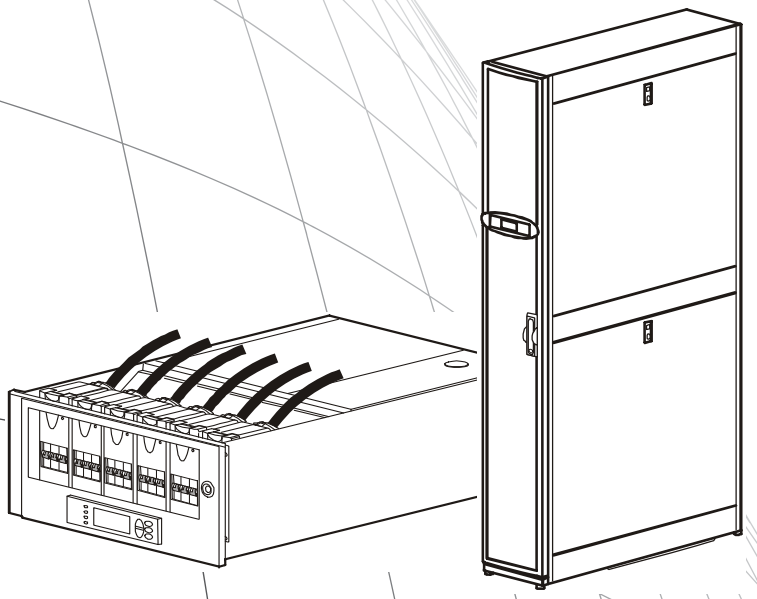
Schneider Electric

User Guide

Modular Power Distribution Units
Remote Power Panel and
Remote Distribution Panel

PDPM138H-5U
PDPM138H-R
PDPM72F-5U
PDPM72F-R
PDPM277H
PDPM144F



Contents

Introduction

Overview

Features

The APC by Schneider Electric Modular Remote Power Panel and Remote Distribution Panel provides power distribution and management of electrical power to equipment racks. The Network Management Card (NMC) of the Modular PDU provides full management capabilities over a network using Telnet, Secure SHell (SSH), HyperText Transfer Protocol (HTTP), HTTP over Secure Sockets Layer (HTTPS), File Transfer Protocol (FTP), and Simple Network Management Protocol (SNMP) versions 1 and 3. The Modular PDU also provides the following features:

- Provides the ability to export a user configuration (.ini) file from a configured Modular PDU to one or more unconfigured Modular PDUs.
- Supports using a Dynamic Host Configuration Protocol (DHCP) server to provide the network (TCP/IP) values for the Modular PDU.
- Provides data and event logs.
- Enables you to configure notification through event logging (by the Modular PDU and Syslog), e-mail, and SNMP traps. You can configure notification for single events or groups of events, based on the severity level or category of events.
- Provides a selection of security protocols for authentication and encryption.

Make the connection to the PDU: A Cat-5 cable is plugged into the ethernet port on the back of the unit. Connect the other end of the cable to the LAN.

A serial cable can be connected in the port above the ethernet port. Connect the other end to a local computer.

Initial setup

Three TCP/IP settings must be defined for the Network Management Card before it can operate on the network:

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

CAUTION

HAZARD TO EQUIPMENT
Never use the loopback address as the default gateway. Doing so disables the Modular PDU. You must then log on using a serial connection and reset TCP/IP settings to their defaults using a local serial login.
Failure to follow these instructions will disable communication with the Modular PDU.

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

Network management features

These applications and utilities work with a Modular PDU that connects to the network through its Network Management Card:

- APC StruxureWare Central™ —Provide enterprise-level power management and management of APC agents, Modular PDUs, information controllers, and environmental monitors
- APC PowerNet™ Management Information Base (MIB) with a standard MIB browser—Perform SNMP SETs and GETs and to use SNMP traps
- APC Device IP Configuration Wizard—Configure the basic settings of one or more NMCs over the network
- APC Security Wizard—Create the components needed for high security for the NMC when using Secure Sockets Layer (SSL) and related protocols and encryption routines

Internal Management Features

Overview

Use the Web interface or the control console interface to manage the Modular PDU.

Access priority for logging on

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

- Local access to the control console from a computer with a direct serial connection to the Modular PDU.
- Telnet or Secure SHell (SSH) access to the control console from a remote computer.
- Web access, either directly or through InfraStruxure Central

Types of user accounts

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

- An Administrator can use all the menus in the Web interface and control console. The default user name and password are both **apc**.
- A Device User can access only the following:
  - In the Web interface, the menus on the **Home**, **Power Distribution**, **Contacts/Relays**, **Alarms**, and **Logs** tabs and the event and data logs.
  - In the control console, the equivalent features and options.

  The default user name is **device**, and the default password is **apc**.
- A Read-Only User has the following restricted access:
  - Access through the Web interface only. You must use the Web interface to configure values for the Read-Only User.
  - Access to the same tabs and menus as a Device User, but without any capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled, and the event and data logs display no button to clear the log.

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

Watchdog Features

Watchdog mechanisms detect internal problems. After a restart, a **System: Warmstart** event is recorded in the event log.

Network interface watchdog mechanism

Watchdog mechanisms protect the NMC from becoming inaccessible over the network. If it does not receive any network traffic for 9.5 minutes, it assumes there is a problem with its interface and restarts.

