USER'S GUIDE

NetworkAIR FM

Contents

Web Interface 16

NetworkAIR FM Menus 22

Introduction

Product Description

Features of the NetworkAIR FM air conditioner

The APC NetworkAIR® FM air conditioner cools the data center environment. It uses a Network Management Card, which provides full management capabilities over a network using multiple open standards, such as HyperText Transfer Protocol (HTTP), Telnet, HyperText Transfer Protocol over Secure Sockets Layer (HTTPS), Simple Network Management Protocol (SNMP), File Transfer Protocol (FTP), and Secure CoPy (SCP). The NetworkAIR FM air conditioner provides the following features:

- Redundant Group control
- Temperature and humidity monitoring
- Input contact monitoring for use with dry contact sensors
- Output relay mapping and management
- Event log accessible by Telnet, FTP, serial connection, SSH (Secure SHell), or a Web browser
- SNMP traps and e-mail notifications sent based on the severity level of the events
- Syslog events sent to configured Syslog servers
- Security protocols for authentication and encryption

Initial setup

You must define the following three TCP/IP settings for the Network Management Card of the NetworkAIR FM air conditioner before it can operate on the network:

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

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

To configure the TCP/IP settings, see the NetworkAIR FM *Operation and Maintenance* manual, available on the APC NetworkAIR FM *Utility* CD and in printed form.

For detailed information on how to use a DHCP server to configure the TCP/IP settings at a Network Management Card, see TCP/IP and Communication Settings.

Network management features

These applications and utilities work with a NetworkAIR FM air conditioner that connects to the network through a Network Management Card.

- APC PowerNet® Management Information Base (MIB) with a standard MIB browser to perform SNMP SETs and GETs and to use SNMP traps.
- The APC Device IP Configuration Wizard to configure the basic settings of one or more NetworkAIR FM air conditioners over the network.
- The APC Security Wizard to create components needed for high security for the NetworkAIR FM air conditioner when you are 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 NetworkAIR FM air conditioner. You can also manage the NetworkAIR FM air conditioner through the SNMP interface by using an SNMP browser with the PowerNet® MIB.

For more information about the NetworkAIR FM air conditioner's user interfaces, see Web Interface and Control Console.

To use the PowerNet MIB with an SNMP browser, see the *PowerNet SNMP Management Information Base (MIB) Reference Guide*, provided on the APC NetworkAIR FM *Utility* CD.

Access priority for logging on

Only one user at a time can log on to the NetworkAIR FM air conditioner. 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 Network Management Card of the NetworkAIR FM air conditioner.
- Telnet or Secure SHell (SSH) access to the control console from a remote computer.
- Web access, either directly or through the InfraStruXure Manager.

See SNMP for information about how SNMP access to the NetworkAIR FM air conditioner is controlled.

Types of user accounts

The Network Management Card of the NetworkAIR FM air conditioner has four levels of access (Administrator, Device User, Read-Only User, and A/C Manager User), all of which are protected by user name and password requirements.

- An Administrator can use all of 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 **Group**, **System**, and **Module** tabs, and the event log, accessible under the **Events** heading on the left navigation menu of the **Logs** tab.
  - 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.

  - Access to the same tabs and menus as a Device User, but without the capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled, and the event log displays no button to clear the log.

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

- An A/C Manager User can access only the menus on the **Group**, **System**, and **Module** tabs, as well sd the event log, accessible under the **Events** heading on the left navigation menu of the **Logs** tab. The A/C Manager can also modify a subset of the settings relevant to the operation of the air conditioner, including the Proportional + Integral + Derivative (PID) control loops. The default user name is **acmanager**, and the default password is **apc**.

To set **User Name** and **Password** values for the Administrator, Device User, Read-Only User, and A/C Manager accounts, see Setting user access (Administration>Security>Local Users>options).

You must use the Web interface to configure values for the Read-Only User.

Recovering from a Lost Password

Use a local computer (a computer that connects to the Network Management Card of the NetworkAIR FM air conditioner through the serial port) to access the control console.

1. Select a serial port at the local computer and disable any service that uses that port.
2. Connect the configuration cable (provided with the NetworkAIR FM air conditioner) to the selected port on the computer and to the serial port at the NetworkAIR FM air conditioner (use connector J2 on the controller board, on the right side of the electrical panel).

3. Run a terminal program (such as HyperTerminal®) and configure the selected port for 2400 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 Network Management Card. The Status LED will flash between orange and green. Immediately press the **Reset** button on the Network Management Card a second time while the LED is flashing to reset the user name and password to their defaults temporarily.
6. Press ENTER as many times as necessary to redisplay the **User Name** prompt, 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. From the **Control Console** menu, select **System**, then **User Manager**.
8. Select **Administrator** and change the **User Name** and **Password** settings, both of which are now defined as **apc**. Select **Accept Changes** to store the new user name and password values.
9. Press CTRL+C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Network Management Card LEDs

Link-RX/TX (10/100) LED

The Link-RX/TX LED on the front of the Network Management Card indicates the network connection status of the card.

Condition	Description
Off	One of the following situations exist: • The Network Management Card is not receiving input power. • The Network Management Card is starting up. • The Network Management Card is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support.
Solid Green	The device is connected to a network operating at 10 Megabits per second (Mbps).
Solid Orange	The device is connected to a network operating at 100 Megabits per second (Mbps).
Flashing Green	The device is receiving or transmitting data packets at 10 Megabits per second (Mbps).
Flashing Orange	The device is receiving or transmitting data packets at 100 Megabits per second (Mbps).

Status LED

This LED indicates the network status of the Network Management Card.

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

1 If you do not use a BOOTP or DHCP server, see the NetworkAIR FM air conditioner*Operation and Maintenance* manual provided in printed format and in PDF on the APC NetworkAIR FM *Utility* CD to configure the TCP/IP settings of the Network Management Card.
2 To use a DHCP server, see TCP/IP and Communication Settings.

Watchdog Features

Overview

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

Network interface watchdog mechanism

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

Resetting the network timer

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

Control Console

How to Log On

Overview

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection with a computer on the same network (LAN) as the NetworkAIR FM air conditioner 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 Manager, which is the equivalent of Device User in the Web interface, or **acmanager** and **apc** for an AC Manager). A Read-Only User has no access the control console.

If you cannot remember your user name or password, see Recovering from a Lost Password.

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 automatically 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 Network Management Card of the NetworkAIR FM air conditioner, at a command prompt, type `telnet` and

the System IP address for the Network Management Card (for example, **`telnet 139.225.6.133`**, when the Network Management Card uses the default Telnet port of 23), and press ENTER.

If the Network Management Card uses a non-default port number (from 5000 to 32767), 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 Manager).

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

You can use a local computer that connects to the NetworkAIR FM air conditioner through the serial port on the controller board, which is on the electrical panel (connector J2) of the unit.

1. Select a serial port at the local computer, and disable any service which uses that port.
2. Use the supplied serial cable (940-0103) to connect the selected port to the serial port on the controller board, which is on the electrical panel (connector J2) of the NetworkAIR FM air conditioner.
3. Run a terminal program (such as HyperTerminal) and configure the selected port for 2400 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.
5. Enter your user name and password.

Main Screen

Example main screen

The following is an example of the screen that appears when you log on to the control console at the NetworkAIR FM air conditioner.

```
User Name : apc
Password  : ***


American Power Conversion               Network Management Card AOS vx.x.x
(c) Copyright 2007 All Rights Reserved  NetworkAIR FM APP           vx.x.x
-------------------------------------------------------------------------------
Name      : NetworkAIR FM                                Date : 07/29/2007
Contact   : Bill Cooper                                  Time : 10:16:58
Location  : Testing Lab                                  User : Administrator
Up Time   : 0 Days 0 Hours 43 Minutes                    Stat : P+ N+ A+

Communication Established
------- 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. The application firmware name identifies the type of device that connects to the network. In the preceding example, the application firmware for the NetworkAIR FM air conditioner is displayed.

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

- Three fields identify the system **Name**, **Contact**, and **Location** values. (In the control console, use the **System** menu to set these values.)

```
Name         : NetworkAIR FM
Contact      : Bill Cooper
Location     : Testing Lab
```

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

```
Up Time      : 0 Days 0 Hours 43 Minutes
```

- Two fields identify the most recent date and time the screen refreshed.

```
Date : 07/29/2007
Time : 10:16:58
```

- The **User** field identifies whether you logged on as Administrator, Device Manager, or A/C Manager. (The Read-Only User account cannot access the control console.)

