Schneider Electric

# User's Guide

## UPS Network Management Card 2

**AP9630, AP9631**

This manual is available in English on the APC Web site (www.apc.com).

Dieses Handbuch ist in Deutsch auf der APC Webseite (www.apc.com) verfügbar.

Este manual está disponible en español en la página web de APC (www.apc.com).

Ce manuel est disponible en français sur le site internet d'APC (www.apc.com).

Questo manuale è disponibile in italiano sul sito web di APC (www.apc.com).

Este manual está disponível em português no site da APC (www.apc.com).

Данное руководство на русском языке доступно на сайте APC (www.apc.com )

本マニュアルの日本語版はAPC ウェブサイト（www.apc.com）からダウンロードできます。

APC 웹싸이트 (www.apc.com) 에 한국어 매뉴얼 있습니다 .

在 APC 公司的网站上（www.apc.com）有本手册的中文版。

This manual is available in English on the enclosed CD.

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

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

Ce manuel est disponible en français sur le CD-ROM ci-inclus.

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

Este manual está disponível em português no CD fornecido.

Данное руководство на русском языке имеется на прилагаемом компакт-диске.

本マニュアルの日本語版は同梱の CD-ROM からご覧になれます。

동봉된 CD 안에 한국어 매뉴얼이 있습니다 .

您可以从包含的 CD 上获得本手册的中文版本。

# Introduction

## Product Description

### Features

The two Schneider Electric UPS Network Management Cards (NMC) mentioned below are Web-based, IPv6 Ready products. They can manage supported devices using multiple open standards such as:

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

The **AP9630** Network Management Card 2:

- Provides UPS control and self-test scheduling features.
- Provides data and event logs.
- Enables you to set up notifications through event logging, e-mail, and SNMP traps.
- Provides support for PowerChute® Network Shutdown.
- Supports using a Dynamic Host Configuration Protocol (DHCP) or BOOTstrap Protocol (BOOTP) server to provide the network (TCP/IP) values of the NMC.
- Supports using the Remote Monitoring Service (RMS).
- Provides the ability to export a user configuration (.ini) file from a configured card to one or more unconfigured cards without converting the file to a binary file.
- Provides a selection of security protocols for authentication and encryption.
- Communicates with StruxureWare Central or InfraStruxure Manager.

The **AP9631** Network Management Card includes all AP9630 Network Management Card features and the following:

- Provides two USB ports, which support upgrading the firmware.
- Supports two universal input/ output ports, to which you can connect:
  - Temperature (AP9335T) or temperature/humidity sensors (AP9335TH)
  - Relay input/output connectors that support two input contacts and one output relay (using the AP9810 Dry Contact I/O Accessory, which is an optional add-on)

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

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

## IPv4 initial setup

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

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

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

To configure the TCP/IP settings, see the Network Management Card *Installation Manual*, available on the Network Management Card *Utility* CD, 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 DHCP, see the “TCP/IP settings for IPv6 screen”.

## Network management with Other Applications

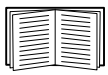
These applications and utilities work with a UPS that connects to the network through an NMC.

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

# Internal Management Features

## Overview

Use the Web 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 Command Line Interface (CLI) guide on the Network Management Card *Utility* CD and 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 — Administrator, Device User, Read-Only User and Network-only User — and these are protected by user name and password requirements.

- An **Administrator** or super user can use all of the menus in the UI and all of the commands in the command line interface. The default user name and password are both `apc`.
- 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 the default password is `apc`.
- A **Read-Only User** has the following restricted access:
  - Access through the UI only.
  - 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 the default password is `apc`.
- A **Network-only User** can only log on using the Web user interface (UI) and CLI (telnet not serial). There is no default name and password.

To set **User Name** and **Password** values for the top three account types, see “Local Users”.

# How to Recover from a Lost Password

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

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

   ```
   user -n <user name> -pw <user password>
   ```

   For example, to change a password to **XYZ**, type:

   ```
   user -n apc -pw XYZ
   ```

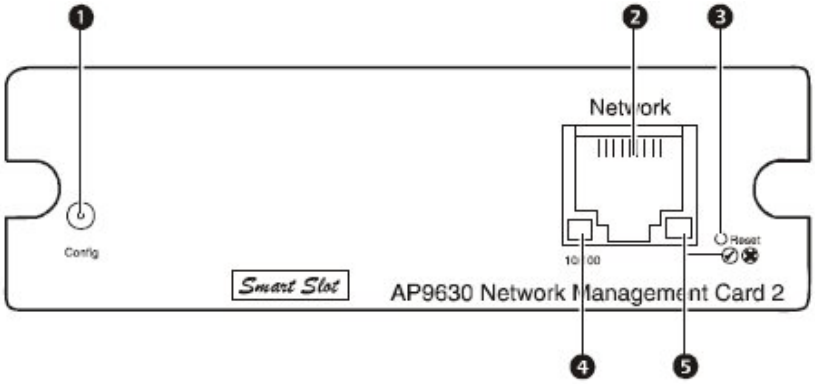
   For a Super User, you must also specify the current password:

   ```
   user -n <user name> -cp <current password> -pw <user password>
   ```

   For example, for a Super User, to change the password to XYZ (from the default user name and password of **apc**):

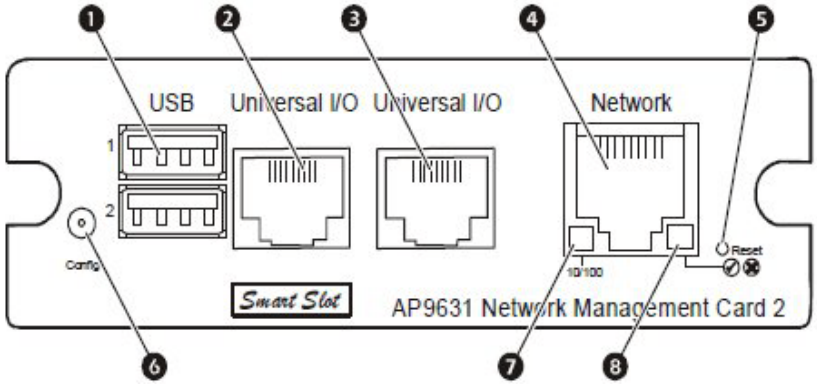
   ```
   user -n apc -cp apc -pw XYZ
   ```
8. Type `quit` or `exit` to log off, reconnect any serial cable you disconnected, and restart any service you disabled.

# Front Panel (AP9630)




| | Item | Description |
|---|---|---|
| ❶ | Serial configuration port | Connects the NMC to a local computer to configure initial network settings or access the command line interface (CLI). |
| ❷ | 10/100 Base-T connector | Connects the NMC to the Ethernet network. |
| ❸ | Reset button | Resets the NMC while power remains on. |
| ❹ | Link-RX/TX (10/100) LED | See “Link-RX/TX (10/100) LED”. |
| ❺ | Status LED | See “Status LED”. |

# Front Panel (AP9631)




| | Item | Description |
|---|---|---|
| ❶ | USB ports | Supports NMC firmware upgrades, see “File Transfers”. |
| ❷ ❸ | Sensor ports | Connect temperature sensors, temperature/humidity sensors, or relay input/ output connectors that support two input contacts and one output relay. |
| ❹ | 10/100 Base-T connector | Connects the NMC to the Ethernet network. |
| ❺ | Reboot button | Reboots (resets) the NMC while power remains on. |
| ❻ | Serial configuration port | Connects the NMC to a local computer to configure initial network settings or access the command line interface (CLI). |
| ❼ | Link-RX/TX (10/100) LED | See “Link-RX/TX (10/100) LED”. |
| ❽ | 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:<br>• The NMC is not receiving input power.<br>• The NMC is not operating properly. It may need to be repaired or replaced. Contact Customer Support. See “APC Worldwide Customer Support”. |
| Solid green | The NMC has valid TCP/IP settings. |
| Solid orange | A hardware malfunction has been detected in the NMC. Contact Customer Support. See “APC Worldwide Customer Support”. |
| 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]<br>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 Installation Manual provided in printed format and on the Network Management Card *Utility* CD in PDF to configure the TCP/IP settings of the NMC.
2. To use a DHCP server, see “DHCP response options”.

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

This LED indicates the network status of the NMC.

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

# Watchdog Features

## Overview

To detect internal problems and recover from unanticipated inputs, the 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, such as an Address Resolution Protocol [ARP] request), it assumes that there is a problem with its network interface and restarts.

## Resetting the network timer

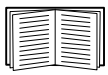
To ensure that the NMC does not restart if the network is quiet for 9.5 minutes, the NMC attempts to contact the default gateway every 4.5 minutes. If the gateway is present, it responds to the NMC, and that response restarts the 9.5-minute timer. If your application does not require or have a gateway, 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.

# Web User Interface

## Introduction

### Overview

The Web user interface (UI) provides options to manage the UPS and the UPS Network Management Card 2 (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

You can use Microsoft® Internet Explorer® (IE) 7.x or higher (on Windows® operating systems only) or Mozilla® Firefox® 3.0.6 or higher (on all operating systems) to access the NMC through its UI. 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
- `device` for a Device User
- `readonly` for a Read-Only User

The default password is `apc` for these three account types. There is no default for a Network-only account type. 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 “Adding and Changing Language Packs”.

When HTTPS is enabled, the NMC generates its own certificate. This certificate negotiates encryption methods with your browser. Refer to the Security Guide on the CD or on the www.apc.com 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.