Resetting the network timer

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

Recover from a Lost Password

1. At the local computer, select a serial port, and disable any service that uses it.
2. Connect the provided serial cable to the computer and the port on the PDU.
3. Run a terminal program (such as HyperTerminal®) and configure the 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 on the back of the unit. The Status LED will flash. Press the **Reset** button a second time while the LED is flashing to reset the user name and password to the default.
6. Press ENTER as many times as necessary to redisplay the **User Name** prompt, then use the default, **apc**, 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. Select **System**, then **User Manager**.
8. Select **Administrator**, and change the **User Name** and **Password** settings from the default **apc**.
9. Press CTRL+C and log off. Return the local computer to its original configuration.

Control Console

Log On

You can use either a local (serial) connection or a remote (Telnet or SSH) connection with a computer on the same network (LAN) as the NMC to access the control console.

Use case-sensitive user name and password entries to log on (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device User). A Read-Only User has no access to the control console.

Remote access to the control console

You can access the control console through Telnet or Secure SHell (SSH). Telnet is enabled by default. Enabling SSH disables Telnet.

To enable or disable these access methods:

- In the Web interface, on the **Administration** tab, select **Network** on the top menu bar, and then the **access** option under **Console** on the left navigation menu.
- In the control console, use the **Telnet/SSH** option of the **Network** menu.

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

To use Telnet to access the control console:

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

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

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

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

Local access to the control console

For local access, use a computer that connects to the Modular PDU through the serial port, to access the control console:

1. Select a serial port at the computer and disable any service that uses the port.
2. Connect the provided serial cable from the selected port on the computer 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, and at the prompts, enter your user name and password.

Main Screen

Sample main screen

The following is an example of the screen that displays when you log on to the control console at the NMC.

```
American Power Conversion               Network Management Card AOS  vx.x.x
(c)Copyright 2009 All Rights Reserved                        NMC APP  vx.x.x
 -------------------------------------------------------------------------
Name     : Test Lab                                  Date : 12/30/2011
Contact  : Don Adams                                 Time : 5:58:30
Location : Building 3                                User : Administrator
Up Time  : 0 Days, 21 Hours, 21 Minutes              Stat : P+ N+ A+

 ------- Control Console -----------------------------------------------

       1- Device Manager
       2- Network
       3- System
       4- Logout
       <ESC>- Main Menu, <ENTER>- Refresh, <CTRL-L>- Event Log
```

Information and status fields

Main screen information fields.

- Two fields identify the APC operating system (AOS) and application (APP) firmware versions.

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

- Three fields identify the system name, contact person, and location of the NMC (In the control console, use the **System** menu to set these values.)

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

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

  ```
  Up Time: 0 Days 21 Hours 21 Minutes
  ```

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

  ```
  Date : 12/30/2011
  Time : 5:58:30
  ```

- The **User** field reports whether you logged in through the **Administrator** or **Device User** account. (The **Read Only User** account cannot access the control console.)

  ```
  User : Administrator
  ```

Main screen status fields.

- The **Stat** field reports the NMC status.

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

P+	The APC operating system (AOS) is functioning properly.
N+	The network is functioning properly.
N?	A BOOTP request cycle is in progress.
N–	The NMC failed to connect to the network.
N!	Another device is using the IP address of this NMC.
A+	The application is functioning properly.
A–	The application has a bad checksum.
A?	The application is initializing.
A!	The application is not compatible with the AOS.

  If P+ is not displayed, contact the APC support staff at **www.apc.com/support** even if you can still access the NMC.

- The status field displays the status of the PDU in which the NMC is installed. Under normal operation, this field displays **Communication Established**.

Control Console Menus

Overview

The control console provides options to monitor and configure the NMC.

How to use control console menus

The menus in the control console list options by number and name. To use an option, type the option's number, press ENTER, and follow any on-screen instructions. If you use an option that changes a setting or value, select **Accept Changes** to save your change before you exit the menu.

While using a menu, you can also do the following:

- Type ? and press ENTER for menu option descriptions if help exists for the menu.
- Press ENTER to refresh the menu
- Press ESC to go back to the menu from which you accessed the current menu
- Press CTRL+C to return to the main (**Control Console**) menu
- Press CTRL+D to toggle between menus
- Press CTRL+L to access the event log

Control console structure

For menus not specific to the NMC but shared among APC network-enabled devices, names and locations of options differ from those of the Web interface. The menu structure in the control console is retained from earlier firmware versions for compatibility with scripts and programs that rely on that structure.

Main menu

Use the main **Control Console** menu to access the control console's management features:

```
1- Device Manager
2- Network
3- System
4- Logout
```

When you log on as Device Manager (equivalent to Device User in the Web interface), you can access only the **Device Manager** menus and the **Logout** menu.

Device Manager menu

An Administrator or Device User can use the options of the **Device Manager** menu to view parameters and display detailed status.

Network menu

To perform these tasks, use the options of the **Network** menu:

- Configure the TCP/IP settings of the NMC or, if the NMC obtains its TCP/IP settings from a server, configure the settings for the type of server (DHCP or BOOTP).
- Use the Ping utility.
- Define settings that affect FTP, Telnet and SSH, the Web interface and SSL, SNMP, e-mail, DNS, and Syslog.

