Contents

Introduction 1

Product Description ................................................................. 1
  Features of the Environmental Manager: Main Module 1
  Initial setup 2

Access Procedures ................................................................. 3
  Overview 3
  Access priority for logging on 3
  Types of user accounts 4

Recovering From a Lost Password ............................................... 5

Rear Panel ................................................................. 6

Watchdog Features ................................................................. 8
  Overview 8
  Network interface watchdog mechanism 8
  Resetting the network timer 8

Hardware Alarms 9

Alarm Messages ................................................................. 9
  A-Link alarms 9
  Sensor hardware alarms 9

Clearing the Hardware Alarms .................................................... 10

Control Console 11

How to Log On ........................................................................... 11
  Overview 11
  Remote access to the control console 11
  Local access to the control console 12

Main Screen ............................................................................. 13
  Sample main screen 13
  Information and status fields 13

Control Console Menus ............................................................... 15
  How to use control console menus 15
  Control console structure 15
Web Interface 18

Introduction ........................................................................................................... 18
   Overview 18
   Supported Web browsers 18

How to Log On ..................................................................................................... 19
   Overview 19
   URL address formats 20

Overview Page .................................................................................................... 21
   Overview 21
   Quick status icons 21
   Recent Device Events 22
   Help 22

How to Use the Tabs, Menus, and Links. .............................................................. 22
   Tabs 22
   Menus 23
   Quick Links 23

Operation and Monitoring 24

Commonly Used Features .................................................................................. 24
   Module configuration 24
   Device configuration 24

Home Tab. ............................................................................................................ 24
   Overview page 24
   System View page 25
   Module View page 26
   Alarm Status page 27

Sensors Tab. ......................................................................................................... 27
   Temperature & Humidity page 27
   User Inputs page 30

Outputs Tab .......................................................................................................... 33
   Beacons page 33
   Relay Output page 35
   Switched Outlet page 36
Administration: Security 37

Local Users .......................................................... 37
  Setting user access (Administration>Security>Local
  Users>options) 37

Remote Users ....................................................... 38
  Authentication (Administration>Security>Remote
  Users>Authentication) 38
  RADIUS (Administration>Security>Remote Users>RADIUS) 39

Configuring the RADIUS Server .................................. 40
  Summary of the configuration procedure 40
  Configuring a RADIUS server on UNIX®, with shadow
  passwords 41
  Supported RADIUS servers 41

Inactivity Timeout (Administration>Security>Auto Log Off) .... 41

Administration: Network Features 42

TCP/IP and Communication Settings ................................ 42
  TCP/IP settings (Administration>Network>TCP/IP) 42
  DHCP response options 44
  Port Speed (Administration>Network>Port Speed) 46

DNS (Administration>Network>DNS>options) ..................... 47

Web (Administration>Network>Web>options) ..................... 49

Console (Administration>Network>Console>options) ............. 51

SNMP ................................................................. 53
  SNMPv1 (Administration>Network>SNMPv1>options) 53
  SNMPv3 (Administration>Network>SNMPv3>options) 55

FTP Server (Administration>Network>FTP Server) .............. 57

Related topics ....................................................... 57

Administration: Notification and Logging 58

Event Actions (Administration>Notification>Event Actions>options) 58
  Types of notification 58
  Configuring event actions 59
Active, Automatic, Direct Notification ........................................... 61
   E-mail notification 61
   SNMP Traps 64
   SNMP Trap Test (Administration>Notification>SNMP
      Traps>test) 65
   Syslog (Logs>Syslog>options) 65

Indirect Notification through Logs or Queries ............................... 67
   Event log (Logs>Events>options) 67
   Data log (Logs>Data>options) 69
   Using FTP or SCP to retrieve log files 72
   Queries (Modbus requests and SNMP GETs) 74

Administration: General Options 75

Identification (Administration>General>Identification) .................... 75

Set the Date and Time ............................................................. 75
   Method (Administration>General>Date & Time>mode) 75
   Daylight Saving (Administration>General>Date & Time>daylight
      saving) 76
   Format (Administration>General>Date & Time>date format) 76