**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 | |

**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` |

# 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**.

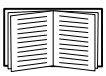
## Icons and Links

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 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”
- “Outlet Groups on Status menu”
- “Battery System on Status menu”
- “Universal I/O on Status menu”
- “Network on Status menu”

## UPS on Status menu

**Path: Status > UPS**

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

| Field | Description |
|---|---|
| **Last Battery Transfer** | The cause of the last switch to battery operation. |
| **Internal Temperature** | The temperature inside the UPS |
| **Runtime Remaining** | How long the UPS can use battery power to support its present load. |
| **UPS Input** | |
| **Input Voltage** | The AC voltage (VAC) being received by the UPS. |
| **Bypass Input Voltage** | The AC voltage (VAC) used when the UPS is in bypass mode.<br>This option is not available for all UPS devices. |
| **UPS Output** | |
| **Output Voltage** | The AC voltage (VAC) that the UPS is supplying to its load. |
| **Load Current** | The current, in Amps, supplied by the input voltage. |
| **Output Load** | The load placed on each phase by the attached equipment, in kVA. |
| **Output Percent Load** | The load placed on each phase by the attached equipment, as a percentage of the kVA available with no redundancy. |
| **Output Percent Power** | The load placed on each phase by the attached equipment, as a percentage of the available kVA. |
| **Output Watts** | The UPS load as a percentage of available Watts. |
| **Output VA** | The UPS load as a percentage of available VA. |
| **Output Efficiency** | The percentage of the input power going directly out to the load. Input power not going to the load is consumed by the UPS. |
| **Output Energy Usage** | The energy used by the load, starting from when the UPS was last reset to defaults. |

| Field | Description |
|---|---|
| **Battery Status** | |
| **Battery Capacity** | The percentage of the UPS battery capacity that is available to support the attached equipment. |
| **Battery Voltage** | The DC voltage of the batteries. |
| **External Batteries** | The number of batteries connected to the UPS, excluding any internal batteries. |

The options below are not available for all UPS devices.

| Field | Description |
|---|---|
| **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. |
| **Actual Battery Bus Voltage** | The available DC power. |
| **External Battery Cabinet Rating** | The battery cabinet Amp-Hour rating of an external battery source. |
| **Batteries** | The total number of batteries (both internal and external) that the UPS has. |
| **Bad Batteries** | The number of “bad” batteries (the batteries that need to be replaced). |
| **Battery Current** | The current being output from the battery. |
| **Next Battery Replacement Date** | Among the installed UPS battery cartridges, this is the earliest recommended date for replacing your batteries. |
| **Intelligence Module** | Information about the Intelligence Module. You may be asked for this information (Firmware Revision, Manufacture Date, Serial Number, and Hardware Revision) when seeking assistance from APC Customer Support. |
| **Input Voltage** | The AC voltage (VAC) being received by the UPS. |
| **Bypass Input Voltage** | The AC voltage (VAC) used when the UPS is in bypass mode. |
| **Input Frequency** | The frequency in Hertz (Hz) of the voltage being received by the UPS. |
| **Frequency** | The frequency in Hertz (Hz) shared by the input voltage and output voltage. |
| **Bypass Frequency** | The frequency in Hertz (Hz) of the voltage used when the UPS is in bypass mode. |
| **Output Current** | The current, in Amps, applied to the load. |
| **Output Frequency** | The frequency in Hertz (Hz) of the output voltage. |
| **Load Power** | The UPS load as a percentage of available Watts. |
| **Apparent Load Power** | The UPS load as a percentage of available VA. |
| **Modules** | Information about the modules installed in the UPS. You may be asked for this information (Firmware Revision, Manufacture Date, Serial Number, and Hardware Revision) when seeking assistance from APC Customer Support. |
| **Power Module** | Information about the power module installed in the UPS. You may be asked for this information when seeking assistance from APC Customer Support. |

# Outlet Groups on Status menu

**Path: Status > Outlet Groups**

This option is not available for all UPS devices. It displays status details of all outlet groups on your UPS. See also “Outlet Groups on Control menu” and “Outlet Groups on Configuration menu”.

# Battery System on Status menu

**Path: Status > Battery System**

This option is not available for all UPS devices.

| Field | Description |
|---|---|
| **Battery System Status** | |
| **State of Charge** | The percentage of the UPS battery capacity that is available to support the attached equipment. |
| **Runtime Remaining** | How long the UPS can use battery power to support its present load. |
| **Positive Bus Voltage** | The UPS device supports both positive and negative battery voltages. |
| **Negative Bus Voltage:** | |
| **Replacement Battery Cartridge SKU** | The part number that you should quote for a replacement battery cartridge. |
| **Battery Pack Status** | |
| **Battery Pack 1, 2...** | The battery pack number as derived from the internal numbering method. |
| **Serial Number** | The serial number of the battery pack. |
| **Health** | This includes any pack battery system errors including the individual cartridge errors. Errors are logged as events. |
| **Status** | The status of the battery pack, including the statuses of the individual cartridges.<br>Other than OK, this value can signal the battery is near end of its life, or the battery lifetime is exceeded for the pack. Errors are logged as events. |

Click on Battery Pack 1,2...to reach the **Battery Pack n** screen page.

| Field | Description |
|---|---|
| **Battery Pack 1, 2...<br>or<br>Internal Pack** | |
| **Serial Number (if present)** | The serial number of the battery pack. |
| **Firmware Revision** | The battery pack revision number. |
| **Temperature** | Temperature as reported by the sensor in the battery compartment. |

| Field | Description |
|---|---|
| **Pack Status** | Errors for the battery pack only, not including the individual cartridge errors. Errors are logged as events and can be:<br>• temperature not in range<br>• general errors<br>• communication errors<br>• a disconnected pack frame<br>• firmware is incompatible with the hardware |
| **Battery Cartridge 1** and (if present) **Battery Cartridge 2** | |
| **Health** | This can be OK, battery near end of life, battery lifetime exceeded, or measured battery near end of life for the cartridge.<br>Errors are logged as events. |
| **Installation Date** | The date when individual cartridges were installed. You can edit this date. |
| **Predicted Replacement Date** | The UPS calculates when the battery should be replaced.<br>The **Health** field above is derived from this date. |
| **Status** | This is specific to the cartridge. See “Pack Status” above for general pack errors. Errors are logged as events and can be:<br>• disconnected cartridge<br>• cartridge needs replacement<br>• cartridge temperature is too high: critical<br>• cartridge temperature is too high: warning. This usually but not always displays before critical above. |

# Universal I/O on Status menu

**Path: Status > Universal I/O**

This option is not available for all UPS devices.

**Temperature & Humidity** displays the name, alarm status, temperature, and humidity (if supported) for each sensor. Click the name of a sensor to edit the name and location and to configure its thresholds and its hysteresis. See “Temperature and Humidity screen” for more details.

**Input Contacts** displays the name, alarm status, and state (open or closed) of each contact. These are automatically found and displayed here when you install the environmental accessory. Click the name of an input contact for detailed status or to configure its values. If contacts are configured and disabled, they do not display here. See “Input Contacts screen” for more details.

**Output Relay** displays the name and state (open or closed) of each relay. These are automatically found and displayed here when you install the environmental accessory. Click the name of an input contact for detailed status or to configure its values. See “Output Relay screen” for more details.

**Recent Environmental Events** displays events that are related to your environmental monitoring, for example a temperature threshold violation or a warning message about an environmental monitor input contact. Click the More Events link to see a full list of recent events.

# 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.

# Controlling UPS and Security

The Control menu options enable you to take immediate actions affecting your UPS and your outlets, and they also have some security and network functions. These options can apply to individual UPS devices and a Synchronized Control Group (SCG), if enabled, see “Synchronized Control of your UPS devices”.

This option is not available for all UPS devices.

See the following sections:

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

## UPS on Control menu

**Path: Control > UPS**

This option applies to individual UPS devices and, for Smart-UPS only, a Synchronized Control Group (SCG), see “Synchronized Control of your UPS devices”.

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.

The actions vary depending on whether you have a UPS device with Outlet Groups or not. The two tables below cover these separately.

- “Actions on the UPS screen for devices WITH Outlet Groups”.
- “Actions on the UPS screen for devices with NO Outlet Groups”.
  This has information on CLI options.

These screen check box options directly below apply to both tables.

| Check Box | Description |
|---|---|
| **Signal PowerChute Network Shutdown Clients** | This is greyed out if no PowerChute clients exist (see “PowerChute Network Shutdown clients”).<br>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 Network Shutdown Parameters** (see “Shutdown on Configuration menu”).<br>However, this option will not notify servers when performing any bypass control actions. |
| **Skip outlet off delays** | Turn off outlets immediately, skipping the configured outlet group delays.<br>You might want to do this in an emergency or to save runtime. Or the load devices might already have been turn off manually. |
| **Apply to Sync Group** | This only displays if synchronized control is enabled. See “Synchronized Control of your UPS devices”.<br>See individual descriptions of the fields in the two tables below. |

For more information about the delays and settings, see “Shutdown on Configuration menu”, “Synchronized Control of your UPS devices”, and “Outlet Groups on Control menu”.

**Actions on the UPS screen for devices WITH Outlet Groups**

| Action | Description |
|---|---|
| **Reboot UPS Outlet Groups** | Applies a Shutdown Immediately, AC Restart command to all outlet groups (see “Outlet Groups on Control menu”). Click Next to see specific details on timing and delays.<br>Turns off the output power of the Switched Outlet Groups and then, if present, the Main Outlet Group. Any outlet group to which the action is applied waits the number of seconds configured for its “Reboot Duration” and “Power On Delay”. (Then, the outlet groups turn on if AC utility power is available, or waits to turn on until AC utility power is available. See “What are Outlet Groups?”).<br>If the UPS is in a **Synchronized Control Group** (SCG), select Yes or No for Apply to Sync Group to choose whether to reboot all enabled members of the group. The UPS waits the number of seconds configured for its Shutdown Delay and Return Delay, then turns on if AC utility power is available, or waits to turn on until AC utility power is available. |
| **Turn On UPS Outlet Groups** | Turns on the Main Outlet Group, if present, and then all Switched Outlet Groups. This option displays only if the UPS is currently turned off. Click Next to see specific details timing and delays.<br>If the UPS is in a **Synchronized Control Group**, select Yes or No for Apply to Sync Group to choose whether to turn on all enabled members of the group. The UPS and outlet groups wait the time configured for “Return Delay”, then turn on. |
| **Turn Off UPS Outlet Groups** | Turns off the output power of the Switched Outlet Groups and then, if present, the Main Outlet Group. Any outlet group to which the action is applied remains off until you turn on its power again. Click Next to see specific details on timing and delays<br>If the UPS is in a **Synchronized Control Group**, select Yes or No for Apply to Sync Group to choose whether to turn off all enabled members of the group. |
| **Put UPS Outlet Groups to Sleep** | Puts the UPS outlet groups into sleep mode by turning off the output power of the UPS for a period of time defined by the following parameters. Click Next to see specific details on timing and delays<br>• The outlet groups wait the times configured as their “Power Off Delay” before turning off their power.<br>• When input power returns, the UPS turns on output power after two configured periods of time elapse: “Sleep Time” and “Power On Delay”.<br>If the UPS is in a **Synchronized Control Group**, select Yes or No for Apply to Sync Group to choose whether to put all enabled members of the group into sleep mode. The NMC of the UPS initiating the action waits up to the number of seconds configured as “Power Synchronized Delay” for enabled group members to regain input power before it starts the “Return Delay”. The UPS waits the number of seconds configured for its “Shutdown Delay”, then turns off. After the hours configured as “Sleep Time” elapse, the UPS waits the number of seconds configured for its “Return Delay”, then turns on if AC utility power is available, or waits to turn on until AC utility power is available. |

For more information about the delays and settings, see “Shutdown on Configuration menu”, “Synchronized Control of your UPS devices”, and “Outlet Groups on Control menu”.