System menu

Use the options of the **System** menu to perform these tasks:

- Control **Administrator** and **Device Manager** access. (**Read Only User** access is managed through the Web interface only.)
- Define the **Name**, **Contact**, and **Location** values for the system.
- Set the date and time used by the NMC.
- Through the **Tools** option:
  - Restart the NMC interface.
  - Reset parameters to their default values.
  - Delete SSH host keys and SSL certificates.
  - Upload an initialization file (.ini file) that has been downloaded from another NMC. The current NMC then uses the values in that .ini file to configure its own settings.
- Access system information about the NMC.

Logout

Select the logout option to log out of the control console.

Web Interface

Supported Web browsers

Use Microsoft® Internet Explorer (IE) 7.x and higher (Windows operating systems) or Mozilla Firefox 3.0.6 or higher (all operating systems) to access the NMC through its Web interface. Other commonly available browsers may work but have not been fully tested by APC. The NMC cannot work with a proxy server. Before using a Web browser to access its Web interface, do one of the following:

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

Log On

Overview

Use the DNS name or System IP address of the NMC for the URL address of the Web interface. The default password is **apc** for all three account types. The default user name differs by account type:

- **apc** for an Administrator
- **device** for a Device user
- **readonly** for a Read-Only user

If you are using HTTPS (SSL/TSL) as your access protocol, your logon credentials are compared with information in a server certificate. If the certificate was created with the APC Security Wizard, and an IP address was specified as the common name in the certificate, you must use an IP address to log on to the NMC. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

URL address formats

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

Common browser error messages at log-on.

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

Home Page

View active alarm conditions and the most recent events recorded in the event log.

Quick status icons. At the upper right corner of every page, icons indicate the current operating status and the number of active alarms of that severity. Click on a quick status icon from any page of the interface to return to the **Home** page.

Critical: A critical alarm exists, which requires immediate action.

Warning: An alarm condition requires attention and could jeopardize data or equipment if not addressed.

Online/No Alarms Present: The Modular PDU is operating normally.

Active alarms. The **Power Distribution** section of the **Home** page summarizes the status of the Modular PDU:

- The **Online** icon displays if no alarms exist.
- One or both of the **Critical** and **Warning** icons display if any alarms exist, and after each icon, the number of active alarms of that severity.

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

Information. This section displays the following information for the Modular PDU.

- Name
- Contact
- Location
- User
- UpTime

Tabs, Menus, and Links

Tabs

In addition to the **Home** page, the following tabs are displayed. Click on a tab to display the options:

- **Power Distribution**: View the power output and configure alarm thresholds.
- **Logs**: View and configure event and data logs.
- **Administration**: Configure security, network connection, notification, and general settings.

Menus

Left navigation menu. Each tab except the home page has a left navigation menu of options.

- A heading with option names below it is not a link. Click an option to display or configure.
- A heading with no option names is the navigational link. Click the heading to display parameters.

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

Quick Links

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

- **Link 1**: The home page of the APC Web site
- **Link 2**: **Testdrive Demo** provides demonstrations of APC Web-enabled products.
- **Link 3**: Information on APC Remote Monitoring Services.

Security

Types of user accounts

The three levels of access are protected by user name and password requirements. During authentication, the user's credentials are compared against the Local User Database and/or are validated against a RADIUS server (depending on configuration). If valid, access with appropriate permissions is granted.

- An Administrator can use all the menus in the Web interface. The default user name and password are both **apc**.
- The default user name for the Device User is **device**, and the default password is **apc**. A Device User can access only the menus on the **Home**, **Power Distribution**, and **Logs** tabs.
- A Read-Only User has only Web interface access. The same menus as Device User are visible but no changes can be made. Links to configuration options are visible but disabled. Event and data logs display no button to clear the log. The default user name is **readonly**, and the default password is **apc**.

Local Users

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

Setting user access. Set the case-sensitive user name and password for each account. 10 characters maximum for user names and 32 characters for passwords. Blank passwords are not allowed.

Remote Users

Path: Administration > Security > Remote Users > Authentication Method

Authentication. Select how remote access to the NMC is administered. See the *Security Handbook*, available on the APC Web site, **www.apc.com** for more information.

- When a user accesses the NMC that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user’s permission level.
- RADIUS user names used with the NMC are limited to 32 characters.

Select one of the following:

- **Local Authentication Only**: RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Authentication**: RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used.
- **RADIUS Only**: RADIUS is enabled. Local authentication is disabled. If the RADIUS server is unavailable, improperly identified, or improperly configured, use a serial connection to change the **Access** setting to **Local Authentication Only** or **RADIUS, then Local Authentication** to regain access.

RADIUS.

Path: Administration > Security > Remote Users >RADIUS

Use this option to do the following:

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

RADIUS Setting	Definition
RADIUS Server	The name or IP address of the RADIUS server. RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number at the end of the RADIUS server name or IP address.
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 to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path.
Switch Server Priority	Change which RADIUS server will authenticate users if two configured servers are listed and **RADIUS, then Local Authentication** or **RADIUS Only** is the enabled authentication method.

Configure the RADIUS Server

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

Configure a RADIUS server on UNIX® with shadow passwords

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`.
- Add user names and attributes to RADIUS “user” file. Verify passwords against `/etc/passwd`.

Supported RADIUS servers

FreeRADIUS, Microsoft Windows 2000 Server and Microsoft Windows 2000 RADIUS Server are supported. Other RADIUS applications may work but have not been fully tested.