System Preferences (Administration>General>Preferences) .......... 77
   Color-coding events in the event log 77
   Changing the default temperature scale 77
   Configuring the default Home page 77

Serial Modbus (Administration>General>Serial Modbus) ............... 78

Reset the Interface (Administration>General>Reset/Reboot) .......... 78

Configuring Links (Administration>General>Quick Links) ........... 79

About the Main Module (Administration>General>About) ............ 80

APC Device IP Configuration Wizard 81

Capabilities, Requirements, and Installation .............................. 81
   How to use the Wizard to configure TCP/IP settings 81
   System requirements 81
   Installation 81

Use the Wizard ........................................................................ 82
   Launch the Wizard 82
   Configure the basic TCP/IP settings remotely 82
   Configure or reconfigure the TCP/IP settings locally 83
Introduction

Product Description

Features of the Environmental Manager: Main Module

The American Power Conversion (APC®) Environmental Manager: Main Module is a rack-mountable product that monitors and controls the essential environmental functions needed to ensure the availability of the racks and enclosures in a room. It provides the following features:

• Monitoring of temperature, humidity, beacon, and relay output.
• Input contact monitoring for use with dry contact, analog, and digital sensors.
• One controlled power outlet.
• Event log accessible by Telnet, FTP, Secure CoPy (SCP), serial connection, or a Web browser.
• Data log accessible by FTP, SCP, or a Web browser.
• Event actions, e-mail notifications, and Simple Network Management Protocol (SNMP) traps based on the severity level of events.

The Main Module does not provide battery backup or surge protection. To ensure that any device connected to the outlet on the Main Module is protected from power failure or power surges, connect the Main Module to an APC UPS.
Initial setup

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

- IP address of the Main Module
- Subnet mask
- IP address of the default gateway

Do not use the loopback address (127.0.0.1) as the default gateway address for the Main Module. Doing so disables the Main Module. 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 *Environmental Manager Main Module Installation and Configuration Manual*, provided in printed form and in PDF form on the *Utility CD*.

For detailed information on how to use a DHCP server to configure the TCP/IP settings at the Main Module, see *TCP/IP and Communication Settings*.
Access Procedures

Overview

Two interfaces (Web interface and control console) provide menus with options that allow you to manage the Main Module.

For more information about the internal user interfaces, see Web Interface or Control Console.

The Simple Network Management Protocol (SNMP) interface allows you to use an SNMP browser with the PowerNet® Management Information Base (MIB) to manage the Main Module.

To use the PowerNet MIB with an SNMP browser, see the PowerNet SNMP Management Information Base (MIB) Reference Guide, which is provided on the Utility CD.

Access priority for logging on

Only one user at a time can log on to the Main Module to use its interface. 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 Main Module.
- 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 Main Module is controlled.
Types of user accounts

The Main Module has three levels of access (Administrator, Device User, and Read-Only 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 menus:
  - In the Web interface, the menus on the *Home*, *Sensors*, and *Outputs* tabs, and the event and data logs, accessible under *Events* and *Data* left navigation menu options of the *Logs* tab.
  - In the control console, the equivalent features and options. (The Device User account-type is called Device Manager in the control console.)
  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 the 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 and data logs display no buttons to clear the logs or to open them in another window.
  The default user name is *readonly*, and the default password is *apc*.

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

To set **User Name** and **Password** values for the three account types, see Setting user access (Administration>Security>Local Users>options)
Recovering From a Lost Password

You can use a local computer that connects to the Main Module 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 serial cable (APC part number 940-0103) to the selected port on the computer and to the RS-232 Console Port at the Main Module.

3. Run a terminal program (such as HyperTerminal®) on your computer and configure the selected port to have 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   - The serial port is not in use by another application.
   - The terminal settings are correct as specified in step 3.
   - The correct cable is being used as specified in step 2.

5. Press the **Reset** button on the rear panel of the Main Module. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.