**Actions on the UPS screen for devices with NO Outlet Groups**

| Action | Description |
|---|---|
| **Reboot UPS** (user interface)<br>`ups -c Reboot` (command line interface, CLI) | Restarts the attached equipment by doing the following. (Click Next to see specific details on timing and delays).<br>• Turns off power at the UPS after Shutdown Delay (on Configuration - Shutdown).<br>• Turns on power at the UPS after the UPS battery capacity returns to at least the percentage configured for Minimum Battery Capacity ((Configuration - Shutdown - End of Shutdown, see “Controlled Early Shutdown and End of Shutdown”). The UPS then waits the time specified as Return Delay (on Configuration - Shutdown).<br>For a **Synchronized Control Group** (SCG) action:<br>1. This option turns off power at the UPS devices that are enabled group members after waiting the time configured as “Shutdown Delay” for the initiating UPS devices.<br>The initiating UPS waits up to the number of seconds specified as “Power Synchronized Delay” to allow time for group members to regain input power. If all group members already regained input power, this delay is omitted. If all group members regain input power during the delay, the rest of the delay is cancelled.<br>2. “Return Delay” starts when the initiating UPS is at its configured Minimum Battery Capacity (Configuration - Shutdown - End of Shutdown, see “Controlled Early Shutdown and End of Shutdown”.<br>A Minimum Battery Capacity of the initiating UPS is also required of SCG members. However, you can reduce a group member’s requirement by configuring that member’s “Return Runtime Duration Offset”. For example, if the initiator’s Minimum Battery Capacity is 50%, and a member’s Minimum Battery Capacity Offset (Configuration - Synchronized Control) is 5%, that member needs battery capacity of 45% to reboot. |
| **Turn UPS On** (user interface)<br>`ups -c On` (CLI) | Turns on power at the UPS. The option only displays when the UPS is turned off. Click Next to see specific details on timing and delays.<br>For a **Synchronized Control Group**, after a delay of a few seconds, the action turns on all enabled group members that have input power. |
| **Turn Off UPS** (user interface)<br>`ups -c Off` (CLI) | Turns off the output power of the UPS immediately, without a shutdown delay. The UPS remains off until you turn it on again.<br>For a **Synchronized Control Group**, this action turns off power at all enabled members of the group. No “Shutdown Delay” value is used. The UPSs turn off after a few seconds and remain off until you turn on their power.<br>Note**:** For a synchronized turn-off action that uses the value of the “Shutdown Delay” of the initiating UPS, use SNMP (for the upsAdvControlUpsOff OID, set the value to turnUpsSyncGroupOffAfterDelay (5)). |
| `ups -c GraceOff` (CLI) | Turns off the outlet power of the UPS after the “Maximum Required Delay” and the configured “Shutdown Delay”. |
| **Put UPS to Sleep**<br>`ups -c GraceReboot` (CLI) | This action is similar to Reboot UPS above, but with an additional delay before the shutdown.<br>The attached equipment shuts down only after the UPS (or the initiating UPS, for a **Synchronized Control Group** action) waits the “Maximum Required Delay”, which is calculated as described in “Shutdown delays and forcing negotiations”.<br>Click Next to see specific details on timing and delays. |

**Actions on the UPS screen for devices with NO Outlet Groups**

| Action | Description |
|---|---|
| **Put UPS To Sleep** (user interface)<br>`ups -c Sleep` (CLI) | Puts the UPS into sleep mode by turning off its output power for a defined period of time. Click Next to see specific details on timing and delays.<br>• The UPS turns off output power after waiting the time configured as "Shutdown Delay".<br>• When input power returns, the UPS turns on output power after two configured periods of time: "Sleep Time" and "Return Delay".<br>• For a **Synchronized Control Group** (SCG) action, the NMC of the initiating UPS waits up to the number of seconds configured as "Power Synchronized Delay" for enabled group members to regain input power before it starts the "Return Delay". If all group members already regained input power, the "Power Synchronized Delay" is omitted. If all group members regain input power during the delay, the rest of the delay is cancelled. |
| `ups -c GraceSleep` (CLI) | Puts the UPS into sleep mode (turns off power for a defined period of time):<br>• The UPS turns off output power after waiting the "Maximum Required Delay" to allow time for PowerChute Network Shutdown to shut down its server with protection, and its "Shutdown Delay".<br>• When input power returns, the UPS turns on output power after two configured periods of time: its "Sleep Time" and "Return Delay".<br>• Re **Synchronized Control Group** (SCG), see final bullet in the row directly above. |
| **Put UPS In Bypass** and **Take UPS Off Bypass** (user interface)<br>`ups -b Enter`<br>`ups -b Exit` (CLI) | These actions are supported:<br>• Only for individual UPS devices, NOT for **Synchronized Control Groups**<br>• Only for Symmetra UPS and some Smart-UPS devices<br>They control the use of bypass mode, which allows maintenance to be performed at a Symmetra UPS and some Smart-UPS devices without turning off power at the UPS.<br>Click Next to see specific details on timing and delays. |

# Outlet Groups on Control menu

**Path: Control > Outlet Groups**

This option is not available for all UPS devices.

Use this option to turn on, turn off, or restart individual outlet groups as distinct from the UPS device. This option can apply to individual UPS devices and a Synchronized Control Group (if enabled, see "Synchronized Control of your UPS devices").

(This screen lists by name and state each UPS outlet group that has been configured through the **Configuration - Outlet Groups** option, see "Outlet Groups on Configuration menu").

You can select any of the following actions (or no action) for each outlet group. These are one-time actions.

- When the state of the outlet group is **off**:
  - **On Immediately**
  - **On with Delay**: Turn on the outlet group after the number of seconds configured as **Power On Delay**. (see "Shutdown on Configuration menu").

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

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

# 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.<br>The UPS and NMC devices are not rebooted. |
| **Reset All**[1] | Caution:This resets all configured values in the management interface you are using, e.g. the Web user interface.<br>Clear the **Exclude TCP/IP** check box to reset ALL configuration values to their defaults.<br>Select the **Exclude TCP/IP** check box to reset all values except how this device obtains its TCP/IP configuration values (default is DHCP). |
| **Reset Only**[1] | **TCP/IP**: Reset how this device obtains its TCP/IP configuration values to the default DHCP. |
| | **Event Configuration**: Reset all changes to event configuration, by event and by group, to their default settings. See “Notification menu” |
| | **UPS to Defaults**: Reset only UPS settings, not network settings, to their defaults. |
| | This option is only available when you have an environmental monitor connected.<br>**Lost Environmental Communication Alarms**: Clear any environmental alarms that are caused by lost communication with an external sensor. For example, if a temperature sensor is disconnected and causes an alarm, resetting lost environmental alarms returns the alarm status for that sensor to Normal.<br>Note: To clear alarms for a sensor that is connected to the universal sensor port of an AP9631 NMC, reconnect the sensor or restart the NMC. |
| | **Control Policy**: Reset the settings that define how the NMC will respond to alarms that are detected at the Dry Contact I/O Accessory. |

[1]Resetting may take up to a minute. The UPS name you configured will not be reset (see “UPS General screen”).

# Configuring your Settings: 1

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”.

- “Outlet Groups on Configuration menu”
- “Power Settings on Configuration menu”
- “Shutdown on Configuration menu”
- “UPS General screen”
- “Self-Test Schedule screen”
- “Shutdown Scheduling”
- “Firmware Update screen”
- “PowerChute Network Shutdown clients”
- “Synchronized Control of your UPS devices”
- “Third Party Support screen”
- “Universal I/O screens”
- “Security menu”

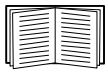
# Outlet Groups on Configuration menu

**Path: Configuration > Outlet Groups**

This option is not available with all UPS devices. With it, you can display and configure your outlet and sequencing delays.

See also “Outlet Groups on Status menu”, “Outlet Groups on Control menu”, and “Shutdown on Configuration menu”.

## What are Outlet Groups?



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

The available settings differ based on the UPS device.

**Main Outlet Groups .** Some UPS devices provide AC utility power to one Main Outlet Group. The Main Outlet Group controls the distribution of power to all Switched Outlet Groups (if present) for the UPS.

- If the Main Outlet Group is off, the Switched Outlet Groups cannot be turned on.
- If you turn off the Main Outlet Group, the UPS turns off the Switched Outlet Groups before it turns off the Main Outlet Group.
- To turn on a Switched Outlet Group, the UPS must turn on the Main Outlet Group first.

**Switched Outlet Groups .** Each Switched Outlet can perform actions independently. You can start or stop these outlets in sequence and also restart devices plugged into these outlets.

The way outlet groups turn on and off depends on their configuration and how you turn the UPS on or off:

- Before you configure the delays for actions when you turn on the UPS output (described in “UPS on Control menu” and “Sequencing settings”), any outlet group that is off turns on by default. When an outlet turns on, it applies power to all devices attached.
- After you configure the actions and delays, they control when outlet groups turn on and off after you turn the UPS on or off. (This is the case whether you turn off using the web UI of the NMC or the display interface at the UPS).

## Configuring your Outlet Groups

**Outlet group name and type.** View the name, type, and delays of your UPS outlets on the **Configuration** - **Outlet Groups** screen. Click the name of an outlet group under **Group** to change its settings including sequencing delays and load shedding options.

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

| Field | Description |
|---|---|
| **Power Off Delay** | When this outlet group is on, it waits this delay in seconds before turning off. By setting different times here for outlets, you can sequence their turn-offs, that is, you can specify the order in which they turn off. |
| **Reboot Duration** | The outlet waits this amount of time before rebooting. |
| **Power On Delay** | When this outlet group is off and receives a signal to turn on, it waits this delay in seconds before turning on. By setting different times here for outlets, you can sequence their turn-ons. |
| **Min Return Runtime** | The minimum amount of time the UPS must be able to support the load before it can turn on again. |

**Load-shedding options.** Load shedding enables you to specify conditions that cause individual Switched Outlet Groups to lose power. It is not available for Main Outlet Groups.

An example of using load shedding would be for turning off non-critical loads like monitors when the UPS is running on battery or is overloaded. This would preserve the battery charge and the runtime for essential loads. Another example would be to disable an automatic restart after an overload in order to investigate the cause of the overload before turning the outlet group back on.