```
User : Administrator
```

Main screen status fields.

- A **Stat** field reports the NetworkAIR FM air conditioner 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 Network Management Card failed to connect to the network.
N!	Another device is using the IP address of the Network Management Card.
A+	The application is functioning properly.
A–	The application has a bad checksum.
A?	The application is initializing.
A!	The application is not compatible with the AOS.

If the AOS status is not P+, contact APC Worldwide Customer Support, even if you can still access the NetworkAIR FM air conditioner.

NetworkAIR FM air conditioner status field.

The **Status** field displays the status of the NetworkAIR FM air conditioner. Under normal operation this field will read **Communication Established**.

Control Console Menus

Using the control console menus

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

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

- Type **?** and press ENTER to access brief menu option descriptions (if the menu has help available).
- Press ENTER to refresh the menu.
- Press ESC to return 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 the menus.
- Press CTRL+L to access the event log.

Control console structure

For menus not specific to the NetworkAIR FM air conditioner but shared among APC network-enabled devices, names and locations of options differ from those of the Web interface.

Main menu

Use the main control console menu to access the management features of the control console.

```
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

Use the options of the **Device Manager** menu to select the components to manage. For more information on these settings, see NetworkAIR FM Menus. For example:

```
1- Group
2- System
3- Module
4- Alarms
5- Display Interface Log
```

Network menu

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

- Configure the TCP/IP settings of the Network Management Card or, if the Network Management Card 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, the Web interface and SSL, SNMP, e-mail, DNS, and Syslog.

System menu

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

- Control **Administrator**, **A/C Manager User**, and **Device Manager** access. (You can control **Read-Only User** access by using the Web interface only.)
- Define the System **Name**, **Contact**, and **Location** values.
- Set the date and time used by the Network Management Card.
- Access System information about the Network Management Card.
- Define RADIUS access and set primary and secondary servers.
- Through the **Tools** option:
  - Restart the NetworkAIR FM air conditioner 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 the Network Management Card of another NetworkAIR FM air conditioner. The current Network Management Card then uses the values in that .ini file to configure its own settings.

Web Interface

Introduction

Overview

The Web interface provides options to manage one or more NetworkAIR FM air conditioners.

See Web (Administration>Network>Web>options) for information on how to select, enable, and disable the protocols that control access to the Web interface and to define the Web-server ports for the protocols.

Supported Web browsers

You can use Microsoft® Internet Explorer (IE) 5.5 and higher (on Windows operating systems only), Firefox, version 1.x, by Mozilla Corporation (on all operating systems), or Netscape® 7.x and higher (on all operating systems) to access the NetworkAIR FM air conditioner through its Web interface. Other commonly available browsers may work but have not been fully tested by APC.

The NetworkAIR FM air conditioner cannot work with a proxy server. Therefore, before you can use a Web browser to access NetworkAIR FM air conditioner's Web interface, you must do one of the following:

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

How to Log On

Overview

You can use a NetworkAIR FM air conditioner's DNS name or System IP address for the URL address of the Web interface. Use your case-sensitive user name and password to log on. The default user name differs by account type:

- **apc** for an Administrator
- **device** for a Device User
- **readonly** for a Read-Only User
- **acmanager** for an A/C Manager User

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

If you are using HTTPS as your access protocol, your login 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 NetworkAIR FM air conditioner. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

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

URL address formats

Type the NetworkAIR FM air conditioner's DNS name or IP address 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 login.

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

URL format examples.

- For a DNS name of Web1:
  - **`http://Web1`** if HTTP is your access mode.
  - **`https://Web1`** if HTTPS (HTTP with SSL) is your access mode.
- For a System IP address of 139.225.6.133 and the default Web server port (80):
  - **`http://139.225.6.133`** if HTTP is your access mode.
  - **`https://139.225.6.133`** if HTTPS (HTTP with SSL) is your access mode.
- For a System IP address of 139.225.6.133 and a non-default Web server port (5000):
  - **`http://139.225.6.133:5000`** if HTTP is your access mode.
  - **`https://139.225.6.133:5000`** if HTTPS (HTTP with SSL) is your access mode.

Home Page

Overview

On the **Home** page of the interface, displayed when you log on, you can view active Group-, System-, and Module-level alarm conditions, the status of the System, and the most recent device events.

Quick status icons

At the upper right corner of every page, one or more icons and accompanying text indicate the current operating status of the NetworkAIR FM air conditioner:

- The **Normal** icon if no alarms exist.
- One or both of the other icons (**Critical** and **Warning)** if any alarms exist, and after each icon, the number of active alarms of that severity.

	**Critical**: A critical alarm exists, which requires immediate action.
	**Warning**: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
	**Normal**: No alarms are present, and the NetworkAIR FM air conditioner is operating normally.

To return to the **Home** page to view its summary of Group, System, and Module status, including the active alarms, click a quick status icon on any page of the interface.

Recent Device Events

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

How to Use the Tabs, Menus, and Links

Tabs

In addition to the tab for the **Home** page, the following tabs are displayed. Click a tab to display a set of menu options:

- **Group**: Assign the System roles, configure Group settings such as the number of Systems in the Group and shutdown events, enable or disable demand fighting and load-sharing, reset Group field service settings, and configure load-sharing properties for each mode of operation (e.g., cooling or reheat).
- **System**: View the status of the System, and view the role of this System in the redundant Group (if applicable). View the System's run hours, the temperature and humidity in the space being cooled, and details and demands for each mode of operation. Configure settings for each mode of operation. Configure input contacts, output relays, and alarm thresholds. Configure start-up actions, select System-level and Module-level events that will cause a System to enter a failure state, and reset System field service settings.
- **Modules**: View each Module's run hours, the temperature and humidity in the space being cooled, and details and demands for each mode of operation.
- **Logs**: View and configure event and data logs.
- **Administration**: Configure security, network connection, notification, and general settings.

Menus

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

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

Top menu bar. The **Home** and **Administration** tabs have a selection of menu options on the top menu bar. Select one of the menu options to display its left navigation menu.

Quick Links

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

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

To reconfigure the links, see Configuring Links (Administration>General>Quick Links)

NetworkAIR FM Menus

Group Tab

Group System Assignment

Web interface. For each System that is a member of the redundant Group, the **System Status** section lists the following:

- Status
- Role
- Run hours
- Communications
- IP address

Click an IP address for a System to open its Web interface.

The **System Assignment** section lists the active Role Assignment Method for this Group.

- To set the System Assignments and Role Assignment Method, click **Configure** (at the lower right).
- For **Dynamic (Automatic Run Hour Balancing)**, set the number of Systems in your Group that will be on-line at all times. The Group controller will then rotate the backup Systems to keep the run hours balanced across the Group.
- For **Static (Manually Assigned Roles)** only, set each System to either **Primary** or **Backup**. This step is unnecessary if you select **Dynamic (Automatic Run Hour Balancing)**.
- After selecting the settings, click **Apply**.

Control console. The **System Assignments** screen in the control console lists the same status information as the Web interface. From the control console menu, select **Device Manager**, then **Group**, and then **System Assignments**.

Enter the number of the option you want to modify, and press ENTER.

- If you choose **Dynamic (Automatic Run Hour Balancing)** for your Role Assignment Method, set option 2 — **Number of Primary Systems**.
- If you choose **Static (Manually Assigned Roles)** for your Role Assignment Method, set options 3 through 6 — **System Role** for each System in the Group.

Choose **Accept Changes**, when you finish modifying settings.

Group General Configuration

Web interface. The **General Settings** section lists properties that can be modified for the Group. Click **Configure** to make changes, and click **Apply**.

In the **Load Sharing** section, enable or disable requests for each mode, and set the value of the threshold at which the Group controller will generate a load-sharing request. Click **Apply**.

In the **Reset Group Defaults**, check the Reset Field Service Defaults box to reset the values for all Group settings that can be modified by a Field Service Engineer. Click **Apply**.

Control console. The **General Settings** option lists properties that can be modified for the Group. From the control console menu, select **Device Manager**, then **Group**, and then **General Configuration**. Enter the number of the selection to change and press ENTER. When you finish making changes, select **Accept Changes**, then press ESC to return to the **General Configuration** menu.

Choose the **Load Sharing** option of the **General Configuration** menu to enable or disable load-sharing requests, and to set the value of the threshold at which the Group controller will generate a load-sharing request for each mode. When you finish making changes, select **Accept Changes**, then press ESC to return to the **General Configuration** menu.

Select the **Reset Group Field Service Defaults** option of the **General Configuration** menu to reset the values for all Group settings that can be modified by a Field Service Engineer. At the prompt, enter Y to reset the values or ESC to exit.

System Tab

General

Web interface. The **General** screen of the Web interface lists properties that are either System-level or common to each Module in the System. From the navigation menu, select **System**, and then **General**.