6. Press ENTER 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**.

9. Select **Accept changes**.

10. Press CTRL+C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.
## Rear Panel

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AC Line Inlet Provides power to the Main Module.</td>
</tr>
<tr>
<td>2</td>
<td>Switched Outlet Provides power to a device at a total maximum amperage of 10 A. Activate a connected device when configured events are activated (for example, turn on a fan when temperature rises above 75°F [24°C]).</td>
</tr>
<tr>
<td>3</td>
<td>Voltage Output Provides 12 V or 24 V to a connected device. See the <em>Environmental Manager Main Module Installation and Quick Configuration</em> manual for more information.</td>
</tr>
<tr>
<td></td>
<td>Relay Output Connects to relay-controlled external devices.</td>
</tr>
<tr>
<td>4</td>
<td>Peripheral port Reserved for future use.</td>
</tr>
<tr>
<td>5</td>
<td>Sensor ports Connect six temperature or temperature/humidity sensors (AP9335T or AP9335TH).</td>
</tr>
</tbody>
</table>
| 6    | User Inputs Connect four sensor devices. Supports the following:  
|      | • Dry contacts  
|      | • 0-5 V digital signals  
|      | • 0-5 VDC analog voltage  
<p>|      | • 4-20 mA current-loop sensors. |
| 7    | Modbus RS-485 port Connect the Main Module to a building management system, using the Modbus protocol. |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| 8    | 10/100 Base-T Network Port | Connect the Main Module to the network; Status and Link LEDs indicate network traffic.  
  - Status LED—blinks orange and green at start-up; indicates the status of the network connection (solid green—IP address established; blinking green—attempting to obtain an IP address).  
  - Link LED—blinks to indicate network traffic (green—operating at 10 mbps; orange—operating at 100 mbps). |
| 9    | RS-232 Console Port | Serial port used to configure initial network settings using the included configuration cable (APC part number 940-0103). |
| 10   | Reset switch | Resets the Main Module. |
| 11   | Power LED | Indicates whether the unit is receiving power (green—receiving power; off—not receiving power). |
| 12   | A-Link ports† | Expansion bus for adding APC TH Modules (AP9341), temperature sensors (AP9520T), and temperature/humidity sensors (AP9520TH). The bus provides communications and power to the TH Modules using standard CAT5 cabling with straight-through wiring. |
| 13   | Beacon port | Connect an alarm beacon (AP9324). |

†A-Link is an APC proprietary CAN (Controller Area Network) bus. Devices compatible with A-Link are not Ethernet devices and cannot coexist on an Ethernet bus with other networking devices, such as hubs and switches.
Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the Main Module 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 Main Module implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Main Module 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 Main Module does not restart if the network is quiet for 9.5 minutes, the Main Module attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the Main Module, and that response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network most of the time and is on the same subnet. The network traffic of that computer will restart the 9.5-minute timer frequently enough to prevent the Main Module from restarting.
Hardware Alarms

Alarm Messages

A-Link alarms

The alarm is accompanied by the following messages.

<table>
<thead>
<tr>
<th>A-Link Interface</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web or control console (status page display)</td>
<td>Alink Power Overload</td>
</tr>
<tr>
<td>Event log</td>
<td>Alink Power Overload</td>
</tr>
</tbody>
</table>

The A-Link messages indicate one of the following problems:
- An improper A-Link connector in one of the A-Link ports
- Too much equipment connected to one of the A-Link ports
- An internal A-Link hardware problem

Sensor hardware alarms

The alarm is accompanied by the following messages.

<table>
<thead>
<tr>
<th>Sensor Interface</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web or control console (front status display)</td>
<td>Sensor Disconnected</td>
</tr>
<tr>
<td>Event log</td>
<td>Sensor Disconnected</td>
</tr>
</tbody>
</table>

The sensor hardware messages indicate one of the following problems:
- An improper connector in one of the sensor ports
- An internal sensor port hardware problem
- A disconnected sensor
Clearing the Hardware Alarms

To clear an A-Link or sensor alarm, remove the devices from the Main Module or TH Module, beginning with any devices known to be in an alarm state, until the alarm stops. Then reconnect the devices one at a time to determine what individual or multiple devices caused the alarm condition.

For information on sensor and A-Link connections, see the *Environmental Manager Main Module Installation and Quick Start Manual*, provided in printed form, and in PDF on the *Utility CD*.