The options enable you to shut down an outlet group 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).
- The UPS is overloaded (the power demand of the devices connected to the UPS exceeds the amount of power the UPS can provide).

You can also enable these actions:

- **Skip outlet off delay**. (Turn the outlet group off immediately, without waiting the number of seconds configured as **Power Off Delay**. By default, this option is disabled.)
- **Stay off after power returns**. (Remain off when AC utility power returns. By default, this option is disabled, and the UPS waits the number of seconds configured as **Power On Delay**, then turns on the outlet groups.)

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

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

UPS: Outlet Group 3, Printer, turned off.
```

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

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

# Power Settings on Configuration menu

**Path: Configuration > Power Settings**

The available settings differ based on the UPS device.

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

- Upper and Lower **Voltage** settings determine the ranges at which the UPS automatically regulates battery output to the load. This protects the load.

  When the upper voltage is breached, the UPS uses its AVR Trim feature; when the lower voltage is breached, the UPS uses its AVR Boost feature (or it switches to battery operation if the UPS does not have AVR Boost).

- Enabling **Green Mode** runs the UPS in bypass, which uses energy more efficiently. However, in green mode the speed of transferring to the UPS battery power when necessary is slower. If your environment needs a fast switching time, you can disable green mode.
- Electrical noise is unwanted electromagnetic energy which lowers the quality of signals and data. When there is too much noise, your UPS intervenes by supplying battery power. You can specify the response to noise through **Sensitivity**. Use the **Reduced** and **Low** options in the Sensitivity drop-down box when there is a lot of noise.
- **Output Watt Rating**: the maximum power rating to meet the requirements of your load devices
- **Bypass** settings define conditions under which the UPS can switch to bypass mode
- **Alarm thresholds** are based on available runtime and redundant power and on UPS load

# Shutdown on Configuration menu

**Path: Configuration > Shutdown**

Use this option to configure your shutdowns by specifying durations on battery, delays before shutting down and restarting, minimum runtime and charge required before restarting, etc. These Shutdown options help to ensure shutdowns with protection.

See the table below and also "Controlled Early Shutdown and End of Shutdown".

For outlet groups, this screen works in conjunction with “Outlet Groups on Configuration menu”.

| Field | Description |
|---|---|
| **Low Battery Duration** | When the UPS goes on battery, it waits this time before turning off. See “Shutdown delays and forcing negotiations”. |
| **Maximum Required Delay** | In a shutdown, the UPS waits this time before shutting down. See “Shutdown delays and forcing negotiations”. |
| **Basic Signaling Shutdown** | Basic signaling provides system shutdown with protection and notification, but does not provide the continuous advanced monitoring features available with advanced or smart signaling.<br>Enable it if your UPS has a basic-signaling cable, does not support advanced signaling, or is configured to communicate in basic signaling. |
| **Basic Low Battery Duration** | Defines the amount of available battery runtime at which the UPS signals a low-battery condition. |
| **Sleep Time** | Defines how long the UPS keeps its output power turned off when you use the sleep fields of the “UPS on Control menu”. |
| **Synchronized Control fields**<br>(see “Synchronized Control of your UPS devices”) | |
| **Shutdown Delay** | Defines how long the UPS waits before it shuts down in response to a sync control turn-off command. |
| **Return Delay** | Defines how long the UPS waits before it turns on after a shutdown initiated by a synchronized control command.<br>If the battery is depleted below the capacity to provide the runtime configured as “Min Return Runtime”, the UPS first waits until the battery is recharged to provide that runtime. |
| **PowerChute Network Shutdown** | |
| **Maximum Required Delay** | Calculates the delay needed to ensure that each PowerChute client has enough time to shut down with protection. It is the longest shutdown delay needed by any server listed as one of the “PowerChute Network Shutdown clients”. See “Shutdown delays and forcing negotiations”. |
| **On-Battery Shutdown Behavior** | After the PowerChute clients shut down their computer systems, this parameter determines whether the UPS turns on automatically or manually when input power is restored. |
| **Authentication Phrase** | Sets the case-sensitive phrase of 15 to 32 ASCII characters to be used during MD5 (decryption) authentication for PowerChute communication. The default setting is “admin user phrase” for Administrator. |

**Controlled Early Shutdown and End of Shutdown.** These options are NOT available with 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:

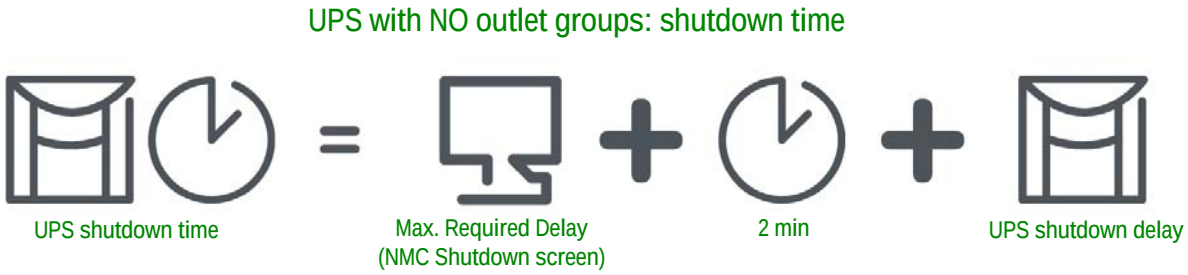
- When the time on battery exceeds a set number of minutes.
- When the runtime remaining of the UPS is less than a set number of minutes. (Runtime is how long the UPS can use battery power to support its present load).
- When the battery charge is less than a set percentage of its total capacity.
- When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

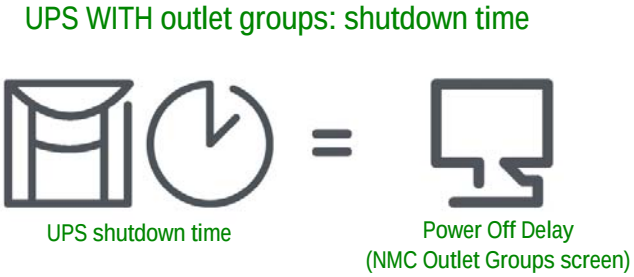
The **End of Shutdown** options enable you to set a condition and a delay time for when a UPS can turn back on after AC utility power is restored. You can specify a **Minimum Battery Capacity** before the UPS will turn back on. Set another pause, if necessary, before turning on with **Return Delay**.

**Shutdown delays and forcing negotiations.** A shutdown time for the UPS is calculated differently for a UPS device *with NO* outlet groups compared to a UPS *with* outlet groups.

1. For a UPS with NO outlet groups, the shutdown time is the **Maximum Required Delay** value on the NMC **Shutdown** screen *plus* 2 minutes *plus* the shutdown delay for the UPS.




2. For a UPS WITH outlet groups, the shutdown time is the **Power Off Delay** value on the NMC **Outlet Groups** screen, see "Outlet Groups on Configuration menu". (Not available with all UPS devices).



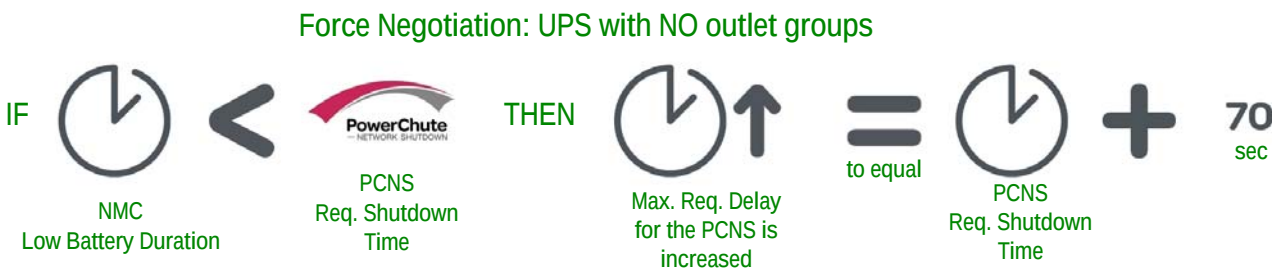

   Note that devices with the prefix SUM behave like #1 above, not #2.

For both types of UPS, the shutdown time is negotiated by the NMC interacting with PowerChute Network Shutdown (PCNS).

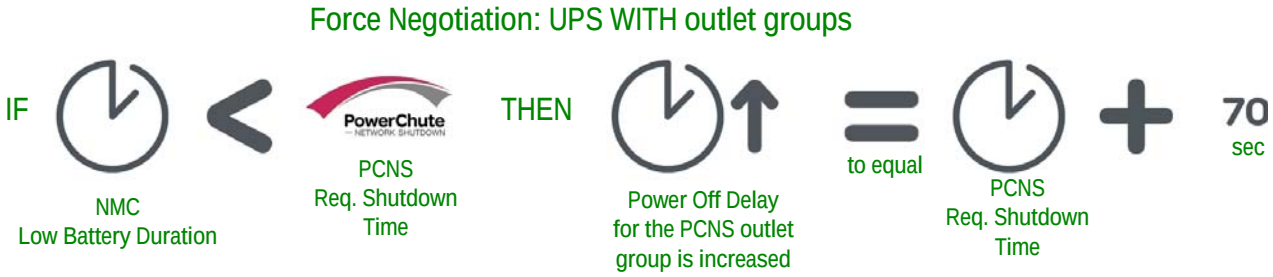
Use the **Force Negotiation** option (**Configuration - Shutdown**) to re-gauge the time when you change or add a PCNS client. When you force a negotiation, the procedure is automatic; the details are discussed below.

PCNS starts with the NMC **Low Battery Duration** value, compares it to its own shutdown time and, if the battery duration time is too low, tells the NMC to increase the values in #1 and #2 below to the PCNS SHUTDOWN REQUIRED TIME* *plus* 70 sec.

1. With NO outlet groups, the **Maximum Required Delay**.



2. With outlet groups, the **Power Off Delay** for the outlet group supplying power to the PCNS client.




*The PCNS SHUTDOWN REQUIRED TIME = the shutdown delay + the shutdown command duration. When the default of 70 seconds is added, the time is always rounded up to nearest minute. E.g., a total here of 3 min 50 sec is rounded up to 4 min; a total of 2 min is still rounded up to 3 min.

**Notes**:

The 70 sec. mentioned is the default OS shutdown time for PCNS.

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

With PCNS v3.x, the **Maximum Required Delay** value is never used by the NMC for a UPS with outlet groups.

# UPS General screen

**Path: Configuration > UPS General**

This screen is not available for all UPS devices.

Some of the options explained below might NOT display for some UPS devices.

| Field | Description |
|---|---|
| **UPS Name** | A name to identify the UPS. |
| **UPS Position** | The physical orientation of the UPS, rack or tower. |
| **Audible Alarm** | Enable or disable the audible alarm of the UPS, and, for some UPS devices, define the condition that will cause the alarm to sound. |
| **LCD Language Preference** | Specify which language you want to use for your UPS display. |
| **Display** | Disable or enable write-access to the UPS display interface.<br>When disabled, the user still has read-access to most screens, but not to sub-screens on the Control and Configuration menus. |
| **Last Battery Replacement** | Enter the month and year of the most recent UPS battery replacement. |
| **Number of Batteries**<br>or<br>**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. |
| **External Battery Cabinet** | The battery cabinet Amp-Hour rating of an external battery source. |

| Field | Description |
|---|---|
| **Battery Charger Rate** | With this field, you can change the UPS charge rate, in percentage terms. Here, 100% represents the manufacturer's recommended rate.<br>For example, to double the charge rate set this to 200%.<br>The rate includes both internal and external batteries. This number does not change when external packs are added or removed. However, removing an external battery pack effectively increases the charging rate. Similarly, adding an external battery pack decreases the charging rate.<br>Caution:Charging at too high a rate can result in boiling and/or venting of electrolytes and/or high gas pressure. Do not change this setting unless you have strong background knowledge in this area. |
| **Battery Type** | Indicate the battery type where **VRLA** is Valve Regulated Lead Acid and **Vented Cell** is a wet cell type battery (as used in cars). |

# Self-Test Schedule screen

**Path: UPS > Configuration > Self-Test Schedule**

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

# Shutdown Scheduling

**Path: Configuration > Scheduling**

This option is not available for all UPS devices.

## For both the UPS and outlet group options

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

Any configured shutdown schedules display along the top of the screen when you select **UPS** or **outlet groups**, 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** or **outlet groups** 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 or a Switched Outlet Group shutdown schedule.**

1. Under **Scheduling**, select either **UPS** or **outlet group.**
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** button.
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 or outlet group 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 and the time specified as the **Return Delay**, see “Return Delay”).

For an outlet group only, specify the group to shut down by selecting the appropriate button.

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

### For the UPS option only: synchronized shutdowns

**Schedule a synchronized shutdown.** When the UPS which initiates the shutdown is an enabled member of a Synchronized Control Group (SCG), then all members of the SCG shut down.

Always schedule the shutdowns through the same member of the SCG. Each UPS in the SCG must have a network connection at the time of the shutdown. See “Synchronized Control of your UPS devices”.

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

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.

## Firmware Update screen

**Path: UPS > Configuration > Firmware Update**

This option is not available for all UPS devices.

The update here refers to *the firmware on the UPS*. Don’t confuse this with an NMC firmware upgrade (see “File Transfers”).

You must turn off your UPS output before performing a firmware update.

Follow these steps to update the firmware. (See “Using FTP to update the UPS firmware” for an alternative way).

1. See the Knowledge Base article IDs FA164737 and FA170679 on the APC website for information on obtaining a firmware update file and further instructions.
2. Choose **Configuration** - **Firmware Update**.
3. Click on the button to locate the downloaded update file on your computer.
4. Click the **Update UPS** button to update the UPS firmware.
5. When the update finishes, check the status under **Last Update Result** or in the Event Log.

## Using FTP to update the UPS firmware

If you have updates to make on many UPS devices, it can be quicker to use FTP. The steps below show an example of how to do this. This is an **alternative** to updating from the “Firmware Update screen”.

1. See the Knowledge Base article IDs FA164737 and FA170679 on the APC website for information on obtaining a firmware update file and further instructions.
2. FTP the update file onto the card’s **upsfw** directory to start the firmware update process.

   The FTP firmware transfer might be aborted if the update file is corrupted or not applicable to the UPS.,

   Here's an example of loading an update file using the DOS FTP command:

   ```
   $ ftp <NMC Network Address Here>
   Connected to <NMC Network Address>.
   220 AP9631 Network Management Card AOS vX.Y.Z FTP server ready.
   User (<NMC Network Address>:(none)): apc
   331 User name okay, need password.
   Password:
   230 User logged in, proceed.
   ftp> cd upsfw
   250 CWD requested file action okay, completed.
   ftp> put “<Path to UPS Firmware File>”
   200 PORT Command okay.
   150 File status okay; about to open data connection.
   226 Closing data connection.
   ftp: 121984 bytes sent in 1.39Seconds 87.70Kbytes/sec.
   ftp> quit
   221 Goodbye.
   ```

3. When the update finishes, check the status under **Last Update Result** on the firmware update page of the web interface or in the Event Log.

# PowerChute Network Shutdown clients

**Path: UPS > Configuration > 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.

# Synchronized Control of your UPS devices

**Path: UPS > Configuration > Sync Control**

This option is not available for all UPS devices.

**What is a Synchronized Control Group (SCG)?** With an SCG you can apply actions simultaneously to each UPS in the group. If you apply an action to an SCG, enabled members of the group behave as follows:

- Each UPS receives the command regardless of its output status (e.g., even if on a low battery).
- The action uses the delay periods (such as **Shutdown Delay** and **Return Delay**) configured *for the initiating UPS*. (See “Shutdown on Configuration menu”).
- When the action begins, a UPS that is unable to participate retains its present output status while the other UPS devices perform the action. So, if a UPS is already in an output state that the action requires (e.g., a UPS is already off when the Reboot UPS action starts), that UPS logs an event, and performs the rest of the action, if any.
- All participating UPS devices synchronize their performance of the action (within a one-second time period under ideal conditions for Smart-UPS), but sometimes longer.
- In reboot and sleep actions:
  - Immediately before the initiating UPS begins waiting the time specified as **Return Delay**, by default it waits up to 120 seconds (its configurable **Power Synchronized Delay**) for any UPS that does not have input power to regain that power.

    Any UPS that does not regain input power during that delay does not participate in the synchronized restart, but waits until its own input power returns before restarting.
  - The LEDs on the front of the UPS do not sequence their lights as they do for a normal (not synchronized) reboot or sleep action.
- UPS status and events are reported in the same way for synchronized actions as for actions on individual UPS devices.

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

- All UPS devices in an SCG must be the same device.
- SCGs are supported for any Smart-UPS with a card slot that accepts a Network Management Card.
- When its membership in an SCG is enabled, the NMC blocks UPS communications from a connected management device on the serial communications port. However, the NMC still allows access to the command line interface on the serial communications port.
- See also the Knowledge Base articles FA156114 and 11135, on the support website www.apc.com.

**Display status of a Synchronized Control Group member.** When SCG is enabled, the following additional information is displayed about the SCG membership of this group member: its **IP address**, its **Input Status** (**Good** is acceptable; **Bad** is not acceptable); and its **Output Status** (**On** or **Off**).

| Field | Description |
|---|---|
| **Group Membership** | When you enable or disable Synchronized Control Group (SCG) membership, the change causes the management interface to reboot the next time you log out, and is implemented at that time.<br>The Sync Control option uses SNMPv3 for group communication. When you enable group membership, SNMPv3 is enabled automatically. |
| **Control Group Number** | The unique identifier of the SCG. This value must be a number from 1 through 65534. A UPS can be a member of only one SCG. All members of an SCG must have the same Control Group Number. |
| **Multicast IP Address** | Specify the IP address used to communicate among members of an SCG. The allowed range is 224.0.0.3 to 224.0.0.254. All members must have the same Multicast IP Address. |