Inactivity Timeout

Path: Administration > Security > Auto Log Off

Configure the time the system waits before logging off an inactive user (default 3 minutes). If the value is changed, you must log off for the change to take effect. If a user closes the browser window without first logging off (clicking **Log Off** at the upper right corner), the user is still considered logged on and no user of that account type can log on until the **Minutes of Inactivity** expire.

Managing Power Distribution

Viewing Modular PDU Information

Power distribution alarm status

Path: Power Distribution > Overview

If an alarm exists, a status icon and accompanying text display at the top of the page.

Viewing output measurements

Path: Power Distribution > System Output

The **System Output** section lists detailed information about power leaving the PDU:

- Voltage: The phase-to-phase output voltage (e.g., L1-2 for phase L1 to phase L2) for a 3-wire connection, or the phase-to-neutral output voltage (e.g., L1 for phase 1 to neutral) for a 4-wire connection.
- Current: The load supported by each phase, in RMS current (Irms).
- Power: The active power, in kW, provided for each phase and for the total of the three phases.
- Frequency: The frequency, in Hz, of the output.

View Module status

Distribution Module Status can be shown **Populated Only** or by **All Locations**. The Status, Rating, Position, Load Name, Current, and Power are shown on each page.

Quick status icons. Color-coded icons show the status of the Modules:

- Red: The Module is causing one or more critical alarms.
- Yellow: The Module is causing one or more warning alarms.
- Gray: The Module is not influencing the status of the PDU or is not installed.
- Green: The PDU is operating normally.

Mass Configuration. All modules can be configured at the same time by clicking on **Mass Configuration** at the bottom right of either the **Populated Only** or by **All Locations** pages. Alarm generation and current threshold settings are selected on this page. Click on Apply to All Modules at the bottom of the page to enable the selections.

View Manufacturing Info

Path: Power Distribution > modules

View the status of the modules. The first selectable heading under **Manufacturing Info** is **modules**. All of the modules are listed in the page with Status, Model Number, Serial Number, Manufacturing Date and the number of Output Cable for each module. A status icon and accompanying text display next to the Status of the Module.

Path: Power Distribution > metering system

View the status of the metering system. The next selectable heading under **Manufacturing Info** is **metering system**. The metering system information for the modules is shown on the page. The Model Number, Serial Number, Manufacture Date and Firmware Revision number are all identified.

Path: Power Distribution > electrical config

View the status of the electrical configuration. The last selectable heading under Manufacturing Info is electrical config. Nominal Voltage and Maximum Panel Current are identified.

Network Settings

TCP/IP settings

Path: Administration > Network > TCP/IP

The **TCP/IP** option (default) displays the current IP address, subnet mask, default gateway, and MAC address of the NMC. **TCP/IP Configuration** provides options for TCP/IP setting configuration when the NMC is powered on, resets, or restarts.

Setting	Description
Manual	Configure the IP address, subnet mask, and default gateway manually. Click **Next** and enter new values.
BOOTP	At 32-second intervals, the NMC requests network assignment from any BOOTP server: If a valid response is received, the network services are started. If a BOOTP server is found, but a request to that server fails or times out, the NMC stops requesting network settings until the NMC is restarted. By default, if previously configured network settings exist, and no valid response to five requests is received, the previously configured settings are used so that the NMC remains accessible. Click **Next** to open the BOOTP Configuration page to edit the number of retries or retry failure action[1]: **Maximum retries**: The number of retries when no response is received, or zero (0) for unlimited retries. **If retries fail**: Select **Use prior settings** (the default) or **Stop BOOTP request**.
DHCP	The NMC requests network assignment from a DHCP server every 32 seconds. By default, the number of retries is unlimited. If a valid response is received, by default the NMC requires the APC cookie from the DHCP server in order to accept the lease and start the network services. If a DHCP server is found, but the request fails or times out, network settings requests are stopped until the NMC is restarted. To change these values, click **Next** for the **DHCP Configuration** page[1]: **Require vendor specific cookie to accept DHCP Address**: Disable/enable. **Maximum retries**: The number of retries when no valid response is received or zero for unlimited retries.
DHCP & BOOTP	The default. The NMC tries to obtain its TCP/IP settings from a BOOTP server first, and if it cannot, from a DHCP server. It switches to **BOOTP** or **DHCP** depending on which server supplied the TCP/IP settings. Click **Next** to configure the settings on the **BOOTP Configuration** and **DHCP Configuration** pages[1] and to specify the **DHCP and BOOTP** setting be retained after either server provides the TCP/IP values.

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

DHCP response options

Each valid DHCP response provides the TCP/IP settings needed to operate on a network and other information that affects the operation of the NMC.

Vendor Specific Information (option 43). Used to determine whether the DHCP response is valid.

- **APC Cookie. Tag 1, Len 4, Data "1APC"**

  Communicates that a DHCP server is configured to service APC devices. By default, the DHCP response must contain the APC cookie to accept the lease.

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

  Enables or disables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** which, by default, is disabled.

  - A value of 1 enables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. When the NMC reboots, it requests network assignment first from a BOOTP server, and then if necessary, from a DHCP server.
  - A value of 2 disables the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** option. The **s**etting switches to **DHCP** when the DHCP response is accepted. The NMC requests network assignment from a DHCP server when it reboots.

TCP/IP options. Used with a valid DHCP response to define TCP/IP settings. All options except the first are described in **RFC2132**.

- **IP Address**: 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** (option 3): The default gateway address that the NMC needs to operate on the network.
- **IP Address Lease Time** (option 51): The time limit 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 wait time after an IP address lease is assigned before the NMC can seek to rebind that lease.