If everything is properly connected and the alarm persists, contact *APC Worldwide Customer Support*.

If the alarm state is activated and nothing is plugged into either the A-Link or sensor ports, turn off the Main Module, and see *Product Information*. 
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 Main Module 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 same user account as Device User in the Web interface). A Read-Only User has no access to the control console.

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

Remote access to the control console

An Administrator can access the control console through Telnet or 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, then the access option under Console on the left navigation menu.
- In the control console, choose the Network menu, then the Telnet/SSH option.

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 Main Module, at a command prompt, type `telnet` and the system IP address for the Main Module (when the Main Module uses the default Telnet port of 23), and press ENTER. For example:
   
   `telnet 198.168.6.133`

   If the Main Module uses a non-default port number (from 5000 to 32768), you must include a colon or a space (depending on your Telnet client) between the IP address 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**

For local access to the control console, use a computer that connects to the Main Module through the serial port on the rear panel of the unit.

1. Select a serial port at the computer, and disable any service that uses the port.
2. Connect the supplied serial cable (APC part number 940-0103) from the selected port on the computer to the serial port on the rear panel of the Main Module.
3. Run a terminal program (e.g., HyperTerminal) on your computer, and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.
5. Enter your user name and password.
Main Screen

Sample main screen

Following is an example of the screen displayed when you log on to the control console at a Main Module.

<table>
<thead>
<tr>
<th>American Power Conversion</th>
<th>Network Management Card AOS</th>
<th>vx.x.x</th>
</tr>
</thead>
<tbody>
<tr>
<td>(c) Copyright 2005 All Rights Reserved</td>
<td>Environmental Manager</td>
<td>vx.x.x</td>
</tr>
</tbody>
</table>

Name : myMgmt System
Contact : Eileen Jenson
Location : Testing lab 1
Date : 07/29/2007
Time : 10:06:10
User : Administrator
Stat : P+ N+ A+

Up Time : 0 Days 19 Hours 28 Minutes

Module ID : Critical

T/H Sensors : Normal
Input Sensors : Normal

Outputs : Normal

Control Console

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

The Module ID field is visible only when A-Link alarms are active.

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, Sample main screen, the application firmware for the Main Module is displayed.

Network Management Card AOS vx.x.x
Environmental Manager vx.x.x
• Three fields identify the system name, contact person, and location of the Main Module. (To set these values at the control console, select the System menu, then Identification.)
  Name : myMgmt System
  Contact : Eileen Jenson
  Location : Testing lab 1

• The Up Time field reports how long the Main Module has been running since it was last reset or since power was applied.
  Up Time: 0 Days 19 Hours 28 Minutes

• Two fields identify the most recent date and time the screen was refreshed.
  Date : 07/29/2007
  Time : 10:06:10

• The User field identifies whether you logged on through the Administrator or Device Manager account. (The Read-Only User account cannot access the control console.)
  User : Administrator

Main screen status fields.
• A Stat field reports the Main Module status.
  Stat : P+ N+ A+

<table>
<thead>
<tr>
<th>P+</th>
<th>The APC operating system (AOS) is functioning properly.</th>
</tr>
</thead>
<tbody>
<tr>
<td>N+</td>
<td>The network is functioning properly.</td>
</tr>
<tr>
<td>N?</td>
<td>A BOOTP request cycle is in progress.</td>
</tr>
<tr>
<td>N−</td>
<td>The Main Module failed to connect to the network.</td>
</tr>
<tr>
<td>N!</td>
<td>Another device is using the IP address of the Main Module.</td>
</tr>
<tr>
<td>A+</td>
<td>The application is functioning properly.</td>
</tr>
<tr>
<td>A−</td>
<td>The application has a bad checksum.</td>
</tr>
<tr>
<td>A?</td>
<td>The application is initializing.</td>
</tr>
<tr>
<td>A!</td>
<td>The application is not compatible with the AOS.</td>
</tr>
</tbody>
</table>
Environmental Manager status fields. The status fields display the status of each of the devices that the Main Module can control or monitor (devices connected to the Main Module or its TH Modules). Normal, Warning, or Critical is displayed.