| **Power Synchronized Delay** | When the initiating UPS of the SCG is ready to turn on, this value is the maximum time that the initiating UPS will wait, if necessary, for other group members to regain input power. (The value is 120 seconds by default).<br>When this delay expires, the initiating UPS will wait to recharge its battery to the runtime specified as **Return Runtime Duration Offset** (below), if necessary, then wait the time specified as “Return Delay”, and then turn on. |
| **Return Runtime Duration Offset** | Specify a number of seconds of runtime that will be subtracted from the “Min Return Runtime” of the initiating UPS. This will determine the available runtime required for this particular group member to turn on.<br>You can configure this value differently for each member of the SCG. |
| **Authentication Phrase** | The case-sensitive phrase (15 to 32 ASCII characters) used to authenticate members of an SCG. All members of an SCG must have the same authentication phrase.<br>The default is “APC ASI auth phrase”. |
| **Encryption Phrase** | The encryption key for the protocol that ensures secure communication among members of an SCG. All members of an SCG must have the same encryption phrase.<br>The default is “APC ASI crypt phrase”. |
| **Synchronized Control Port** | The network port that SCGs use to communicate. You can use any non-standard port from 5000 to 32768. |

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

This option only displays with Smart-UPS VT devices when you have set up a parallel configuration. It lists all parallel units (UPS devices that share a load, continuing to provide power to the load if a parallel unit is not operating). The UPS to which you are logged on is listed first. Use **Add Unit** to add a parallel UPS, and specify its name and IP address.

# Third Party Support screen

**Path: Configuration > Third Party Support > EnergyWise**

Cisco® EnergyWise™ enables the measurement and management of the power consumption of network devices. It can be used to reduce the consumption, and associated costs, of your UPS and its attached devices.

The **EnergyWise** screen on this NMC user interface facilitates the use of a Cisco EnergyWise switch to monitor and control your UPS and its devices. This includes turning off the UPS and individual Switched Outlets (if your UPS has them).

The EnergyWise functionality in the NMC can ONLY be used in conjunction with a Cisco EnergyWise switch. Use this NMC EnergyWise screen to configure the communications between the devices (including the UPS) and the Cisco EnergyWise switch.

Any reporting, analysis, and controlling (like turning off an outlet) is done using the Cisco switch.

Select EnergyWise from the NMC Configuration menu option. Use the initial **EnergyWise Configuration** screen to set the communication parameters with the Cisco switch. The domain name and shared secret password (if used) must be the same as those used on the switch.

| Field | Description |
|---|---|
| **Version** | The current toolkit version of EnergyWise on the NMC.<br>This must be the same as the version on your Cisco EnergyWise switch. |
| **EnergyWise** | This option is disabled by default. Select it to enable EnergyWise communication. |
| **Port** | Specify the network port which the NMC will use to communicate with EnergyWise (43440 by default). The range is 0–65535. |
| **Domain Name** | Specify the name of the domain shared between the NMC and the Cisco EnergyWise switch. |
| **Secure Mode** | Select this check box to enable secure mode for communication between the NMC and the switch. This is optional. |
| **Shared Secret** | If you select the Secure Mode check box, you must then enter the secret shared password used between your devices and the switch. |

When you have set the parameters, click Apply and the Cisco switch polls the domain and finds your UPS and any attached devices, including those attached using Switched Outlet Groups.

The lower half of this screen shows your devices and categorizes them under **Parent** and **Child** (if relevant).

The Parent is always your UPS. If you have devices attached to Switched Outlet Groups, they display under the Child Configuration heading.

The associated fields, **Name**, **Role**, **Keywords**, and **Importance** can be edited by clicking on the Name link or you can accept the defaults. It is mandatory to have values in Name and Importance.

The values in **Role**, **Keywords**, **Importance**, must use standard specification values from Cisco EnergyWise. They enable the querying of the state of your devices.

| Field | Description |
|---|---|
| **Name** | The Name used to identify the parent and associated children of the UPS. |
| **Role** | This is a search category available to the Cisco switch.<br>The role defines the device's job or function within the network.<br>The parent role default value is "Uninterruptible Power Supply". The child role's default value is "Outlet Group", if supported. |
| **Keywords** | This is a search category available to the Cisco switch.<br>Keywords are a way of grouping the parent and associated children devices. This enables the filtering of search results and reporting.<br>The default value of a parent is "apc,ups,smartups". The default of each child is "apc,ups,smartups,outlet". |
| **Importance** | Use the Importance field to rate or prioritize a device.<br>The value can be an integer number from 1 to 100 where 1 is the least important and 100 is the most important. The default value of both the parent and each child is 1. |

# Universal I/O screens

The **Universal I/O** menu is relevant when you have installed the temperature and humidity sensors (AP9335T/ TH) or the Dry Contact I/O Accessory (AP9810). Using these is often referred to as environmental monitoring.

## Temperature and Humidity screen

**Path: Universal I/O > Temp & Humidity**

This displays the name, alarm status, temperature, and humidity (if supported) for each sensor. Click the name of a sensor to edit the name and location and to configure its thresholds and its hysteresis.

**Thresholds.** For each sensor, you set the thresholds for temperature and (if supported) humidity measured at the sensor. When a threshold is breached, the alarm signals.

**High** and **Low** are warning messages. **Maximum** and **Minimum** are critical, they must be dealt with.

**Hysteresis.** Use the Hysteresis value to avoid getting alarms repeatedly for the same violation of the temperature or humidity threshold.

When the temperature or humidity that causes a violation tends to waver slightly up and down, it can repeatedly trigger the alarm. A greater hysteresis value can prevent this.

If the hysteresis value is not great enough, the wavering can first cause a threshold violation and then clear it, meaning the alarm can be triggered several times. See the examples below, after noting the following.

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

Example of rising but wavering humidity: Say the *maximum* humidity threshold is 65%, and the humidity hysteresis is 10%. Then, the humidity rises above 65%, causing an alarm. It then wavers down to 60% and up to 70% repeatedly, but — because of the 10% hysteresis value — the alarm is not cleared and therefore no new alarm occurs. For the existing alarm to clear, the humidity would have to drop below 55% (which is 65% *minus* 10%).

Example of falling but wavering temperature: Say the *minimum* temperature threshold is 12°C, and the temperature hysteresis is 2°C. Then the temperature drops below 12°C, causing an alarm. It then wavers back up to 13°C and then down to 11°C repeatedly, but — because of the 2°C hysteresis value — the alarm is not cleared and therefore no new alarm occurs. For the existing alarm to clear, the temperature would have to rise above 14°C (which is 12°C *plus* 2°C).

## Input Contacts screen

**Path: Universal I/O > Input Contacts**

**Input Contacts** displays the name, alarm status, and state (open or closed) of each contact. These are automatically found and displayed here when you install the environmental accessory.

Click the name of an input contact for detailed status or to configure its values. When disabled, the contact generates no alarm even when it is in the abnormal position. Other fields are discussed below:

| Field | Description |
|---|---|
| **Alarm Status** | **Normal** if this input contact is not reporting an alarm, or the severity of the alarm if this input contact is reporting an alarm. If not enabled for a contact, it displays **Disabled**. |
| **State** | The present state of this input contact: **Closed** or **Open**. |
| **Normal State** | The normal (non-alarm) state of this input contact: **Closed** or **Open**. |
| **Severity** | The severity of the alarm that the abnormal state of this input contact generates: **Warning** or **Critical**. |

## Output Relay screen

**Path: Universal I/O > Output Relay**

**Output Relay** displays the name and state (open or closed) of each relay. These are automatically found and displayed here when you install the environmental accessory.

Click the name of an input contact for detailed status or to configure its values. The fields are discussed below:

| Field | Description |
|---|---|
| **State** | The current state of this output relay: **Closed** or **Open**. |
| **Normal State** | The normal (non-alarm) state of this output relay: **Closed** or **Open**. |
| **Control** | To change the current state of this output relay, select this check box and click Apply. |
| **Delay** | The number of seconds a selected alarm condition must exist before the output relay is activated. Use this setting to avoid activating an alarm for brief transient conditions.<br>If additional mapped alarms occur after the delay begins, the delay does not restart but continues counting down until the output relay is activated. |
| **Hold** | The minimum number of seconds the output relay remains activated after the alarm occurs.<br>Even if the activating alarm condition is corrected, the output relay remains activated until this time period expires. |

## Configuring the Control Policy

**Path: Universal I/O > Control Policy**

On an AP9631 NMC with up to two connected Dry Contact I/O Accessories (AP9810), you can:

- configure output relays to open or close based on UPS events and input contacts, see “Configuring an output to respond to an event”
- configure the UPS to take action based on input contacts, see “Configuring the UPS or output to respond to an input alarm”

Not all UPS devices can be configured to respond to input contacts.

**Configuring an output to respond to an event.**

1. From the **Configuration** menu, select **Universal I/O** and **Control Policy**.
2. Click the **Add Policy** button.
3. Click a category or sub-category name to view corresponding events.
4. To configure, click an event name, select the output relay check box that will change state when this event occurs, and click **Save Policy**.

**Configuring the UPS or output to respond to an input alarm.**

1. From the **Configuration** menu, select **Universal I/O** and **Control Policy**.
2. Click the **Add Policy** button.
3. Click the **I/O Contact** sub-category.
4. Choose the event with the same severity as the input contact. For example, if the severity of the input contact is critical, then choose the critical event.

   The NMC supports up to four inputs. You must specify the input that will be associated with this event.
5. In the **Port** drop-down list, select the Universal Sensor **Port** number (1 or 2) to which the Dry Contact I/O Accessory is installed.
6. In the **Zone** drop-down list, select the zone letter (A or B) of the contact to which the input is installed.
7. Define the action the UPS will perform (if any) when the input changes state.
8. Select the output that will open or close (if any).
9. Click **Save Policy**.

The action you configure occurs once.

If you restore the output to its normal state before the alarm condition clears, the output will not open or close again unless the alarm condition clears and then reoccurs.

# 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.

**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 2 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.

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. |

**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”.

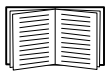
**Path: Configuration > Security > Local Users > Default Settings**

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*, available on the *Utility* CD and on the www.apc.com 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.

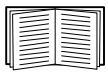
Select one of the following:

- **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”.

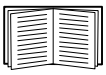
## RADIUS screen

**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).<br>Note: RADIUS servers use port 1812 to authenticate users, this can't be changed. |
| **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. |

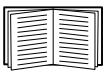


See also "Remote Users authentication" above and "Configuring the RADIUS Server" below.

## Configuring the RADIUS Server

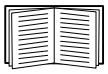
### Summary of the configuration procedure.

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*, available on the *Utility* CD and on the www.apc.com 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.
3. 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 and Microsoft IAS 2003 are supported. Other commonly available RADIUS applications might work but have not been fully tested.

## Firewall screen

**Path: Configuration > Security > Firewall**

| Menu option | Description of use |
|---|---|
| **Configuration** | Enable or disable the overall firewall functionality. Any configured policy is also listed, even if the firewall is disabled. |
| **Active Policy** | Select an active policy from the available firewall policies. The validity of policy is also listed here. |
| **Active Rules** | When a Firewall is enabled (see Configuration above in this table), this lists the individual rules that are being enforced by a current active policy. You can edit existing rules and add or delete new rules here. |
| **Create/Edit Policy** | Create a new policy or edit an existing one. |
| **Load Policy** | Load a policy file (with a .fwl suffix) from a source external to this device. |
| **Test** | Temporarily enforce the rules of a chosen policy, for a time that you specify. |

# 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”.

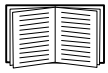
- “Network on Configuration menu”
- “Notification menu”
- “General menu”
- “Logs on Configuration menu”

# 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 UPS Network Management Card 2 (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:<br>• If it receives a valid response, it starts the network services.<br>• 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.<br>• 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:<br>• 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.<br>• 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.<br>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 UPS Network Management Card 2 (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.<br>When a router advertisement is received, the NMC checks whether the M and O flags are set. The NMC interprets them as follows:<br>• **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.<br>• **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".<br>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.<br>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.<br>• **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 ID FA156110 at http://www.apc.com/site/support/index.cfm/faq/index.cfm.

**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 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.

## 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).

## 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.
- **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 log off from the NMC user interface).

You can enable access to this UI through either **HTTP** or **HTTPS** or through both, by using the Enable check boxes. 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 NMC *Utility* CD 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 Network Management Card *Utility* CD 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 > SSL Host Key**

**Console access.** You need to enable console access in order to update your UPS firmware, see "Firmware Update screen". 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 does not encrypt user names, passwords, and data during transmission whereas SSH 2 does.

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 Network Management Card *Utility* CD. 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. Clients are available from various vendors.

## 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 **StruxureWare Central** to manage a UPS on the public network of an StruxureWare system, you *must* have SNMP v1 or SNMP v3 enabled in the NMC interface. Read access will allow the StruxureWare device to receive traps from the NMC, but Write access is required while you use the NMC user interface to set the StruxureWare device as a trap receiver.

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