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

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

Port Speed

Path: Administration > Network > Port Speed

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

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

DNS

Path: Administration > Network > DNS > *options*

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

- Select **servers** to specify the IP addresses of the primary (and optional secondary) DNS server. For the NMC to send e-mail, at least the IP address of the primary DNS server must be defined.
  - The NMC waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server (if specified). 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 defining the IP addresses of the DNS servers, enter the DNS name of a computer on your network to look up the IP address for that computer to verify operation.
- Select **naming** to define the host name and domain name of the NMC:
  - **Host Name**: Configured here to enter a host name in any field in the NMC interface (except e-mail addresses) that accepts a domain name.
  - **Domain Name**: Configured here only. In the NMC interface (except e-mail addresses), the NMC adds this domain name when only a host name is entered.
    - To override the expansion of a host name by the addition of the domain name, set the domain name field to its default, `somedomain.com`, or to `0.0.0.0`.
    - To override the expansion of a host name entry, include a trailing period. The NMC will treat it as if it were a fully qualified domain name and will not append the domain name.
- Select **Test** to send a DNS query that tests the setup of your DNS servers:
  - As **Query Type**, select the method to use for the DNS query:
    - **by Host**: the URL name of the server
    - **by FQDN**: the fully qualified domain name
    - **by IP**: the IP address of the server
    - **by MX**: the Mail Exchange used by the server
  - As **Query Question**, identify the value to be used for the selected query type:

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

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

Web

Path: Administration > Network > Web > *options*

Option	Description
access	Log off to activate changes to any of these selections: • **Disable**: Disables access to the Web interface. • **Enable HTTP** (the default): Enables Hypertext Transfer Protocol (HTTP), which provides Web access by user name and password, but does not encrypt user names, passwords, or data during transmission. • **Enable HTTPS**: Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL). SSL encrypts user names, passwords, and data during transmission. Authenticates the NMC by digital certificate. When HTTPS is enabled, your browser displays a small lock icon. **HTTP Port**: The TCP/IP port (80 by default) used to communicate by HTTP. **HTTPS Port**: The TCP/IP port (443 by default) used to communicate by HTTPS. For either, the port setting can be changed to an unused port from 5000 to 32768 for additional security. Use a colon (:) in the address field of the browser to specify the port number.
ssl cipher suites	Enable or disable any of the SSL encryption ciphers and hash algorithms: • **DES**: A block cipher that provides authentication by Secure Hash Algorithm. • **RC4_MD5** (default enabled): A stream cipher that provides authentication by MD5 hash algorithm. • **RC4_SHA** (default enabled): A stream cipher that provides authentication by Secure Hash Algorithm. • **3DES**: A block cipher that provides authentication by Secure Hash Algorithm.
ssl certificate	**Status**: • **Not installed**: A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Using **Add or Replace Certificate File** installs the certificate to the correct location, **/sec** 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. • **Valid certificate**: A valid certificate was installed or generated by the NMC. Click the link to view the certificate. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the NMC generates a default certificate, a process which delays access to the interface for up to five minutes.** You can use the default certificate, but a security alert message displays whenever you log on. **Add or Replace Certificate File**: Enter or browse to the certificate file created with the Security Wizard. See the *Security Handbook* on the APC Web site, **www.apc.com**, for more information. **Remove**: Delete the current certificate.

Console

Path: Administration > Network > Console > *options*

Option	Description
access	Choose one of the following for access by Telnet or Secure SHell (SSH): • **Disable**: Disables all access. • **Enable Telnet** (the default): Telnet transmits user names, passwords, and data without encryption. • **Enable SSH v1 and v2**: Do not enable both versions 1 and 2 of SSH unless you require both. They use extensive processing power. • **Enable SSH v1 only**: Encrypts user names, passwords, and data for transmission. There is little or no delay as you log on. • **Enable SSH v2 only**: Transmits user names, passwords, and data in encrypted form with more protection than version 1. There is a noticeable delay as you log on. Configure the ports to be used by these protocols: • **Telnet Port**: (23 by default). Change to an unused port from 5000 to 32768 for added security. Use a colon (:) or space to specify the non-default port (as required by your Telnet client program). • **SSH Port**: (22 by default). Change the port setting to an unused port from 5000 to 32768 for additional security. See your SSH client documentation for the format required to specify a non-default port.
ssh encryption	Enable/disable encryption algorithms compatible with SSH version 1 or version 2 clients: If your SSH v1 client cannot use **Blowfish**, you must also enable **DES**. Your SSH v2 client selects the algorithm that provides the highest security. If the client cannot use the default algorithms (**3DES** or **Blowfish**), enable an AES algorithm that it can use (**AES 128** or **AES 256**)
ssh host key	**Status** indicates the status of the host key (private key): • **SSH Disabled: No host key in use:** When disabled, SSH cannot use a host key. • **Generating**: The 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 **/sec** directory (the required location on the NMC): •A 1024-bit host key created by the APC Security Wizard •A 768-bit RSA host key generated by the NMC **Add or Replace**: Upload a host key file created by the Security Wizard: If you use FTP or Secure CoPy (SCP) to transfer the host key file, specify the **/sec** directory as the target location. **If you enable SSH with no host key loaded, it can take up to 5 minutes to create a host key, and the SSH server is not accessible during that time.** **Remove**: Removes the current host key.