Control Console Menus

How to use control console menus

The menus in the control console list options by number and name. To use an option, type the option’s number 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 the menu.

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

- Type ? and press ENTER to access brief menu option descriptions, if help exists for the menu.
- Press ENTER to refresh the menu.
- Press ESC to go back to the menu from which you accessed the current menu.
- Press CTRL+C to return to the main (Control Console) menu.
- Press CTRL+D to toggle through the T/H Sensors, Input Sensors, Outputs, and Module Identification menus.
- Press CTRL+L to access the event log.

Control console structure

For menus that are not specific to the Main Module or the TH Modules, option names and location of options may be different from the Web interface. These menu items are shared among APC network-enabled devices, and the menu structure in the control console has been retained from an earlier firmware version to ensure compatibility with scripts and programs that may rely on that structure.
Main menu

Use the **Main** 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, you can access only the **Device Manager** menus and the **Logout** option.

Device Manager menus

Use the **Device Manager** menu to select the components to manage. For example:

1- T/H Sensors
2- Input Sensors
3- Outputs
4- Module Identification

Use the **T/H Sensors** option to view the temperature, humidity (if applicable), and alarm status recorded by each temperature and humidity sensor connected to the system. This option also allows users to configure temperature thresholds and rate-of-change settings, enable or disable alarm generation, and reset rate-of-change alarms.

Use the **Input Sensors** option to view the name, status, location, and identification information for each input contact connected to the system, and to configure settings that are specific to the type of input installed.

See **User Inputs page** for information about configuration settings.

Use the **Outputs** option to view information about beacons, the switched outlet, or the relay output. Configure the identification information and normal state of the output devices, map alarms that will activate the output device, and manually change the state of the device.
Use the **Module Identification** option to view the model number, serial number, and hardware version of each Main Module or TH Module, and the version of firmware it is running. Configure the name and location of the device and, for TH Modules, configure the identification (ID) number or cause the identification LED to blink.

### Network menu

Use the **Network** menu to complete the following tasks:
- Configure the TCP/IP settings for the Main Module.
- Use the Ping utility (available only through the control console).
- Define settings that affect the DNS, FTP, Telnet/SSH, Web interface, SSL, SNMPv1, SNMPv3, e-mail, Modbus, and Syslog features of the Main Module.

### System menu

Use the **System** menu to complete the following tasks:
- Control Administrator and Device Manager access. (You cannot control Read-Only User access through the control console.)
- Define the system **Name**, **Contact**, and **Location** values.
- Set the **Date** and **Time** used by the Main Module.
- Through the **Tools** menu:
  - Restart the Main Module interface.
  - Reset parameters to their default values.
  - Delete SSH host keys and SSL certificates.
  - Upload an initialization file.
  - Transfer files.
- Through the **RADIUS** menu:
  - Define access, primary and secondary servers, and primary and secondary server secrets.
  - Set Timeout in seconds.
- Access system information about the Main Module.
Web Interface

Introduction

Overview

The Web interface provides options to manage the Main Module, TH Modules connected to the Main Module, and other supported devices.

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, version1.x, by Mozilla Corporation (on all operating systems), or Netscape® 7.x and higher (on all operating systems) to access the Main Module through its Web interface. Other commonly available browsers also may work but have not been fully tested by APC.

To use the Web interface, it is not required that you enable JavaScript® for your Web browser. It is recommended, however, for optimal functioning of the interface.

In addition, the Main Module cannot work with a proxy server. Therefore, before you can use a Web browser to access the Web interface, you must do one of the following:

- Configure the Web browser to disable the use of a proxy server for the Main Module.
- Configure the proxy server so that it does not proxy the specific IP address of the Main Module.
How to Log On

Overview

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

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

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

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 Main Module. 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 **Overview Page**.
URL address formats

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

Common browser error messages at log-on.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Browser</th>
<th>Cause of the Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>“You are not authorized to view this page” or</td>
<td>Internet Explorer,</td>
<td>Someone else is logged on.</td>
</tr>
<tr>
<td>“Someone is currently logged in...”</td>
<td>Netscape, Firefox</td>
<td></td>
</tr>
<tr>
<td>“The connection was refused...”</td>
<td>Netscape</td>
<td>Web access is disabled, or the URL was not correct.</td>
</tr>
<tr>
<td>“This page cannot be displayed.”</td>
<td>Internet Explorer</td>
<td></td>
</tr>
<tr>
<td>“Unable to connect...”</td>
<td>Firefox</td>
<td></td>
</tr>
</tbody>
</table>

URL format examples.