The **Configuration** section of the **General** screen lists delays, the **Fast Startup** setting, which is applicable only to certain installations, and options for using data from environmental sensors.

- Primary Sensor Selection
- Remote Sensor Data
- Start-up Delay
- Mode Delay
- Communication Loss Shutdown Delay
- Fast Startup

The **Identification** section allows you to define contact information for this device.

- Name
- Contact
- Location

Control console. From the control console menu, select **Device Manager**, then **System**, and then **General**.

The **General** screen of the control console provides three options.

- Status
- Demands & Actuals
- Configuration

The **Status** option displays the following:

- The temperature and humidity
- The sensor and method used to calculate the control temperature and humidity
- The setpoints and mode status for each mode

```
------- Status ---------------------------------------------------------------
 System is ON

                Status          Role            Run Hours
 System:        On Line         Primary         662

                Avg. Return     Avg. Remote     High Remote     Low Remote
 Temperature:   22.8 C, 73.0 F  25.8 C, 78.4 F  32.8 C, 91.0 F  20.6 C, 69.0 F
 Humidity:      52.9% RH         44.5% RH

                Cool            Reheat          Humidify        Dehumidify
 Mode Status:   Disabled        Enabled         Enabled         Enabled
 Setpoint:      22.7 C, 72.9 F  22.1 C, 71.8 F  45.2% RH        63.1% RH

 Control Method:                Return (Average Temperature & Humidity)
 Coil Fluid Temperature:        20.0 C, 55.3 F


<ESC>- Back, <ENTER>- Refresh, <CTRL-L>- Event Log

>
```

The **Demands & Actuals** option displays the demanded and actual output for each mode.

```
------- Demands & Actuals ---------------------------------------------------

                                        Demands & Actuals
 DX Cooling Demand                      50 %
 DX Dehumid Demand                      50 %
 Actual DX Cool/Dehumid                 25 %

 Coil Fluid Cooling Demand              50 %
 Coil Fluid Dehumid Demand               0 %
 Actual Coil Fluid Cooling              50 %

 Electric Reheating Demand              43 %
 Steam/Hot Water/Hot Gas Reheating      On

 Humidification Demand                  27 %
 Actual Humidification                  51 %

<ESC>- Back, <ENTER>- Refresh, <CTRL-L>- Event Log
>
```

The **Configuration** option provides three menus.

- Properties
- Timing
- Identification

The **Properties** menu lists properties that are either System-level or common to each Module in the System. Options throughout the Web interface are dependent on these settings; for example, the interface displays different cooling settings depending on whether **Coil Configuration** is set to **DX** or **Chilled Water**.

The **Timing** menu lists delays and the Fast Start-up setting, which is applicable only to certain installations.

- Start-up delay
- Mode delay
- Communication loss shutdown delay
- Fast Start-up

The **Identification** menu allows you to define contact information for this device.

- Name
- Contact
- Location

Cooling

Web interface. From the navigation menu, select **System**, and then **Cooling** to access the **Cooling** screen.

Control console. From the **Device Manager** menu, select **System**, **Cooling**, and then **Control** or **Timing**.

Use the **Control** section to set up the cool mode. Enter a setpoint and deadband, enable the mode, and designate it as an essential or nonessential function.

The Proportional + Integral + Derivative (PID) control loop is used to control the cool mode for MultiCool, Chilled Water, and Economizer-equipped Modules.

The loops must be tuned after the room load is in place, and then periodically if the room load changes. Only a qualified service technician should perform PID tuning.

Use the **Timing** menu to set the timers, rotation periods, and delays related to cooling. The available delays vary, depending on the configuration of your System. To access the **Timing** menu, select **Device Manager**, then **System**, then **Cooling**.

Humidity Control

The **Humidify**, **Dehumidify**, and **Reheat** sections control each of these modes. Select **Configure** to enter setpoints and deadbands, enable the modes, and designate them as essential or nonessential functions.

The following settings are specific to each indicated mode:

- **Configured Humidity Control Method** — Set the System to use either the relative humidity or the dew point of the air at the selected control sensors for the humidify and dehumidify modes.

  The **Humidity Control Method** will be set to **Dew Point** automatically if the System is part of a Redundant Group or is using the remote sensors as the primary sensors.

- **Proportional Control Sensitivity Band** — Set the humidifier to output at 100% capacity when the relative humidity in the room drops this number of percentage points below the setpoint.
- **Capacity** — Set the dehumidify mode to use either the full capacity of the compressors and coil for dehumidification, or to use half of their capacity.
- **PID Control** — Tune the Proportional + Integral + Derivative (PID) control loop for each mode. PID controls are available for the reheat and dehumidify modes, depending on the System configuration.

  The loops must be tuned after the room load is in place, and then periodically if the room load changes. Only a qualified service technician should perform PID tuning.

Inputs/Outputs

Input Contact Configuration (Web interface). You can name and assign a behavior to each input contact. The settings for each input contact include:

- Name
- Normal State
- Delay
- Action

From the **System** menu, select **Inputs/Outputs**, then click the **Configure** button under **Input Contacts Status**. After you modify any input contacts, click the **Apply** button below the last contact.

Input Contact Configuration (control console). From the **Device Manager** menu, select **System**, then select **PCIOM**, and then **Input Contacts**. Enter the number of the input contact you want to modify. The settings for each input contact are the same as for the Web interface. Select **Accept Changes** after you finish.

You can assign the following actions to an input contact. When the input contact changes state, the controller performs the assigned action.

Action Name	Description
Status Only	Displays a status event in the event log.
Major Alarm	Activates a major alarm condition.
Minor Alarm	Activates a minor alarm condition.
Remote Run/Stop	Shuts down (or starts up) the System normally, observing all of the System and Module delays.
Nonessential Stop	Disables the modes marked as nonessential, but allows essential modes to continue to operate.
Immediate Shutdown	Removes power from the System without waiting for the normal delays to expire.

Output Relay Configuration (Web interface). From the **System** menu, select **Inputs/Outputs**, then click the **Configure** button under **Output Relay Configuration**.

Output Relay Configuration (control console). From the **Device Manager** menu, select **System**, then select **PCIOM**, then **Output Relays**.

Set each output relay to either normally **Open** or normally **Closed**. After you modify output relays, select **Apply** (Web interface) or **Accept Changes** (control console) to save your changes.

See Output Mapping for a list of events, alarms, contacts, and relays that you can map to each output relay.

Output Mapping

Events, alarms, input contacts, and other output relays can all be mapped to an output relay. The output mapping screen allows you to manage these mapped events for each available relay.

A maximum of 150 mappings between events and output relays are available to the System. These 150 mappings do not include mapping from input contacts to output relays and from output relays to output relays.

Web interface. From the navigation menu, select **System** and then **Output Mapping**. The Web interface lists output mapping in a table, with event types as rows and available relays as columns. The cell at the intersection of a row and column contains the number of the relay to which you are mapping the event. To make changes, click **Configure** and enter the numbers of the outputs to which to map this event. Click **Apply**.

Cell Code	Definition
–	The event type is not mapped to this relay.
Number	The event type is mapped to this relay.

Control console. The control console lists event types by category. From the **Device Manager** menu, select **System**, then **PCIOM**, and then **Output Relay Mapping** to display the following categories:

- Input Contact Events
- Output Relay Events
- System Events
- Main Module Events
- Expansion Module 1 Events (if installed)
- Expansion Module 2 Events (if installed)

Select a category and then an event type. Enter the numbers of all contacts to which to map this event, separated by commas. Select **Accept Changes**.

System events.

System Event Type	Description
Any Alarm	An alarm is active for this System.
System On	The System has power and is operating.
System Off-line	The System is in a fail-over state.
High Environmental Temperature	The environmental temperature reported to the System is above the alarm threshold.
Low Environmental Temperature	The environmental temperature reported to the System is below the alarm threshold.
High Environmental Humidity	The environmental humidity measured by the System is above the alarm threshold.
Low Environmental Humidity	The environmental humidity measured by the System is below the alarm threshold.
Fire Detected	The System has detected a fire or high temperature within a Module.
Smoke Detected	The System has detected smoke within a Module.
Econ Isolator	The Economizer coolant isolation valve is open (if this System is equipped with the Econ isolator).
Supply Sensor Failure	The temperature and humidity probe that measures the air leaving the System has failed.
Return Sensor Failure	The temperature and humidity probe that measures the air entering the System has failed.
Remote Sensor Removed	The remote temperature and humidity probe has been removed from the CAN bus.
Primary Sensors Failed	The primary string of temperature and humidity sensors for the System has failed.

System Event Type	Description
Secondary Sensors Failed	The secondary string of temperature and humidity sensors for the System has failed.
Secondary Sensors Active	The secondary string of temperature and humidity sensors for the System is active.