SNMP

Path: Administration > Network > SNMPv1 > *options*

SNMPv1. 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 to receive status information and use SNMP traps.

Option	Description
access	**Enable SNMPv1 Access:** Enables SNMP version 1 as a method of communication with this device.
access control	Configure up to four access control entries to specify which NMSs have access to this device. The access control opening page, by default, assigns one entry to each of the four SNMPv1 communities. Edit to apply more than one entry to a community to grant access by several IP addresses, host names, or IP address masks. To edit the access control settings, click its community name. • Leave the default access control entry unchanged and the community has access from any location on the network. • Multiple access control entries for one community name means one or more of the other communities will have no access control entry. If no access control entry is listed, that community has no access to the device. **Community Name:** The name that a NMS uses to access the community. The maximum length is 15 ASCII characters. The default names are `public`, `private`, `public2`, and `private2`. **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address 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 (default) can also be expressed as 255.255.255.255: Access by any NMS on any segment. **Access Type**: The actions an NMS can perform through the community. • **Read**: GETS only, at any time • **Write**: GETS at any time, and SETS when no user is logged onto the Web interface. • **Write+**: GETS and SETS at any time. • **Disabled**: No GETS or SETS at any time.

Path: Administration > Network > SNMPv3 > *option*

SNMPv3. For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users. An SNMPv3 user must have a user profile assigned in the MIB software program to perform GETs and SETs, browse the MIB, and receive traps. You must have a MIB program that supports SNMPv3. The NMC supports only MD5 authentication and DES encryption.

Option	Description
access	**SNMPv3 Access:** Enables SNMPv3 as a method of communication with this device.

Option	Description
user profiles	By default, lists the settings of four user profiles, configured with the user names **apc snmp profile1** through **apc snmp profile4**, no authentication and no privacy (no encryption). To edit the following settings for a user profile, click a user name in the list. **User Name:** The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters. **Authentication Passphrase:** A phrase of 15 to 32 ASCII characters (`apc auth passphrase`, by default) that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time. **Privacy Passphrase:** A phrase of 15 to 32 ASCII characters (`apc crypt passphrase`, by default) that ensures the privacy of the data (by means of encryption) that an NMS is sending to this device or receiving from this device through SNMPv3. **Authentication Protocol:** Supports MD5 authentication. Authentication will not occur unless MD5 is selected as the authentication protocol. **Privacy Protocol:** Supports DES as the protocol for encrypting and decrypting data. Privacy of transmitted data requires that DES is selected. It cannot be selected unless an authentication protocol is selected.
access control	Configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles. Edit the settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks. • Leave the default access control entry unchanged for a user profile and all NMSs that use that profile have access to this device. • Multiple access entries for one user profile, means there can be no access control entry for one or more of the other user profiles. If no access control entry is listed for a user profile, NMSs using that profile have no access to this device. To edit the access control settings for a user profile, click its user name. **Access:** Mark the **Enable** checkbox to activate access control. **User Name:** Select the user profile to which access control will apply. The choices are the four user names you configured in 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 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

Path: Administration > Network > FTP Server

The **FTP server** settings enable (by default) or disable access to the FTP server and specify the TCP/IP port (21 by default) that the FTP server uses to communicate with the NMC. The FTP server uses both the specified port and the port one number lower than the specified port. Change the **Port** setting to the number of any unused port from 5001 to 32768 for added security. Users must then use a colon (:) to specify the non-default port number. FTP transfers files without encryption. For higher security, disable the FTP server, and transfer files with Secure CoPy (SCP). Selecting and configuring Secure SHell (SSH) enables SCP automatically. For an NMC to be accessible for management by InfraStruxure Central, FTP Server must be enabled in the NMC interface.

Notification

Event Actions

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

Types of notification

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

- Active, automatic notification. The specified users or monitoring devices are contacted directly.
  - E-mail notification
  - SNMP traps
  - Remote Monitoring
- Indirect notification through the event log. If none of the direct notification methods are configured, users must check the log to determine which events have occurred.

Configure event actions

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

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

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

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.
2. In the list of events, review the marked columns to see whether the action you want is already configured. (By default, logging is configured for all events.)
3. To view or change the current configuration, such as recipients to be notified by e-mail, or Network Management Systems (NMSs) to be notified by SNMP traps, click on the event name. If no Syslog server is configured, items related to Syslog configuration are not displayed.

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

1. Select **Administration** > **Notification** > **Event Actions > by group**.
2. Choose how to group events:
   – **Grouped by severity:** to select all events of one or more severity levels. You cannot change the severity of an event.
   – **Grouped by category:** to select all events in one or more pre-defined categories.
3. Click **Next** to do the following:
   a. Select event actions for the group of events.
      • To choose any action except **Logging** (the default), first have at least one recipient or receiver configured.
      • If you choose **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** (or both) on the next page.
   b. Enable/disable the newly configured event action for this group of events.

Automatic Direct Notification

E-mail notification

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 secondary (optional) Domain Name System (DNS) servers.
- The IP address or DNS name for **SMTP Server** and **From Address**.
- The e-mail addresses for a maximum of four recipients.

SMTP.

Path: Administration > Notification > E-mail > server

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

E-mail recipients.

Path: Administration > Notification > E-mail > recipients

Identify up to four e-mail recipients.