**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.

**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 an NMS must use to access the community. The maximum length is 15 ASCII characters, and the default names are `public`, `private`, `public2`, and `private2`.

**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.

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 (`apc auth passphrase`, by default) 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 (`apc crypt passphrase`, by default) 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.

## 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.<br>For encrypted file transfer, use Secure CoPy (SCP). SCP is automatically enabled when you enable SSH, but you must disable the FTP Server here to enforce high-security file transfer.<br>**Note**: At any time that you want a device to be accessible for management by InfraStruXure Central or Manager, FTP Server must be enabled in the Network Management Card interface of that UPS.<br>For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available on the Utility CD or from the APC Web site. |
| **Port** | The TCP/IP port of the FTP server (21 by default).<br>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.<br>**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. |

# Notification menu

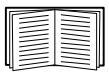
See these sections:

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

## 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
  - Remote Monitoring Service
  - Syslog notification
- Indirect notification
  - Event log. If no direct notification is configured, users must check the log to determine which events have occurred

    You can also log system performance data to use for device monitoring. See “Data log” 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:

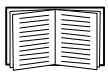
1. Select the **Configuration** menu, then **Notification**, **Event Actions**, and **By Event**.

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 “E-mail notification parameters”.

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 “E-mail notification parameters” directly below.

**E-mail notification parameters.** These configuration fields define e-mail 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 |
|---|---|
| **Delay *n* time before sending** | If the event persists for the specified time, the notification is sent. If the condition clears before the time expires, no notification is sent. |

| Field | Description |
|---|---|
| **Repeat at an interval of *n*** | The notification is sent repeatedly at the specified interval (the default is every 2 minutes until the condition clears). |
| **Up to *n* times** | During an active event, the notification repeats for this number of times. |
| or | |
| **Until condition clears** | The notification is sent repeatedly until the condition clears or is resolved. |

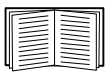
For events that have an associated clearing event, you can also set these parameters. (An example of an event with its clearing event is `UPS: Lost communication with the battery packs` and `UPS: Restored communication with the battery packs`).

## 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:<br>• In the format *user@* [*IP_address*] (if an IP address is specified as **Local SMTP Server**)<br>• In the format *user@domain* (if DNS is configured and the DNS name is specified as **Local SMTP Server**) in the e-mail messages.<br>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.<br>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 port number, with a default of 25. The range is 1–65535. |
| **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. |

| Field | Description |
|---|---|
| **Advanced** | |
| **Use SSL/TLS** | • **Never**: The SMTP server does not require nor support encryption.<br>• **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.<br>• **Always**: The SMTP server requires the STARTTLS command to be sent on connection to it.<br>• **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.<br>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.<br>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 “Adding and Changing Language Packs”. |
| **Server** | Select one of the following methods for routing e-mail:<br>• **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.<br>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.<br>• **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.<br>• **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. |
| **Powernet MIB Trap Generation/ RFC1628 "** | Choose between these two MIB trap generation types for each trap created.<br>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.<br>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. |

| Field | Description |
|---|---|
| **SNMPv1** | Community Name: The name (“public” by default) used as an identifier when SNMPv1 traps are sent to this trap receiver.<br>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:

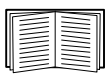
- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver itself is enabled.
- If a host name is selected for the **To** address, that host name can be mapped to a valid IP address.

**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.

## Remote Monitoring Service

**Path: Configuration > Notification > Remote Monitoring**

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



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

**Registration.** Once you have purchased the service, you activate RMS for the NMC. Select **Enable APC Remote Monitoring Service**, choose between **Register Company and Device** and **Register Device Only**, complete the form, and click the Apply button.

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

# General menu

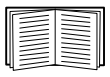
This menu deals with miscellaneous configuration items including device identification, date and time, exporting and importing your NMC configuration options, the three links at the bottom left of the screen, and consolidating data for troubleshooting purposes.

## Identification screen

**Path: Configuration > General > Identification**

Define the **Name** (the device 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
- StruxureWare Central
- InfraStruxure Manager



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 Network Management Card *Utility* CD and the website, www.apc.com.

The **Name** and **Location** fields also identify the device when you register for the Remote Monitoring Service. See "Remote Monitoring Service" for more information.

## 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 an StruxureWare Central obtains its time settings by using StruxureWare Central 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. |

| Field | Description |
|---|---|
| **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). |
| **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's 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).<br>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.<br>The following definitions are from RFC3164:<br>• **Emergency**: The system is unusable<br>• **Alert**: Action must be taken immediately<br>• **Critical**: Critical conditions<br>• **Error**: Error conditions<br>• **Warning**: Warning conditions<br>• **Notice**: Normal but significant conditions<br>• **Informational**: Informational messages<br>• **Debug**: Debug-level messages<br>Following are the default settings for the **Local Priority** settings:<br>• **Severe** is mapped to **Critical**<br>• **Warning** is mapped to **Warning**<br>• **Informational** is mapped to **Info**<br>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**

This option is not available for all UPS devices.

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 equipment 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 screen”.

- 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 and About 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***

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 SNMP authentication failures. ii) Abnormal internal system events.

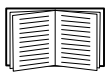
You can enable event color coding for through "Local Users" on the Configuration menu.

**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 FTP or Secure CoPy (SCP) to view the Event Log. See "How to use FTP or SCP 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 FTP or SCP to retrieve the log first, see “How to use FTP or SCP 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.

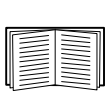
| Field | Description |
|---|---|
| **FTP Server** | The IP address or host name of the server where the file will reside. |
| **User Name**<br>**Password** | The user name with password required to send data to the repository file. This user must also be configured to have read and write access to the 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.<br>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 FTP or SCP to retrieve log files

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

- The file reports all events or data recorded since the log was last deleted or, in the case of the Data Log, truncated because it reached maximum size.
- The file includes information that the Event Log or Data Log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, and **Location** values and IP address of the NMC
  - The unique **Event Code** for each recorded event (*event.txt* file only)
  - 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*, available on the Network Management Card *Utility* CD and on the website (www.apc.com) for information on available protocols and methods for setting up the type of security you need.

**To use SCP to retrieve the files.** Enable SSH on the NMC, see “Console access”.

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 for the user name and password. For the Device User, the defaults are `device` for user name and `apc` for password.
3. Use the `get` command to transmit the text of a log to your local drive.

   `ftp>get event.txt`

   or

   `ftp>get data.txt`
4. You can use the `del` command to clear the contents of either log.

   `ftp>del event.txt`

   or

   `ftp>del data.txt`

   You will not be asked to confirm the deletion.

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

   – If you clear the Event Log, a new *event.txt* file records the event.
5. Type `quit` at the `ftp>` prompt to exit from FTP.

# 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.

# Energy Usage

**Path: Logs > Energy Usage**

This menu option is not available for all UPS devices.

The cumulative energy usage figures for your UPS device display at the top of the screen, with a week-by-week breakdown in the table at the bottom of the screen.

| Field | Description |
|---|---|
| **Energy Usage** | The amount of energy, in kilowatt-hours, consumed thus far by your UPS. For example, a UPS providing power to a 350 W light bulb for 1000 hours consumes 350 kWh of energy. |
| **Total Cost** | The estimated total cost of energy used thus far. For example, a light bulb consuming 350kWh of energy over 1000 hours with a price of $0.10 per kWh costs $35 over that period of time. |
| **$CO_2$ Emissions** | The estimated quantity of $CO_2$ released by the AC utility company into the environment to provide the energy used thus far. |

Costs and $CO_2$ emissions vary greatly by energy source and distribution network. You can obtain a rough estimate by choosing your country from the **Location** drop-down box, or use the "**(edit)**" link to input your own cost and emissions data.

Editing a location creates a custom location and does not alter the default figures for that location. For example, if you choose **IE-Ireland** from the drop-down list and subsequently use edit to change data, then an entry called **Custom (IE-Ireland)** is created at the top of the drop-down list.

# 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 screen".

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 the Network Management Card 2

## About the UPS device

**Path: About > UPS**

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

| Field | Description |
|---|---|
| **Model/ SKU/ Serial Number** | These fields identify your UPS device. |
| **UPS Position** | The physical orientation of the UPS, rack or tower. |
| **Manufacture Date** | The date your UPS was manufactured. |
| **Firmware Revision** | The revision numbers of the firmware modules currently installed on the UPS |
| **Firmware Revision2** | The second revision number of the firmware currently installed on the UPS. This is used when multiple processors require different versions. |
| **Apparent Power Rating** | The total VA capability of the UPS. |
| **Real Power Rating** | The total load capability (in Watts) of the UPS. |
| **Apparent Power Rating/Phase** | The VA capability of each UPS phase.<br>More technically, it is the present apparent power for each phase in Volt-Amps (VA). Apparent power is the product of RMS (root mean square) volts and RMS amperes. |
| **Real Power Rating/Phase** | The total load capability (in Watts) of the UPS.<br>The present active bypass power for each phase in watts (W). Active power is the time average of the instantaneous product of voltage and current. |
| **About UPS Monitoring Software** | Contains various information about software directly monitoring the UPS serially or over USB. |
| **Internal Battery SKU/ External Battery SKU** | These fields identify the part numbers for your batteries. This can be useful when troubleshooting problems. |

## 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.apcc.com/tools/download.

| Field Label | Description |
|---|---|
| **Name** | The name of the firmware module.<br>The **Application Module** name differs according to the UPS device type, e.g. **sumx** applies to Smart-UPS devices, **sy** to Symmetra devices.<br>The APC AOS module is always named **aos**, and the boot monitor module is always named **bootmon**. |
| **Version** | The version number of the firmware module. Version numbers of the modules may differ, but compatible modules are released together. Never combine application modules and AOS modules from different releases.<br>**Note:** If the boot monitor module must be updated, a boot monitor module is included in the firmware release. Otherwise, the boot monitor module that is installed on the card is compatible with the firmware update.<br>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.

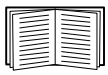
Click **Generate Logs** to create the file and then **Download**. You are asked whether you want to view or save the zipped file.

# Device IP Configuration Utility

## Capabilities, Requirements, and Installation

The Device IP Configuration Utility 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 Utility scans the IP addresses in the defined range and discovers cards that already have a DHCP-assigned IP address.



For detailed information on the Utility, see the Knowledge Base on the support page of the www.apc.com website and search for 3061 (the ID of the relevant article).

To use the DHCP Option 12 (AOS 5.1.5 or higher), see Knowledge Base ID FA156110.

### System requirements

The Utility runs on Microsoft Windows 2000, Windows Server® 2003, Windows Server 2012 and on both 32- and 64-bit versions of Windows XP, Windows Vista, Windows 2008, Windows 7 and Windows 8 operating systems.

This utility supports cards that have firmware version 3.0.x or higher and is for IPv4 only.

### Installation

To install the Utility from the *Utility* CD:

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

To install the Utility from a downloaded executable file:

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

When installed, the Utility 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 UPS Network Management Card 2 (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:

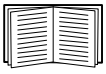
1. If possible, use the interface of an NMC to configure it with the settings to export. (Directly editing the .ini file risks introducing errors).
2. To use FTP to retrieve config.ini from the configured NMC:
   a. Open a connection to the NMC, using its IP address:

      `ftp> open` *`ip_address`*

   b. Log on using the Administrator user name and password.
   c. Retrieve the config.ini file containing the NMC's settings:

      `ftp> get config.ini`

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



To retrieve configuration settings from multiple NMCs and export them to other NMCs, see *Release Notes: ini File Utility, version 2.0*, available on the Network Management Card *Utility* CD and at www.apc.com. Or see it in the KBase, http://www.apc.com/site/support/index.cfm/faq/index.cfm.

**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:

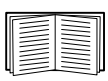
     `ftp> open` *ip_address*

  b. 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, version 2.0* on the Network Management Card *Utility* CD or view it in the KBase, http://www.apc.com/site/support/index.cfm/faq/index.cfm.

# 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.*<br>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

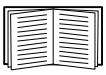
A device associated with the NMC from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the device (such as a UPS) is not present or is not discovered, the config.ini file contains a message under the appropriate section name, instead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