Module events.

Module Event Type	Description
Any Alarm	An alarm is active for this System.
Maintenance Required	A component of the Module is above the recommended number of run hours.
Cooling Failure	The cool mode cannot operate because of a failure. Check the event log for a specific alarm.
High Supply Temperature	The supply temperature is above the temperature threshold.
Low Supply Temperature	The supply temperature is below the temperature threshold.
Humidifier Failure	The humidifier has failed.
Humidifier Replace Cylinder	The humidifier cylinder must be replaced.
Condensate Pump Failure	The condensate pump has failed.
Blower Controller 1 Failure	The controller for Blower 1 has failed.
Blower Controller 2 Failure	The controller for Blower 2 has failed.
High Filter Differential Pressure	The air filter is clogged.

Module Event Type	Description
Low Air Flow	Air flow through the Module is insufficient to maintain normal operation.
Air Block Interlock Open	The air block is not properly secured.
Water Detected	The Module has detected water at the leak sensor.

Input contact events. You can map each available input contact to an output relay.

Output relay events. You can map each available output relay to another output relay.

Shutdown events

Enable or disable one or more events from a list of the events that will cause this system to shut down.

Any of the following System-level events can be set to cause the System to shut down.

- Any Minor Alarm
- Any Major Alarm
- High Environmental Temperature
- Low Environmental Temperature
- High Environmental Humidity
- Low Environmental Humidity
- Fire Alarm
- Smoke Alarm
- Communications Lost
- Supply Sensor Failure
- Return Sensor Failure
- Primary Sensor Failure
- Secondary Sensor Failure
- No Sensors Available

Any of the following Module-level events can be set to cause the System to shut down.

- Maintenance Required
- Cooling Failure
- Humidifier Failure
- Blower Controller 1 Failure
- Blower Controller 2 Failure
- High Filter Differential Pressure
- High Supply Temperature
- Low Supply Temperature
- Loss Or Low Air flow
- Humidifier Replace Cylinder
- Air Block Interlock Open
- Water Detected
- Condensate Pump Failure

Web interface. Select **System**, then **Shutdown Events**. Click **Configure** and enable or disable each event by marking its checkbox. When you finish, click **Apply**.

Control console. The control console lists event types by category. From the **Device Manager** menu, select **System**, then **Shutdown Events**, and then either **System-Level** or **Module-Level** to display the events. When you finish, select **Accept Changes**.

Reset Control

In both the Web interface and the control console, you can reset failures and change settings back to their default values.

Web interface. Select **Reset Control** under the System menu to reset failures, run hours, and settings to their default values.

Control console. From the control console menu, select **Device Manager**, then **System**, and then **Reset Control.**

Reset Option	Action Taken
Reset System Failure	Reset a System after a failure. If you do not reset the alarm or event that caused the failure, the System will fail again, until the alarm or event is cleared.
Reset System User Defaults	Reset the user-level settings to their default values.
Reset System Field Service Defaults	Reset the field service-level settings to their default values.
Reset System Run Hours	Reset the run hours for this System.

Run hours and maintenance alarms are reset in the **Module** menu, under **Status**. Select **Reset Maintenance Alarms or Run Hours** to navigate to the screen.

In the control console, the **Select Run Hours to Reset** and **Select Maintenance Alarms to Clear** options are under **Run Hours** on the **General Status** screen of the **Module** menu.

Modules Tab

Status

The **Status** field of the **Modules** menu provides the following information for the various components of the Modules in the System:

- Temperature
- Humidity
- Pressures
- Run hours

Web interface. To reset the run hours for a component to zero, or to reset a maintenance interval alarm, select **Reset Maintenance Alarms or Run Hours** from the bottom right of the screen. Select a reset option from the drop-down menu, and then set the components in each Module to reset. Click **Apply** to reset. It is also possible to reset maintenance alarms or run hours for components listed in the **Cooling**, **Humidity Control**, and **Blowers** menus.

Control console. To reset the run hours for a component to zero, or to reset a maintenance interval alarm, select **Device Manager** from the control console menu, then **Module**, then **General Status**, and then **Run Hours**. Select a reset option and then enter a letter (found next to each component on the screen) for each value you want to reset. Press ENTER to reset those values.

Properties

The **Properties** field of the **Modules** menu provides the following information for the various components of the Modules in the System:

- Module configuration
- Blower frequency
- Alarm detectors
- Module identification

Cooling

Chilled water Systems do not display compressor data.

The **Cooling** field of the **Modules** menu provides the following information for the various components of the Modules in the System:

- Compressor status
- Compressor pressures
- Compressor run hours
- Fluid valve positions, in % Open (if applicable)

Humidity Control

The **Humidity Control** field of the **Modules** menu provides the following information for the various components of the Modules in the System:

- Humidifier status
- Reheat type
- Humidifier and heater run hours
- Humidifier mode (can be modified from this screen)

Blowers

The **Blowers** field of the **Modules** menu provides the following information for the various components of the Modules in the System:

- Blower status
- Blower and blower controller run hours

Alarms

Status

The **Alarm Status** screen displays the active alarms for the Group, the System and for each Module in the System.

The **Severity**, **Date**, **Time**, and **Description** fields display information for each active alarm.

The **Clear Active System and Module Alarms** field enables you to reset active System and Module alarms. If the underlying cause of the alarm is not cleared, the alarm will occur again.

- Web interface — Mark the **Clear Active Systems and Module Alarms** checkbox. This option is at the bottom of the **Status** screen of the **Alarms** menu.
- Control console — Select **Device Manager**, and then select **Clear Active System and Module Alarms** from the **Alarms** menu.

The **Clear Active Group Alarms** field enables you to reset active Group alarms. If the underlying cause of the alarm is not cleared, the alarm will occur again.

- Web interface — Mark the **Clear Active Group Alarms** checkbox. This option is at the bottom of the **Status** screen of the **Alarms** menu.
- Control console — Select **Device Manager**, and then select **Clear Active Group Alarms** from the **Alarms** menu.

Configuration

Use the **Configuration** screen to set the temperature run hour delays and thresholds, humidity run hour delays and thresholds, and maintenance intervals (in hours).

Web interface. The temperature and humidity run hour delays and thresholds are all displayed on the same page. Click the **Configure** button to modify any of the settings on this page, and click **Apply** when you finish.

Control console. Select **Device Manager**, then select **Configuration** from the **Alarms** menu.

Temperature Setting	Description
Alarm Delay	Set the amount of time the blower must be on before a humidity alarm can be issued.
Supply High Threshold	Set the high temperature threshold for the air at the supply temperature sensor.
Supply Low Threshold	Set the low temperature threshold for the air at the supply temperature sensor.
Control High Threshold	Set the high temperature threshold for the air at the sensor being used to control the air conditioner.
Control Low Threshold	Set the low temperature threshold for the air at the sensor being used to control the air conditioner.
Coil Fluid High	Set the high temperature threshold for coolant at the inlet to the fluid coil.
Coil Fluid Low	Set the low temperature threshold for coolant at the inlet to the fluid coil.

Humidity Setting	Description
Alarm Delay	Set the amount of time the blower must be on before a humidity alarm can be issued.
Control High Threshold	Set the high humidity threshold for the air at the sensor being used to control the air conditioner.
Control Low Threshold	Set the low humidity threshold for the air at the sensor being used to control the air conditioner.

Maintenance Intervals

For each of the following components, set the number of hours you want the component to run before the System generates an alarm. Click **Apply** when you finish.

- Compressor 1
- Compressor 2
- Heater
- Humidifier
- Blower 1
- Blower 2
- Blower Controller 1
- Blower Controller 2

Administration: Security

Local Users

Setting user access (Administration>Security>Local Users>*options*)

You set the case-sensitive user name and password for each account type in the same manner. Maximum length is 10 characters for a user name and 32 characters for a password. Blank passwords (passwords with no characters) are not allowed.

For information on the permissions granted to each account type (Administrator, Device User, Read-Only User, and A/C Manager User), see Types of user accounts.

Account Type	Default User Name	Default Password	Permitted Access
Administrator	apc	apc	Web Interface and Control Console
Device User	device	apc	
Read-Only User	readonly	apc	Web Interface only
A/C Manager User	acmanager	apc	Web Interface (when basic authentication is selected), and Control Console

Remote Users

Authentication (Administration>Security>Remote Users>Authentication Method)

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

For information about local authentication (not using the centralized authentication of a RADIUS server), see the *Security Handbook,* available on the *Utility* CD and on the APC Web site at **www.apc.com**.

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

- When a user accesses the Network Management Card or another network-enabled device that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user's permission level.
- RADIUS user names used with the Network Management Card are limited to 32 characters.

