSH.

Use XMODEM to upgrade one NMC

To use XMODEM to upgrade one NMC that is not on the network:

1. Connect the provided micro-USB cable (part number 960-0603) to the NMC and to the USB port on a local computer.
2. Press the **Reset** button on the NMC.
3. When the NMC detects a USB connection while it is booting up, it will wait 90 seconds to allow enough time for the operating system to recognize and configure a virtual communication port. When the virtual communication port is ready, run a terminal program, such as HyperTerminal or Tera Term to select the virtual communication port.
4. Press the **Enter** key twice, or until the Boot Monitor prompt displays: `BM>`

   NOTE: If no connection to the Boot Monitor is made within 90 seconds of rebooting the NMC, the NMC will continue with its normal boot process.
5. Type `XMODEM`, then press **Enter**.
6. From the terminal program's menu, select XMODEM, then select the `.nmc3` file to transfer using XMODEM. After the XMODEM transfer is complete, the Boot Monitor prompt returns.

   Type `reset` or press the **Reset** button to restart the NMC.

NOTE: A driver is required to connect to the NMC console via Windows 7. The driver can be downloaded from the AP9544/AP9547 product page on the **APC website**, located in the **Software / Firmware** section. No driver is required for Windows 10.

1. When you connect the NMC via the micro-USB cable, a device called "NMC3-CDC" is discovered in "Other Devices".
2. Right-click on this device and select "Update Driver Software..."
3. Select the "Browse my computer for driver software" option and navigate to the download location of the driver (usb_cdc_ser.inf).
4. Accept the unsigned driver security message.

Windows will now recognize the NMC and assign a COM port to the device.

Use a USB drive to transfer and upgrade the files

This feature is available in bootloader version v1.3.3.1 and higher. Before starting the transfer, make sure the USB drive is formatted in FAT, FAT16 or FAT32.

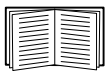
1. Download the firmware upgrade file.
2. Create a folder named **apcfirm** on the USB flash drive.
3. Place the `.nmc3` file in the **apcfirm** directory.
4. Use a text editor to create a file named **nmc3.rcf.** (The file extension must be .rcf, not .txt for example.)
5. In **nmc3.rcf**, add a line for the firmware package to be upgraded.
   For example, to upgrade 3-Phase Easy UPS **application** version v1.5.0.6, type:

   NMC3=apc_hw21_eu3p_1-0-0-1.nmc3
6. Place nmc3.rcf in the **apcfirm** folder on the flash drive.
7. Insert the flash drive into a USB port on your NMC, see "Front Panel (AP9544/AP9547)".
8. Reboot the NMC and wait for the card to reboot fully.
9. Check that the upgrade was completed successfully using the procedures in "Verifying Upgrades".

Upgrading the firmware on multiple Network Management Cards

Use one of these three methods:

- **NMC Firmware Upgrade Utility on Windows**. See “Using the NMC Firmware Upgrade Utility for multiple upgrades on Windows”.
- **Use FTP or SCP**. To upgrade multiple NMCs using an FTP client or using SCP, write a script which automatically performs the procedure.
- **Export configuration settings**. You can create batch files and use a utility to retrieve configuration settings from multiple NMCs and export them to other NMCs.



See *Release Notes: ini File Utility,* available on the Knowledge Base, **http://www.apc.com/site/support/**.

Using the NMC Firmware Upgrade Utility for multiple upgrades on Windows. After downloading the Upgrade Utility from the NMC downloads page on the **APC website**, double click on the .exe file and unzip the contents.

1. Locate the `devices.txt` file in the directory with the Utility. Open and modify this file with a text editor to enter the necessary information, for each NMC device to be upgraded:
   - [Device]: This section header must be included for each NMC to be upgraded.
   - Host: The IPv4 address of the device.
   - Protocol: SCP or FTP.
   - Port: The associated port of SCP or FTP.
   - Username: The username of an Administrator, enabled on the NMC.
   - Password: The password of an Administrator, enabled on the NMC

   Remove all comments and semicolons from `devices.txt`, and save your changes.

   For example:

   ```
   [Device]
   Host=192.168.0.1
   Protocol=SCP
   Port=22
   Username=apc
   Password=apc


   [Device]
   Host=192.168.0.2
   Protocol=SCP
   Port=22
   Username=apc
   Password=apc
   ```

   You can use an existing `devices.txt` file if it already exists.
2. Open the Firmware Upgrade Utility. If the correct details were provided in the `devices.txt` file, the following message will appear in the Utility:

   ```
   A device list was detected and imported, therefore the hosts listed in
   the event window below will be used as the active.
   ```
3. Click **Start Update** in the Utility to start the firmware version upgrade(s).

Verifying Upgrades

Verify the success of the transfer

To verify whether a firmware upgrade succeeded, you can use the `xferStatus` command in the command line interface to view the last transfer result.

Last Transfer Result codes

Possible transfer errors include the TFTP or FTP server not being found, or the server refusing access, the server not finding or not recognizing the transfer file, or a corrupt transfer file.

Verify the version numbers of installed firmware

Path: About - Network

Use the Web UI to verify the versions of the upgraded firmware modules. You could also use an SNMP GET to the MIB II **sysDescr** OID. In the command line interface, use the **about** command.

Changing UI Language

You can display the NMC user interface (UI) in different languages by selecting a language from the **Language** drop-down box in the **Login** screen.