```
UPS not discovered
IEM not discovered
```

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

## Errors generated by overridden values

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

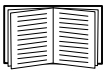


See “Contents of the .ini file” for information about which values are overridden.

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 Utility”.

# File Transfers

## Upgrading Firmware

When you upgrade the firmware on the UPS Network Management Card 2 (NMC), you obtain the latest new features, performance improvements, and bug fixes. For UPS firmware, see “Firmware Update screen”.

Upgrading here means simply placing the module files on the NMC, there is no installation as such. Check regularly on **www.apcc.com/tools/download** for any new upgrades.

### Firmware module files (Network Management Card 2)

A firmware version has three modules, and they *must* be upgraded (that is, placed on the NMC) in this order:

| | Module | Description |
|---|---|---|
| 1 | boot monitor (**bootmon**) | Roughly equivalent to the BIOS of a PC |
| 2 | American Power Conversion Operating System (**AOS**) | Can be thought of as the NMC operating system |
| 3 | **application** | Specific to the UPS device type, e.g. the Smart-UPS model, the Symmetra model |

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

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

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

- `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.
- `bin`: Indicates that this is a binary file.

## Firmware File Transfer Methods

Upgrade the bootmon module first, then the AOS module, and finally, the application module by placing them on the NMC in that order.

Obtain the free, latest firmware version from **www.apcc.com/tools/download**. To upgrade the firmware of one or more NMCs, use one of these five methods:

- On a Windows operating system, use the **Firmware Upgrade Utility** downloaded from the www.apc.com website. See “Using the Firmware Upgrade Utility”.
- On any supported operating system, use **FTP or SCP** to transfer the individual AOS and application firmware modules. 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 serial connection to transfer the individual firmware modules from your computer to the NMC. See “Use XMODEM to upgrade one NMC”.

- Use a **USB drive** to transfer the individual firmware modules from your computer (AP9631 only). See “Use a USB drive to transfer and upgrade the files (AP9631 only)”.
- For upgrades to **multiple NMCs**, see “Upgrading the firmware on multiple Network Management Cards” and “Using the Firmware Upgrade Utility for multiple upgrades on Windows”.

## Using the Firmware Upgrade Utility

This Firmware Upgrade Utility is part of the firmware upgrade package available on the www.apc.com 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 Firmware Upgrade Utility automates the transferring of the firmware modules, *in the correct module order.* The utility only works with an NMC that has an IPv4 address.

Unzip the downloaded firmware upgrade file and double-click the .exe file. Then enter the IP address, the user name, and the password in the dialog fields and click **Upgrade Now**. You can use the **Ping** button to test your entered details. See also “Using the Firmware Upgrade Utility for multiple upgrades on Windows”.

**Using the Utility for manual upgrades, primarily on Linux.** On non-Windows operating systems, the Firmware Upgrade Utility extracts the individual firmware modules, but does not upgrade the NMC. See “Firmware File Transfer Methods” for the different upgrade methods after extraction.

To extract the firmware files:

1. After obtaining the files from the downloaded firmware upgrade file, run the **Firmware Upgrade Utility** (the .exe file).
2. At the prompts, click **Next**>, and then specify the directory location to which the files will be extracted.
3. When the **Extraction Complete** message displays, close the dialog box.

## 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 files, perform these steps (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two though):

1. The firmware module files must be extracted, see “To extract the firmware files:”.
2. At a computer on the network, open a command prompt window. Go to the directory that contains the firmware files, and list the files:

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

   For file information, see “Firmware module files (Network Management Card 2)”.
3. Open an FTP client session:

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

4. 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.
5. Log on as Administrator (**apc** is the default user name and password).
6. Upgrade the AOS. (Always upgrade the AOS before the application module).

   `ftp> bin`
   `ftp> put apc_hw05_aos_`*`nnn`*`.bin` (where *nnn* is the firmware version number)
7. When FTP confirms the transfer, type `quit` to close the session.
8. After 20 seconds, repeat step 3 through step 7, using the application module file name at step 6.

**SCP.** To use Secure CoPy (SCP) to upgrade firmware for the NMC, follow these steps (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two though):

1. Locate the firmware modules, see “Using the Utility for manual upgrades, primarily on Linux.”.
2. Use an SCP command line to transfer the AOS firmware module to the NMC. The following example uses *nnn* to represent the version number of the AOS module:

   `scp apc_hw05_aos_`*`nnn`*`.bin apc@158.205.6.185:apc_hw05_aos_`*`nnn`*`.bin`
3. Use a similar SCP command line, with the name of the application module, to transfer the application firmware module to the NMC. (Always upgrade the AOS before the application module).

## Use XMODEM to upgrade one NMC

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

To transfer the files (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two though):

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

   (Always upgrade the AOS before the application module).
7. To install the application module, repeat step 5 and step 6. In step 6, use the application module file name.
8. Type `reset` or press the **Reset** button to restart the NMC.

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

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

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

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

   BM=apc_hw05_bootmon_102.bin
   AOS=apc_hw05_aos_515.bin
   APP=apc_hw05_sumx_514.bin
6. Place upload.rcf in the **apcfirm** folder on the flash drive.
7. Insert the flash drive into a USB port on your NMC, see “Front Panel (AP9631)”.
8. Reset the NMC and wait for the card to reboot fully.
9. Check that the upgrade was completed successfully using the procedures in “Verifying Upgrades”.

## Upgrading the firmware on multiple Network Management Cards

Use one of these three methods:

- **NMC2 Firmware Upgrade Utility on Windows**. See “Using the 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 Network Management Card *Utility* CD and in the KBase, http://www.apc.com/site/support/index.cfm/faq/index.cfm.

**Using the Firmware Upgrade Utility for multiple upgrades on Windows.** After downloading the Upgrade Utility from the NMC downloads page on the www.apc.com website, double click on the exe file to run the utility (which ONLY works with IPv4) and follow these steps to upgrade your NMC firmware:

1. In the utility dialog, type in an IP address, a user name, and a password, and choose the **Ping** button if you need to verify the IP address.
2. Choose the **Device List** button to open the `iplist.txt` file. Here you should type all UPS devices to upgrade with the necessary information: IP, user name, and password.

   For example,
   SystemIP=192.168.0.1
   SystemUserName=apc
   SystemPassword=apc

You can use an existing `iplist.txt` file if it already exists.

3. Select the **Upgrade From Device List** check box to use the `iplist.txt` file.
4. Choose the **Upgrade Now** button to start the firmware version upgrade(s).
5. Choose **View Log** to verify any upgrade.

# 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. Alternatively, you can use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

## 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.

# Adding and Changing Language Packs

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

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

The language pack files are available on the Network Management Card firmware download area on the website, www.apc.com. The language packs are included in the firmware upgrade package.

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

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

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