Select one of the following:

- **Local Authentication Only**: RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Authentication**: RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server is unavailable, local authentication is used.
- **RADIUS Only**: RADIUS is enabled. Local authentication is disabled.

If **RADIUS Only** is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, you must use a serial connection to the control console and change the **Access** setting to **Local Authentication Only** or **RADIUS, then Local Authentication** to regain access.

RADIUS (Administration>Security>Remote Users>RADIUS)

Use this option to do the following:

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

RADIUS Setting	Definition
RADIUS Server	The server name or IP address of the RADIUS server. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.
Secret	The shared secret between the RADIUS server and the Network Management Card.
Timeout	The time in seconds that the Network Management Card waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path.
Switch Server Priority	Change which RADIUS server will authenticate users if two configured servers are listed and **RADIUS, then Local Authentication** or **RADIUS Only** is the enabled authentication method.

Configuring the RADIUS Server

Summary of the configuration procedure

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

For examples of the RADIUS users file with Vendor Specific Attributes (VSAs) and an example of an entry in the dictionary file on the RADIUS server, see the APC *Security Handbook*.

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

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

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

Configuring a RADIUS server on UNIX® with shadow passwords

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

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

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

- Add user names and attributes to the RADIUS "user" file, and verify 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

APC supports FreeRADIUS and Microsoft Windows IAS Server. Other commonly available RADIUS applications may work but have not been fully tested by APC.

Inactivity Timeout (Administration>Security>Auto Log Off)

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

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

Administration: Network Features

TCP/IP and Communication Settings

TCP/IP settings (Administration>Network>TCP/IP)

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

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

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

Setting	Description
Manual	The IP address, subnet mask, and default gateway must be configured manually. Click **Next>>**, and enter the new values.
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Network Management Card requests network assignment from any BOOTP server: • If it receives a valid response, it starts the network services. • If it finds a BOOTP server, but a request to that server fails or times out, the Network Management Card stops requesting network settings until it is restarted. • By default, If previously configured network settings exist, and it receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible. Click **Next>>** to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail [1]: • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. • **If retries fail**: Select **Use prior settings** (the default) or **Stop BOOTP request**.
DHCP	At 32-second intervals, the Network Management Card requests network assignment from any DHCP server. By default, the number of retries is unlimited. • If it receives a valid response, by default it requires the APC cookie from the DHCP server in order to accept the lease and start the network services. • If it finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted. To change these values, click **Next>>** for the **DHCP Configuration** page[1]: • **Require vendor specific cookie to accept DHCP Address**: Disable or enable the requirement that the DHCP server provide the APC cookie. • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.

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

Setting	Description
DHCP & BOOTP	The default setting. The Network Management Card tries to obtain its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server. If it obtains its TCP/IP settings from either server, it switches this setting to **BOOTP** or **DHCP**, depending on the type of server that supplied the TCP/IP settings to the Network Management Card. Click **Next>>** to configure the same settings that are on the **BOOTP Configuration** and **DHCP Configuration** pages[1] and to specify that the **DHCP and BOOTP** setting be retained after either type of 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 Network Management Card, which uniquely identifies it on the local area network (LAN)
   - **User Class**: The name of the application firmware module

DHCP response options

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

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

- **APC Cookie. Tag 1, Len 4, Data "1APC"**
  Option 43 communicates to the Network Management Card that a DHCP server is configured to service APC devices. By default, this DHCP response option must contain the APC cookie for the Network Management Card to accept the lease.

To disable the requirement of an APC cookie, see DHCP.

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

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

- **Boot Mode Transition. Tag 2, Len 1, Data 1/2**
  This option 43 setting enables or disables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**, which, by default, is disabled.
  - A data value of 1 enables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. Whenever the Network Management Card reboots, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.
  - A data value of 2 disables the **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** option. The **TCP/IP Configuration** setting option switches to **DHCP** when the Network Management Card accepts the DHCP response. Whenever the Network Management Card reboots, it will request its network assignment from a DHCP server only.

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

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

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

- **IP Address** (from the **yiaddr** field of the DHCP response, described in **RFC2131)**: The IP address that the DHCP server is leasing to the Network Management Card.
- **Subnet Mask** (option 1): The Subnet Mask value that the Network Management Card needs to operate on the network.
- **Router,** i.e., Default Gateway (option 3): The default gateway address that the Network Management Card needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the Network Management Card.

- **Renewal Time, T1** (option 58): The time that the Network Management Card must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): The time that the Network Management Card must wait after an IP address lease is assigned before it can seek to rebind that lease.

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

- **Network Time Protocol Servers** (option 42): Up to two NTP servers (primary and secondary) that the Network Management Card can use.
- **Time Offset** (option 2): The offset of the Network Management Card's subnet, in seconds, from Coordinated Universal Time (UTC).
- **Domain Name Server** (option 6): Up to two Domain Name System (DNS) servers (primary and secondary) that the Network Management Card can use.
- **Host Name** (option 12): The host name that the Network Management Card will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the Network Management Card will use (64-character maximum length).
- **Boot File Name** (from the **file** field of the DHCP response, described in **RFC2131**): The fully qualified directory-path to an user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the Network Management Card will download the .ini file. After the download, the Network Management Card uses the .ini file as a boot file to reconfigure its settings.

Port Speed (Administration>Network>Port Speed)

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

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

DNS (Administration>Network>DNS>*options*)

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

- Select **servers** to specify the IP addresses of the primary and optional secondary DNS server. For the Network Management Card to send e-mail, at least the IP address of the primary DNS server must be defined.
  - The Network Management Card waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the Network Management Card does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the Network Management Card or on a nearby segment (but not across a wide-area network [WAN]).
  - After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for that computer.
- Select **naming** to define the host name and domain name of the Network Management Card:
  - **Host Name**: After you configure a host name here and a domain name in the **Domain Name** field, users can enter a host name in any field in the Network Management Card interface (except e-mail addresses) that accepts a domain name.

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

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

Query Type Selected	Query Question to Use
by Host	The URL
by FQDN	The fully qualified domain name, *`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 (Administration>Network>Web>*options*)

Option	Description

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

Option	Description
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** (enabled by default): A stream cipher that provides authentication by MD5 hash algorithm. • **RC4_SHA** (enabled by default): A stream cipher that provides authentication by Secure Hash Algorithm. • **3DES**: A block cipher that provides authentication by Secure Hash Algorithm.
ssl certificate	Add, replace, or remove a security certificate. **Status**: • **Not installed**: A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Using **Add or Replace Certificate File** installs the certificate to the correct location, **/sec** on the Network Management Card. • **Generating**: The Network Management Card is generating a certificate because no valid certificate was found. • **Loading**: A certificate is being activated on the Network Management Card. • **Valid certificate**: A valid certificate was installed or was generated by the Network Management Card. Click on this link to view the certificate's contents. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the Management Card generates a default certificate, a process which delays access to the interface for up to five minutes.** You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on. **Add or Replace Certificate File**: Enter or browse to the certificate file created with the Security Wizard. See "Creating and Installing Digital Certificates" in the *Security Handbook* on the APC NetworkAIR FM *Utility* CD to choose a method for using digital certificates created by the Security Wizard or generated by the Network Management Card. **Remove**: Delete the current certificate.

Console (Administration>Network>Console>*options*)

Option	Description

access	Choose one of the following for access by Telnet or Secure SHell (SSH):
	• **Disable**: Disables all access to the control console.
	• **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**: SSH version 1 encrypts user names, passwords, and data for transmission. There is little or no delay as you log on.
	• **Enable SSH v2 only**: SSH version 2 transmits user names, passwords, and data in encrypted form with more protection than version 1 from attempts to intercept, forge, or alter data during transmission. There is a noticeable delay as you log on.
	
	Configure the ports to be used by these protocols:
	• **Telnet Port**: The Telnet port used to communicate with the Network Management Card (23 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) or a space, as required by your Telnet client program, to specify the non-default port. For example, for port 5000 and an IP address of 152.214.12.114, your Telnet client requires one of the these commands:
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• **SSH Port**: The SSH port used to communicate with the Network Management Card (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port.

ssh encryption	Enable or disable encryption algorithms (block ciphers) 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 enabled 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**)

Option	Description
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 Network Management Card is creating a host key because no valid host key was found. • **Loading**: A host key is being activated on the Network Management Card. • **Valid**: One of the following valid host keys is in the **/sec** directory (the required location on the Network Management Card): •A 1024-bit host key created by the APC Security Wizard •A 768-bit RSA host key generated by the Network Management Card **Add or Replace**: Browse to and upload a host key file created by the Security Wizard: If you use FTP or Secure CoPy (SCP) instead to transfer the host key file, you must specify the **/sec** directory as the target location in the command. To use the APC Security Wizard, see the *Security Handbook* on the APC NetworkAIR FM *Utility* CD. **NOTE:** To reduce the time required to enable SSH, create and upload a host key in advance. **If you enable SSH with no host key loaded, the Management Card takes up to 5 minutes to create a host key, and the SSH server is not accessible during that time.** **Remove**: Remove the current host key.