Setting	Description
To Address	The user and domain names of the recipient. To 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.
SMTP Server	Select one of the following methods for routing e-mail: • **Local**: Through the NMC's SMTP server. This setting (recommended) ensures that the e-mail is sent before the NMC's 20-second time-out and retried several times (if necessary). Also do one of the following: •Enable forwarding at the NMC's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Check with the SMTP server administrator before changing its configuration. •Set up a special e-mail account for the NMC to forward e-mail to an external mail account. • **Recipient**: With this setting, the NMC tries to send the e-mail only once, directly to the recipient's SMTP server. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent. When the recipient uses the NMC's SMTP server, this setting has no effect.
E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.
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.

Email test (Administration > Notification > E-mail > test). Send a test message to a configured recipient.

SNMP Traps

Path: Administration > Notification > SNMP Traps > trap receivers

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

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

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

SNMPv1 option.

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

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

SNMP Trap Test

Path: Administration > Notification > SNMP Traps > test

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

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

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

Syslog

Path: Logs > Syslog > *options*

The NMC can send messages to up to four Syslog servers when an event occurs. The Syslog servers record events that occur at network devices in a log that provides a centralized record of events. See **RFC3164** online for more information about Syslog.

Identifying Syslog Servers.

Path: Logs > Syslog > servers

Setting	Definition
Syslog Server	Uses IP addresses or host names to identify from one to four servers to receive Syslog messages sent by the 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.

Syslog Settings.

Path: Logs > Syslog > settings

Setting	Definition
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the NMC's Syslog messages (**User**, by default). **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.
Severity Mapping	Maps the severity level of NMC or Environment events to available Syslog priorities. You should not need to change the mappings. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the four **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info**

Path: Logs > Syslog > test

Syslog Test and Format example. Send a test message to the Syslog servers configured through the **servers** option.

1. Select a severity to assign to the test message.
2. Define the test message, according to the required message fields.
   Example: `APC: Test Syslog` is valid.
   – 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 event code.

Queries (SNMP GETs)

See "SNMP" on page 19 for a description of SNMPv1 and SNMPv3 settings that enable an NMS to perform informational queries. With SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without allowing remote configuration changes.

General Options

NMC Information

Identification

Path: Administration > General > Identification

Define values for **Name** (the device name), **Location** (the physical location), and **Contact** (the person responsible for the device) used by the NMC's SNMP agent. These settings are the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifiers (OIDs).

Set the Date and Time

Path: Administration > General > Date & Time > mode

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

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

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

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

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

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

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

Format. Select the format to display all dates in this user interface. Each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months display with a leading zero.

.ini file

Path: Administration > General > User Config File

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

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

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

Temperature Units

Path: Administration > General > Preferences

Check the box to Enable the Event Log Color Coding.

Select the temperature scale (Fahrenheit or Celsius) in which all temperature measurements will display.

Reset the Interface

Path: Administration > General > Reset/Reboot

Action	**Definition**
Reboot Management Interface	Restarts the interface of the NMC.
Reset All[1]	Select **Exclude TCP/IP** to reset all values except TCP/IP; clear **Exclude TCP/IP** to reset all configuration values.
Reset Only[1]	**TCP/IP settings**: Set TCP/IP Configuration to **DHCP & BOOTP**, its default setting, requiring that the NMC receive its TCP/IP settings from a DHCP or BOOTP server.
	Event configuration: Reset all changes to event configuration, by event and by group, to their default settings.
1. Resetting may take up to a minute.	

Serial Modbus

Path: Administration > General > Serial Modbus

Check the box to enable Modbus Access.

Set the Baud Rate to 9600 or 19200

Target Unique ID (1 to 247): Enter the ID number in the box.

Click on **Apply** to apply the changes or Cancel to leave without making changes.

Configuring Links

Path: Administration > General > Quick Links

Select the **Administration** tab, **General** on the top menu bar, and **Quick Links** on the left navigation menu to view and change the URL links displayed at the bottom left of each page of the interface. By default, these links access the following Web pages:

- **Link 1**: The home page of the APC Web site.
- **Link 2**: A page where you can use samples of APC Web-enabled products.
- **Link 3**: The home page of the APC Remote Monitoring Service.

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

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

About the NMC

Path: Administration > General > About

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

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

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

Logs

Event log

Path: Logs > Events > *options*

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

For all configurable events and their current configuration go to: **Administration** > **Notification** > **Event Actions** >**by event**.

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

- By default, view the event log as a page of the Web interface.
- To see the listed events on one page, click **Launch Log in New Window** from the event log page to display a full-screen view of the log. In your browser's options, JavaScript® must be enabled for you to use the **Launch Log in New Window** button.

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

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

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

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

- To remove an active filter, click **Filter Log**, then **Clear Filter (Show All)**. Events not selected from the **Filter By Severity** list never display in the filtered event log, even if the event occurs in a selected category from the **Filter by Category** list. Events not selected from the **Filter by Category** list never display in the filtered event log, even if devices in the category enter an alarm state selected from the **Filter by Severity** list.

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

- When the log is full, the older entries are deleted.
- To delete all events recorded in the log, click **Clear Log** on the Web page that displays the log. Deleted events cannot be retrieved.

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

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

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

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

Define, in the **Log Interval** setting, how frequently data is sampled and stored in the data log, and view the calculation of how many days of data the log can store, based on the interval you selected.

When the log is full, the older entries are deleted. To avoid automatic deletion of older data, enable and configure data log rotation, described in the next section.