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

Troubleshooting

Network Management Card Access Problems

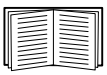
Visit the Knowledge Base at www.apc.com/support for step-by-step troubleshooting, and helpful solutions to common issues. To contact customer support, see “APC by Schneider Electric Worldwide Customer Support”.

Problem	Solution
Unable to ping the NMC	If the NMC’s Status LED is green, try to ping another node on the same network segment as the NMC. If that does not work, it is not a problem with the NMC. If the Status LED is not green, or if the ping test succeeds, perform the following checks: • Verify that the NMC is properly seated in the UPS. • Verify all network connections. • Verify the IP addresses of the NMC and the NMS. • If the NMS is on a different physical network (or subnetwork) from the NMC, verify the IP address of the default gateway (or router). • Verify the number of subnet bits for the NMC’s subnet mask.
Cannot allocate the communications port through a terminal program	Before you can use a terminal program to configure the NMC, 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 disabled, and SSH is enabled. SSH and Telnet can be enabled/disabled independently. • For SSH, the NMC may be creating a host key. The NMC can take up to one minute to create the host key, and SSH is inaccessible for that time.
Cannot access the user interface (UI)	• Verify that HTTP or HTTPS access is enabled. • Make sure you are specifying the correct URL — one that is consistent with the security system used by the NMC. SSL requires https, not http, at the beginning of the URL. • Verify that you can ping the NMC. • Verify that you are using a Web browser supported for the NMC. See “APC by Schneider Electric Worldwide Customer Support”. • If the NMC has just restarted and SSL security is being set up, the NMC may be generating a server certificate. The NMC can take up to one minute to create this certificate, and the SSL server is not available during that time.

SNMP Issues

Problem	Solution
Unable to perform a GET	• Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3). • Use the command line interface or UI to ensure that the NMS has access. See “SNMP screens”.
Unable to perform a SET	• Verify that SNMP is enabled. SNMPv1 and SNMPv3 are disabled by default. • Verify the read/write (SET) community name (SNMPv1) or the user profile configuration (SNMPv3). • Use the command line interface or UI 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 screens”.
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** 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 UI to correct the trap receiver definition. • For SNMPv3, check the user profile configuration for the NMS, and run a trap test. See “SNMP screens”, “Trap Receivers”, and “SNMP Traps test screen”.
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.

Modbus Problems



For detailed information on Modbus registers and bit descriptions, see the *Modbus Register Maps* available on the **APC website**.

APC USB Wi-Fi Device (AP9834) Problems

Problem	Solution
Unable to connect to wi-fi network	• Verify that the APC USB Wi-Fi Device is correctly inserted in a USB port of an AP9544/AP9547 card. • Verify that the correct Wi-Fi settings are provided in the NMC Web UI or CLI. • Verify that there are no Wi-Fi-related events in the NMC's Event Log. If the Wi-Fi settings are entered incorrectly or left blank, the NMC will log an error to the Event Log. For example: "USB Wi-Fi Device error. Wi-Fi Settings". If the issue still persists, contact a network administrator to diagnose connection issues.
Unable to resolve the Device's solid red LED state	• Verify that the correct Wi-Fi settings are provided in the NMC Web UI or CLI. • Resolve any Wi-Fi-related events in the NMC's Event Log. For example: "USB Wi-Fi Device error. Wi-Fi Settings". • Re-enable the wired connection and configure the Wi-Fi settings via an alternative method: – Web UI (**Configuration > Network > Wi-Fi**) – Command Line Interface (`wifi` command) – config.ini file (`NetworkWiFi` section) If the wired connection is no longer available, connect the micro-USB cable (960-0603) to the console port of the NMC to access the CLI, and transfer the config.ini file using the xferINI command. For more information see the **Network Management Card for Easy UPS CLI Guide**. If the issue still persists, contact Customer Support. See "APC by Schneider Electric Worldwide Customer Support".

LED Descriptions

Condition	Description
Off	One of the following situations exists: • The Device is not inserted in a USB port on an AP9544/AP9547 NMC. • The NMC's firmware does not support Wi-Fi. Wi-Fi support is available in firmware version 1.4 and higher. See "File Transfers". • The Device is not operating properly. It may need to be repaired or replaced. Contact Customer Support. See "APC by Schneider Electric Worldwide Customer Support".
Solid green	The Device is connected to an access point but there is no network activity.
Flashing green	The Device is connected to an access point and the Wi-Fi network is active.

Condition	Description
Solid red	One of the following situations exists: • There is a permanent error with the Device. • There is a permanent error with the NMC Wi-Fi settings. • There are unresolvable issues connecting to an access point.
Flashing red	The Device is in the process of making a Wi-Fi connection to an access point.

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.

Copyright Notices

Cryptlib Cryptology Library

Cryptlib copyright © Digital Data Security New Zealand Ltd 1998.

Berkeley Database

Copyright © 1991, 1993 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Lua

Copyright © 1994–2021 Lua.org, PUC-Rio.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

APC by Schneider Electric Worldwide Customer Support

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

- Visit the Schneider Electric Web site to access documents in the Schneider Electric Knowledge Base and to submit customer support requests.
  - **www.apc.com** (Corporate Headquarters)
    Connect to localized Schneider Electric Web sites for specific countries, each of which provides customer support information.
  - **www.apc.com/support/**
    Global support searching Schneider Electric Knowledge Base and using e-support.
- Contact the Schneider Electric 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 representative or other distributors from whom you purchased your product.

990-91545C-001 **7/2023**