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

SNMPv1 (Administration>Network>SNMPv1>*options*)

All user names, passwords, and community names for SNMP are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMP access or set the access for each community to Read. (A community with Read access can receive status information and use SNMP traps.)

When using InfraStruXure Manager to manage the NetworkAIR FM air conditioner on the public network of an InfraStruXure system, you must have SNMP enabled in the Network Management Card interface. Read access will allow InfraStruXure Manager to receive traps from the Network Management Card of the NetworkAIR FM air conditioner, but Write access is required while you use the interface of the Network Management Card to set InfraStruXure Manager as a trap receiver.

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

Option	Description
access	**Enable SNMPv1 Access:** Enables SNMP version 1 as a method of communication with this device.
access control	You can configure up to four access control entries to specify which Network Management System (NMSs) have access to this device. The opening page for access control, by default, assigns one entry to each of the four available SNMPv1 communities, but you can edit these settings to apply more than one entry to any community to grant access by several specific IP addresses, host names, or IP address masks. To edit the access control settings for a community, click its community name. • If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network. • If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device. **Community Name:** The name that a NMS must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are **`public`**, **`private`**, **`public2`**, and **`private2`**. **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows: • 149.225.12.255: Access only by an NMS on the 149.225.12 segment. • 149.225.255.255: Access only by an NMS on the 149.225 segment. • 149.255.255.255: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. **Access Type**: The actions an NMS can perform through the community. • **Read**: GETS only, at any time • **Write**: GETS at any time, and SETS when no user is logged onto the Web interface or Control Console. • **Write+**: GETS and SETS at any time. • **Disabled**: No GETS or SETS at any time.

SNMPv3 (Administration>Network>SNMPv3>*options*)

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

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

The Network Management Card supports only MD5 authentication and DES encryption.

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

Option	Description
access control	You can configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles, but you can edit these settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks. • If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device. • If you configure multiple access entries for one user profile, the limit of four entries requires that one or more of the other user profiles must have no access control entry. If no access control entry is listed for a user profile, no NMS that uses that profile has any access to this device. To edit the access control settings for a user profile, click its user name. **Access:** Mark the **Enable** checkbox to activate the access control specified by the parameters in this access control entry. **User Name:** Select from the drop-down list the user profile to which this access control entry will apply. The choices available are the four user names that you configure through the **user profiles** option on the left navigation menu. **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. An IP address mask that 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 (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 Network Management Card. The FTP server uses both the specified port and the port one number lower than the specified port.

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

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 detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available on the APC NetworkAIR FM *Utility* CD or from the APC Web site.

Administration: Notification and Logging

Event Actions (Administration>Notification>Event Actions>*options*)

Types of notification

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

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

For another method of indirect notification, see SNMP. SNMP enables an NMS to perform informational queries. For SNMPv1, configuring the most restrictive SNMP access type, READ, enables informational queries without the risk of allowing remote configuration changes.

You can also log system performance data to use for device monitoring. See Data log (Logs>Data>options) for information on how to configure and use this data logging option.

Configuring event actions

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

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

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

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

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

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

- Identifying Syslog Servers (Logs>Syslog>servers)
- E-mail recipients (Administration>Notification>E-mail>recipients)
- Trap Receivers (Administration>Notification>SNMP Traps>trap receivers)

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

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by group** under **Event Actions** on the left navigation menu.
2. Choose how to group events for configuration:
   - Choose **Grouped by severity**, and then select all events of one or more severity levels. You cannot change the severity of an event.
   - Choose **Grouped by category**, and then select all events in one or more pre-defined categories.
3. Click **Next>>** to move from page to page to do the following:
   a. Select event actions for the group of events.
      - To choose any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
      - If you choose **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** (or both) on the next page.
   b. Select whether to leave the newly configured event action enabled for this group of events or to disable the action.

Active, Automatic, Direct Notification

E-mail notification

Overview of setup. Use the Simple Mail Transfer Protocol (SMTP) to send e-mail to up to four recipients when an event occurs.

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

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

See DNS (Administration>Network>DNS>options).

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

See SMTP (Administration>Notification>E-mail>server).

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

See E-mail recipients (Administration>Notification>E-mail>recipients).

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

SMTP (Administration>Notification>E-mail>server).

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

E-mail recipients (Administration>Notification>E-mail>recipients). Identify up to four e-mail recipients.

Setting	Description
To Address	The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, **myacct100@skytel.com**). The pager gateway will generate the page. To bypass the DNS lookup of the mail server's IP address, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly. **NOTE**: The recipient's pager must be able to use text-based messaging.

SMTP Server	Select one of the following methods for routing e-mail:
	• **Local**: Through the NetworkAIR FM air conditioner's SMTP server. This setting (recommended) ensures that the e-mail is sent before the NetworkAIR FM air conditioner's 20-second time-out, and, if necessary, is retried several times. Also do one of the following:
	  • Enable forwarding at the NetworkAIR FM air conditioner's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Check with the administrator of your SMTP server before changing its configuration to allow forwarding.
	  • Set up a special e-mail account for the NetworkAIR FM air conditioner to forward e-mail to an external mail account.
	• **Recipient**: Directly to the recipient's SMTP server. With this setting, the NetworkAIR FM air conditioner tries to send the e-mail only once. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent.
	When the recipient uses the NetworkAIR FM air conditioner's SMTP server, this setting has no effect.

Format	Select the information that will be included in the e-mail: • **Long**—The device's identification information, IP address, and serial number; the date and time of the event; the event code; and the event description. • **Short**—The event description only.
E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.

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

SNMP traps

Trap Receivers (Administration>Notification>SNMP Traps>trap receivers). View trap receivers by NMS IP/Host Name. You can configure up to six trap receivers.

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

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

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.)

See SNMPv3 (Administration>Network>SNMPv3>options) for information on creating user profiles and selecting authentication and encryption methods.

SNMP Trap Test (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 (Logs>Syslog>*options*)

The NetworkAIR FM air conditioner 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 (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 NetworkAIR FM air conditioner.
Port	The user datagram protocol (UDP) port that the NetworkAIR FM air conditioner will use to send Syslog messages. The default is **514**, the UDP port assigned to Syslog.

Syslog Settings (Logs>Syslog>settings).

Setting	Definition
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the NetworkAIR FM air conditioner's Syslog messages (**User**, by default). **NOTE: User** best defines the Syslog messages sent by the NetworkAIR FM air conditioner. **Do not** change this selection unless advised to do so by the Syslog network or system administrator.
Severity Mapping	Maps each severity level of NetworkAIR FM air conditioner events to available Syslog priorities. You should not need to change the mappings. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the **Local Priority** settings: • **Critical** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** **NOTE:** To disable Syslog messages, see Configuring event actions.

Syslog Test and Format Example (Logs>Syslog>test). Send a test message to the Syslog servers configured through the **servers** option.

1. Select a severity to assign to the test message.
2. Define the test message, according to the required message fields:
   – The priority (PRI): The Syslog priority assigned to the message's event, and the facility code of messages sent by the NetworkAIR FM air conditioner.

– The Header: A time stamp and the IP address of the NetworkAIR FM air conditioner.
– The message (MSG) part:
  • The TAG field, followed by a colon and space, identifies the event type.
  • The CONTENT field is the event text, followed (optionally) by a space and the event code.

For example, **`APC: Test Syslog`** is valid.

Indirect Notification through Logs or Queries

Event log (Logs>Events>*options*)

Displaying and using the event log (Logs>Events>log). View or delete the event log. By default, the log displays all events recorded during the last two days, in reverse chronological order.

- **Displaying the event log:** You can view the event log as a page of the Web interface (the default view) or, to see more of the listed events without scrolling, click **Launch Log in New Window** from that 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.

  You can also use FTP or Secure CoPy (SCP) to view the event log. See Using FTP or SCP to retrieve log files.

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

- **Filtering the log by event**: To specify the events that display in the log, click **Filter Log**. Unmark the checkbox of an event category or alarm severity level to remove it from view. Text at the right corner of the event log page indicates that a filter is active. The filter is active until you clear it or the device restarts. To remove an active filter, click **Filter Log**, then **Clear Filter (Show All)**.