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

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

Parameter	Description
Unique File Name	Add a date stamp prefix to the filename, using the format *MMDDYYY_filename.txt*. If updates occur more than once on the same day, the data is appended to the file created that day.
Delay *X* hours between uploads.	The number of hours between uploads of data to the file.
Upload every *X* minutes	The number of minutes between attempts to upload data to the file after an upload failure.
Up to *X* times	The maximum number of times the upload will be attempted after an initial failure.
Until Upload Succeeds	Attempt to upload the file until the transfer is completed.

To upload the file one time and then disable future uploads:

1. In the **Data Log Rotation** field, mark the **Enable** check box.
2. Click the **Upload Now!** button.
3. Clear the **Enable** check box.

Using FTP to retrieve log files

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

- The file reports all events or data recorded since the log was last deleted or (for the data log) truncated because it reached maximum size.
- The file includes information that the event log or data log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, and **Location** values and IP address of the 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 unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.

To use FTP to retrieve the files. 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 (**Administration>Network**) has been changed from its default (**21**), you must use the non-default value in the FTP command. See “FTP Server” on page 21. For Windows FTP clients, use the following command, including spaces: `ftp>open` ***`ip_address port_number`*** (For some FTP clients, a colon instead of a space is used between the IP address and the port number.)
2. Use the case-sensitive **User Name** and **Password** for Administrator or Device User to log on. For Administrator, **apc** is the default for **User Name** and **Password**. For the Device User, the defaults are **device** for **User Name** and **apc** for **Password**.
3. Use the **get** command to transmit the text of a log to your local drive.

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

   `ftp>`**`del event.txt`** **or** `ftp>`**`del data.txt`**

You will not be asked to confirm the deletion.

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

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

APC Device IP Configuration Wizard

The APC Device IP Configuration Wizard configures the IP address, subnet mask, and default gateway of one or more NMCs. You can use the Wizard in either of the following ways:

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

System requirements

The Wizard runs on Microsoft Windows 2000, Windows 2003, and Windows XP operating systems.

Installation

Install the Wizard from a downloaded executable file:

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

Launch the Wizard

The installation creates a shortcut link in the **Start** menu to launch the Wizard. Most software firewalls must be temporarily disabled for the Wizard to discover unconfigured NMCs.

The Upload Event

The following event occurs when the receiving NMC completes using the .ini file to update its settings.
`Configuration file upload complete, with` *`number`* `valid values`

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

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

Messages in config.ini

A device associated with the NMC from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the device is not present or is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values. 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. Because the overridden values are device-specific and not appropriate to export to other NMCs, ignore these error messages. To prevent these error messages, you can delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

File Transfers

Upgrading Firmware

Upgrade the firmware to obtain the latest bug fixes and performance improvements. Keep firmware versions consistent across your network.

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

The APC Operating System (AOS) and application module files used with the NMC share the same basic format: `apc_`*`hardware-version`*`_`*`type`*`_`*`firmware-version`*`.bin`

- `apc`: Indicates that this is an APC file.
- ***`hardware-version`*****:** `hw0`*`x`* identifies the version of the hardware on which you can use this binary file.
- ***`type`*****:** Identifies whether the file is for the APC Operating System (AOS) or the application module for the NMC.
- ***`version`*****:** The version number of the file.
- `bin`: Indicates that this is a binary file.

Obtain the latest firmware version

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

Manual upgrades, primarily for Linux systems. If no computer on your network is running a Microsoft Windows operating system, upgrade the firmware of your NMC by using the separate AOS and application firmware modules. Obtain the individual firmware modules by downloading the automated tool from **www.apcc.com/tools/download**, then extracting the firmware files from the tool. To extract the firmware files:

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

Firmware File Transfer

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

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

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

FTP. Use FTP to upgrade one NMC over the network.

- The NMC must be connected to the network, and its system IP, subnet mask, and default gateway must be configured.
- The FTP server must be enabled at the NMC.
- The firmware files must be extracted from the firmware upgrade tool.

To transfer the files:

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

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

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

   - `apc_hw03_aos_`***xxx***`.bin`
   - `apc_hw03_`**application_*xxx***`.bin`

2. Open an FTP client session: `C:\apc>`**ftp**
3. Type `open` and the NMC's IP address, and press ENTER. If the **port** setting for the FTP Server has changed from its default of **21**, you must use the non-default value in the FTP command.
   – For Windows FTP clients, separate a non-default port number from the IP address by a space. For example:
   ```
   ftp> open 150.250.6.10 21000
   ```
   – Some FTP clients require a colon instead before the port number.

4. Log on as Administrator (**apc** is the default user name and password).
5. Upgrade the AOS. In the example, *xxx* is the firmware version number:

```
ftp> bin
ftp> put apc_hw03_aos_xxx.bin
```

6. When FTP confirms the transfer, type **quit** to close the session.
7. After 20 seconds, repeat step 2 through step 6. In step 5, use the application module file name.

Verifying Upgrades and Updates

To verify a firmware upgrade succeeded, use the **Network** menu and select the **FTP Server** option to view **Last Transfer Result**, or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last Transfer Result codes.

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

Verify the version numbers of installed firmware.

Verify the versions of the upgraded firmware modules: **Administration** > **General** > **About**, or use an SNMP GET to the MIB II **sysDescr** OID.

APC Worldwide Customer Support

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

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

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

990-4697 **3/2012**