```
sy3p_510_esESzhCnjaJAptBrkoKo.lpk
```

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

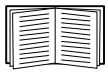
You might want to change the UI language to one that is not currently available to you. To do this, download the language pack from the website, and follow these steps:

1. Connect to your NMC using FTP.
2. Change to the **lang** folder of the NMC:
   `cd lang`
3. Transfer the required language pack to the NMC:
   `put <full path/language pack name>.lpk`
4. When the file finishes the transfer, log off FTP and the NMC will reboot.
5. When the reboot is complete, the new language pack is ready for use.

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

# Troubleshooting

## Network Management Card Access Problems



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

If the problem still persists, see "APC 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:<br>• Verify that the NMC is properly seated in the UPS.<br>• Verify all network connections.<br>• Verify the IP addresses of the NMC and the NMS.<br>• If the NMS is on a different physical network (or subnetwork) from the NMC, verify the IP address of the default gateway (or router).<br>• 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 enabled. Enabling SSH automatically disables Telnet.<br>• 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.<br>• 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.<br>• Verify that you can ping the NMC.<br>• Verify that you are using a Web browser supported for the NMC. See "APC Worldwide Customer Support".<br>• 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).<br>• Use the command line interface or UI to ensure that the NMS has access. See "SNMP screens". |
| Unable to perform a SET | • Verify the read/write (SET) community name (SNMPv1) or the user profile configuration (SNMPv3).<br>• 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.<br>• 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.<br>• For SNMPv3, check the user profile configuration for the NMS, and run a trap test.<br>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. |

# Synchronization Problems

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

# 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.

# Radio Frequency Interference

**Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.**

## USA—FCC

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference. The user will bear sole responsibility for correcting such interference.

## Canada—ICES

This Class A digital apparatus complies with Canadian ICES-003.

*Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.*

## Japan—VCCI

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると、電波

妨害を引き起こすことがあります。この場合には、使用者が適切な対策を講ずるように要求されることがあります

## Taiwan—BSMI

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

## Australia and New Zealand

**Attention:** This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

## European Union

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. APC cannot accept responsibility for any failure to satisfy the protection requirements resulting from an unapproved modification of the product.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide a reasonable protection against interference with licensed communication equipment.

**Attention:** This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

## Korean 한국

A 급 기기 ( 업무용 방송통신기기 )

이 기기는 업무용 (A 급 ) 으로 전자파적합등록을 한 기기이오니판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정외의지역에서 사용하는 것을 목적으로 합니다 .

# APC Worldwide Customer Support

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

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

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



**990-3402F-001** **7/2014**