  Events are processed through the filter using **OR** logic.
  - Events with unselected severity levels never display in the filtered event log, even if the event occurs in a category you selected in the Filter by Category list.
  - Events from unselected event categories never display in the filtered event log, even if devices in the category enter an alarm state you selected in the Filter by Severity list.
- **Deleting the event log**: To delete all events recorded in the log, click **Clear Event Log** on the Web page that displays the log. Deleted events cannot be retrieved.

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

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

See Configuring by event.

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.

Data log (Logs>Data>*options*)

Displaying and using the data log (Logs>Data>log). View a log of the temperature and humidity of supply and return air, measured at the NetworkAIR FM air conditioner. View the average temperature and humidity of supply and return air for the System, and view the suction pressure and discharge pressure recorded by the NetworkAIR FM air conditioner. Each entry is listed by the date and time the data was recorded.

- **Displaying the data log**: You can view the data log as a page of the Web interface (the default view) or, to see more of the data without scrolling, click **Launch Log in New Window** from that 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.

  Alternatively, you can use FTP or Secure CoPy (SCP) to view the data log. See Using FTP or SCP to retrieve log files.

- **Filtering the log by date or time**: To display the entire data log, or to change the number of days or weeks for which the log displays the most recent events, select **Last**. Select a time range from the drop-down menu, then click **Apply**. The filter configuration is saved until the device restarts.
  To display data logged during a specific time range, select **From**. Specify the beginning and ending dates and times for which to display data, then click **Apply**. The filter configuration is saved until the device restarts.

  Enter the time using the 24-hour clock format.

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

Graphing the data log (Logs>Data>graphing). Use this option to display the logged data records in a graph.

Data log graphing is an enhancement of the data log feature. To use this enhancement, JavaScript must be enabled in your browser. Alternatively, you can use FTP or SCP to import the data log into a spreadsheet application, and graph data in the spreadsheet. For FTP and SCP instructions, see Using FTP or SCP to retrieve log files.

How the graphing enhancement displays data and how efficiently it performs will vary depending on computer hardware, computer operating system, and the Web browser used to access the interface of the unit. Reducing the number of data points or data lines being graphed may improve performance.

Parameter	Description
Graph Data	Graph up to 4 data items. To graph multiple data items, hold down the CTRL key (or the Command key, for Macintosh® computers), then select the data items that correspond to the abbreviated column headings in the data log.
Graph Time	Specify the time period for which the data items will be graphed. • **Last**: Select the beginning time from which to graph the data records (2, 4, or 8 hours ago; 1, 2, or 4 days ago; or 1, 2, or 4 weeks ago). The graph will end at the most recent data record. • **From**: To customize the time period for the logged data records to graph, enter the beginning and end date and time. For the date, each letter m (for month), d (for day), and y (for year) represents one digit. For the time, each letter h (for hour) and m (for minute) represents one digit. Single-digit hours, minutes, days, and months are displayed with a leading zero.

Click **Apply** to view the graph, or click **Cancel** to discard the changes. Click **Launch Graph in New Window** to display the graph in a new browser window that provides a full-screen view.

The graph legend shows the color of the graph line for each selected data item. If the data items do not have the same unit of measurement, the units are displayed in the legend. If the data items do have the same units, the unit is displayed on the left side of the graph.

Move the mouse pointer over any horizontal line to view the date, time, and Y-axis value for that data record.

Use the **Zoom** menu to increase or decrease the magnification of the graph. The blue bar at the top left corner of the graph changes size to indicate the number of total data records being displayed and the relative location of the displayed data records. To re-center the graph, click any point on the graph or the blue bar.

Setting the data collection interval (Logs>Data>interval). Define 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.

Configuring 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.

Parameter	Description
Filename	The name of the repository file (an ASCII text file).
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 uploads of data to the file.
Maximum Retries	The maximum number of times the upload will be attempted after initial failure.
Failure Wait Time	How long in minutes before an attempt to upload data times out.

Using FTP or SCP to retrieve log files

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

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

The NetworkAIR FM air conditioner uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits.

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

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

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

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

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

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

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

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

1. At a command prompt, type **ftp** and the NetworkAIR FM air conditioner's IP address, and press ENTER.

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

   ```
   ftp>open ip_address port_number
   ```

   

   To set a non-default port value to enhance security for the FTP Server, see FTP Server (Administration>Network>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 **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.

Queries (SNMP GETs)

See SNMP 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.

Administration: General Options

Identification (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 SNMP agent of the NetworkAIR FM air conditioner. These settings are the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifiers (OIDs).

For more information about MIB-II OIDs, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide,* available on the APC NetworkAIR FM *Utility* CD and the APC Web site, **www.apc.com**.

Set the Date and Time

Method (Administration>General>Date & Time>mode)

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

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.

Setting	Definition
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 NetworkAIR FM air conditioner accesses the NTP Server for an update.
Update Using NTP Now	Initiate an immediate update of date and time by the NTP Server.

Daylight saving (Administration>General>Date & Time>daylight saving)

Enable either 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 DST:

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

Format (Administration>General>Date & Time>date format)

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

Use an .ini File (Administration>General>User Config File)

Use the settings from one NetworkAIR FM air conditioner to configure another. Retrieve the config.ini file from the configured NetworkAIR FM air conditioner, customize that file (e.g., to change the IP address), and upload the customized file to the new NetworkAIR FM air conditioner. The file name can be 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.**

Status	Reports the progress of the upload. The upload succeeds even if the file contains errors, but a system event r reports the errors in the event log.
Upload	Browse to the customized file and upload it so that the current NetworkAIR FM air conditioner can use it to set its own configuration.

To retrieve and customize the file of a configured NetworkAIR FM air conditioner, see Exporting Configuration Settings.

The config.ini file can be uploaded using HTTP or HTTPS. Using HTTP, the config.ini file is transmitted in plain text. To securely upload a config.ini file in which you change passwords, use HTTPS.

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

System Preferences (Administration>General>Preferences)

Color-coding events in the event log

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

Text Color	Alarm Severity
Red	**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	**Normal**: No alarms are present. The NetworkAIR FM air conditioner and all connected devices are operating normally.

Changing the default temperature scale

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

Reset the Interface (Administration>General>Reset/Reboot)

Action	Definition
Reboot Management Interface	Restarts the interface of the NetworkAIR FM air conditioner.
Reset All[1]	Check-mark **Include TCP/IP** to reset all configuration values; unmark **Include TCP/IP** to reset all values except TCP/IP
Reset Only[1]	**TCP/IP settings**: Set TCP/IP Configuration to **DHCP & BOOTP**, its default setting, requiring that the NetworkAIR FM air conditioner receive its TCP/IP settings from a DHCP or BOOTP server. See TCP/IP settings (Administration>Network>TCP/IP).
	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.	

Configuring Links (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 Module (Administration>General>About)

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

APC Device IP Configuration Wizard

Capabilities, Requirements, and Installation

Using the Wizard to configure TCP/IP settings

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

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

System requirements

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

Installation

To install the Wizard from the *Utility* CD:

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

To install the Wizard from a downloaded executable file:

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

Use the Wizard

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

Launch the Wizard

The installation creates a shortcut link in the **Start** menu to launch the Wizard.

Configure the basic TCP/IP settings remotely

Prepare to configure the settings. Before you run the Wizard:

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

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

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

On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the Network Management Card or device after the Wizard transmits the settings.

4. Click **Finish** to transmit the settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
5. If the Wizard finds another unconfigured Network Management Card or device, it displays the screen to enter TCP/IP settings. Repeat this procedure beginning at step 3, or to skip the Network Management Card or device whose MAC address is currently displayed, click **Cancel**.

Configure or reconfigure the TCP/IP settings locally

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

Exporting Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

An Administrator can retrieve the .ini file of a NetworkAIR FM air conditioner and export it to another NetworkAIR FM air conditioner or to multiple NetworkAIR FM air conditioners.

1. Configure a NetworkAIR FM air conditioner to have the settings you want to export.
2. Retrieve the .ini file from that NetworkAIR FM air conditioner.
3. Customize the file to change at least the TCP/IP settings.
4. Use a file transfer protocol supported by the NetworkAIR FM air conditioner to transfer a copy to one or more other NetworkAIR FM air conditioners. For a transfer to multiple NetworkAIR FM air conditioners, use an FTP or SCP script or the APC .ini file utility.

Each receiving NetworkAIR FM air conditioner uses the file to reconfigure its own settings and then deletes it.

Contents of the .ini file

The config.ini file you retrieve from a NetworkAIR FM air conditioner contains the following:

- *section headings* and *keywords* (only those supported for the device from which you retrieve the file)*:* Section headings are category names enclosed in brackets ([ ]). Keywords, under each section heading, are labels describing specific NetworkAIR FM air conditioner 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, e.g., in the **[NetworkTCP/IP]** section, the default value for **Override** (the MAC address of the NetworkAIR FM air conditioner) blocks the exporting of values for the **SystemIP**, **SubnetMask**, **DefaultGateway**, and **BootMode**.

Detailed procedures

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

1. If possible, use the interface of a NetworkAIR FM air conditioner 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 NetworkAIR FM air conditioner:
   a. Open a connection to the NetworkAIR FM air conditioner, 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 NetworkAIR FM air conditioner's settings:

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

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

To retrieve configuration settings from multiple NetworkAIR FM air conditioners and export them to other NetworkAIR FM air conditioners, see *Release Notes: ini File Utility, version 1.0,* available on the APC NetworkAIR FM *Utility* CD and at **www.apc.com**.

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

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, **LinkURL1=""** indicates that the URL is intentionally undefined.

- Enclose in quotation marks any values that contain leading or trailing spaces or are already enclosed in quotation marks.
- To export scheduled events, configure the values directly in the .ini file.
- To export a system time with the greatest accuracy, if the receiving NetworkAIR FM air conditioners 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 NetworkAIR FM air conditioner. To transfer the .ini file to another NetworkAIR FM air conditioner, do either of the following:

- From the Web interface of the receiving NetworkAIR FM air conditioner, select the **Administration** tab, **General** on the top menu bar, and **User Config File** on the left navigation menu. Enter the full path of the file, or use **Browse**.

  

  The config.ini file can be uploaded using HTTP or HTTPS. Using HTTP, the config.ini file is transmitted in plain text. To securely upload a config.ini file in which you change passwords, use HTTPS.

- Use any file transfer protocol supported by NetworkAIR FM air conditioners (e.g., 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 NetworkAIR FM air conditioner 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 NetworkAIR FM air conditioner:

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

Exporting the file to multiple NetworkAIR FM air conditioners. To export the .ini file to multiple NetworkAIR FM air conditioners:

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

To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* on the APC NetworkAIR FM *Utility* CD.

The Upload Event and Error Messages

The event and its error messages

The following event occurs when the receiving NetworkAIR FM air conditioner 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 NetworkAIR FM air conditioner 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 NetworkAIR FM air conditioner 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, for another reason, 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.

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 NetworkAIR FM air conditioners, ignore these error messages. To prevent these error messages, you can delete the lines that contain the **`Override`** keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Related Topics

On Windows operating systems, instead of transferring .ini files, you can use the APC Device IP Configuration Wizard to update the basic TCP/IP settings of NetworkAIR FM air conditioners and configure other settings through their user interface.

See APC Device IP Configuration Wizard.

File Transfers

Upgrading Firmware

Benefits of upgrading firmware

When you upgrade the firmware on the Network Management Card of the NetworkAIR FM air conditioner:

- You obtain the latest bug fixes and performance improvements.
- New features become available for immediate use.

Keeping the firmware versions consistent across your network ensures that all NetworkAIR FM air conditioners support the same features in the same manner.

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 AOS and application module files used with the Network Management Card share the same basic format:

apc_*hardware-version*_*type*_*firmware-version*.bin

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

Obtain the latest firmware version

Automated upgrade tool for Microsoft Windows systems. An upgrade tool automates the transferring of the firmware modules on any supported Windows operating system. Obtain the latest version of the tool at no cost from **www.apc.com/tools/download**. At this Web page, find the latest firmware release for your APC product (in this case, the Network Management Card of your NetworkAIR FM air conditioner) and download the automated tool, not the individual firmware modules. **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, you must upgrade the firmware of your Management Cards by using the separate AOS and application firmware modules.

Obtain the firmware modules from **www.apcc.com/tools/download**.

Firmware File Transfer Methods

To upgrade the firmware of a NetworkAIR FM air conditioner's Network Management Card, use one of these methods:

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

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

Use FTP or SCP to upgrade one Network Management Card

FTP. For you to use FTP to upgrade one Network Management Card over the network:

- The Network Management Card must be connected to the network, and its system IP, subnet mask, and default gateway must be configured
- The FTP server must be enabled at the Network Management Card.

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 Network Management Card'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 5. In step 5, use the application module file name.

SCP. If you use the high security of SSH for the control console, use SCP to upgrade the Network Management Card securely. To use Secure CoPy (SCP) to upgrade firmware for a Network Management Card:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the Network Management Card. The following example uses *xxx* to represent the version number of the AOS module:
   `scp apc_hw03_aos_xxx.bin apc@158.205.6.185:apc_hw03_aos_xxx.bin`
3. Use a similar SCP command line, with the name of the application module, to transfer the second firmware module to the Network Management Card.

How to upgrade multiple Network Management Cards

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

See *Release Notes: ini File Utility, version 1.0,* available on the APC NetworkAIR FM *Utility* CD.

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

Use XMODEM to upgrade one Network Management Card

To upgrade the firmware for a Network Management Card that is not on the network:

1. Obtain the individual firmware modules (the AOS module and the application module) from **www.apc.com/tools/download**.
2. Select a serial port at the local computer and disable any service that uses the port.
3. Connect the configuration cable provided with the NetworkAIR FM air conditioner to the selected port and to the serial port at the Network Management Card of the NetworkAIR FM air conditioner.
4. Run a terminal program such as HyperTerminal, and configure the selected port for 2400 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
5. Press ENTER to display the **User Name** prompt.
6. Enter the Administrator user name and password (**apc** by default for both).
7. From the **Control Console** menu, select **System**, then **Tools**, then **File Transfer**, then **XMODEM**; and type **`Yes`** at the prompt to continue.
8. Select a baud rate, change the terminal program's baud rate to match your selection, and press ENTER. A higher baud rate causes faster upgrades.
9. From the terminal program's menu, select the binary AOS file to transfer using XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 2400. The Network Management Card automatically restarts.
10. Repeat step 4 through step 9 to install the application module. In step 9, use the application module file name, not the AOS module file name.

For information about the format used for firmware modules, see Firmware files.

Verifying Upgrades and Updates

Verify the success or failure of the transfer

To verify whether a firmware upgrade succeeded, use the **Network** menu in the control console and select the **FTP Server** option to view the result of the last file transfer, or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last Transfer Result codes

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

Verify the version numbers of installed firmware.

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

Troubleshooting

Access Problems

Problem	Solution
Unable to ping the Network Management Card of the NetworkAIR FM air conditioner	If the Management Card's Status LED is green, try to ping another node on the same network segment as the Management Card. If that fails, it is not a problem with the Management Card. If the Status LED is not green, or if the ping test succeeds, perform the following checks: • Verify all network connections. • Verify the IP addresses of the Management Card and the NMS. • If the NMS is on a different physical network (or subnetwork) from the Management Card, verify the IP address of the default gateway (or router). • Verify the number of subnet bits for the Management Card's subnet mask.
Cannot allocate the communications port through a terminal program	Before you can use a terminal program to configure the Management Card, you must shut down any application, service, or program using the communications port.
Cannot access the control console through a serial connection	Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.
Cannot access the control console remotely	• Make sure you are using the correct access method, Telnet or Secure SHell (SSH). An Administrator can enable these access methods. By default, Telnet is enabled. Enabling SSH automatically disables Telnet. • For SSH, the Management Card may be creating a host key. The Management Card can take up to 5 minutes to create the host key, and SSH is inaccessible for that time.

Problem	Solution
Cannot access the Web interface	• Verify that HTTP or HTTPS access is enabled. • Make sure you are specifying the correct URL — one that is consistent with the security system used by the Management Card. SSL requires **https**, not **http**, at the beginning of the URL. • Verify that you can ping the Management Card. • Verify that you are using a Web browser supported for the Management Card. See Supported Web browsers. • If the Management Card has just restarted and SSL security is being set up, the Management Card may be generating a server certificate. The Management Card can take up to 5 minutes to create this certificate, and the SSL server is not available during that time.

SNMP Issues

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

Index

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

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 an APC Customer Support center by telephone or e-mail.
  - Regional centers

Direct InfraStruXure Customer Support Line	(1)(877)537-0607 (toll free)
APC headquarters U.S., Canada	(1)(800)800-4272 (toll free)
Latin America	(1)(401)789-5735 (USA)
Europe, Middle East, Africa	(353)(91)702000 (Ireland)
Western Europe (inc. Scandinavia)	+800 0272 0272
Japan	(0) 36402-2001
Australia, New Zealand, South Pacific area	(61) (2) 9955 9366 (Australia)

  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

Contact the APC representative or other distributor from whom you purchased your APC product for information on how to obtain local customer support.

Copyright

990-1608C **10/2007**