- For a DNS name of Web1:
  - `http://Web1` if HTTP is your access mode
  - `https://Web1` if HTTPS is your access mode
- For a System IP address of 198.168.6.133, when the Main Module uses the default Web server port (80):
  - `http://198.168.6.133` if HTTP is your access mode
  - `https://198.168.6.133` if HTTPS is your access mode
- For a System IP address of 198.168.6.133, when the Main Module uses a non-default Web server port (5000, in this example):
  - `http://198.168.6.133:5000` if HTTP is your access mode
  - `https://198.168.6.133:5000` if HTTPS is your access mode
Overview Page

Overview

The first time you log on at the Web interface, the **Home** tab’s top menu bar option **Overview** displays a summary of active alarm conditions and the most recent events recorded in the event log.

To change the page that displays at login, see System Preferences (Administration>General>Preferences).

Quick status icons

One or more icons and accompanying text indicate the current operating status of the devices connected to the Main Module:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Critical" /></td>
<td><strong>Critical</strong>: A critical alarm exists, which requires immediate action.</td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Warning" /></td>
<td><strong>Warning</strong>: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.</td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Normal" /></td>
<td><strong>Normal</strong>: No alarms are present. The Main Module and all connected devices are operating normally.</td>
<td></td>
</tr>
</tbody>
</table>

At the upper right corner of every page, the Web interface displays the same icons to report the status of the devices connected to the Main Module:

- 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.
To return to the **Overview** page to view a summary of the Main Module status, including the active alarms, click a quick status icon on any page of the interface.

**Recent Device Events**

On the **Overview** 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.

**Help**

Click **Help**, located in the upper right hand corner of the Web interface, to view context-sensitive information.

**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.

- **Home**—view a summary of active alarm or warning conditions; this tab is displayed at login
- **Sensors**—view the status of each temperature/humidity sensor and each input, and configure thresholds for alarm conditions
- **Outputs**—view the status of each beacon and configure the beacons, relay output, and switched outlet
- **Logs**—view and configure event and data logs
- **Administration**—configure security, network connection, notification, and device settings.
Menus

**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.

**Left navigation menu.** Each tab (except the Home tab) 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.

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:** A demonstration page where you can use samples of APC Web-enabled products
- **Link 3:** Information about APC Remote Monitoring Services

To reconfigure the links, see Configuring Links (Administration>General>Quick Links).
Operation and Monitoring

Commonly Used Features

Module configuration

From any table with a Module Name column heading, you can configure the Main Module or any TH Module. Click the name of the module to configure in the Module Name column to do the following:
- Enter the name and location of the module.
- Assign a new identifier number to a TH Module.
- Blink a TH Module’s Identifier # LED for up to ten minutes.
- View module factory information.

Device configuration

From any table displaying device names, you can configure devices connected to a Main Module or TH Module. Click on the device name in the Name column, make configuration changes, and click Apply.

Home Tab

Overview page

The Home tab’s top menu bar option Overview is displayed at initial login.

To change the page that displays at login, see System Preferences (Administration>General>Preferences).

View the number of temperature/humidity sensors, user input sensors, and beacons connected to the system, and view the ten most recent active alarms for the relay output, switched outlet, temperature/humidity sensors, user input sensors, and beacons. The Recent Device Events table lists the five most recent device events, in reverse chronological order.
If sensors, beacons, or modules are disconnected from the system, this page displays the name of the disconnected device, with a device status of Lost Comm (lost communication).

**System View page**

The **Home** tab’s top menu bar option **System View** displays the following information about the devices installed on the system:

- **Status**—Critical (a device connected to this module is reporting an alarm that requires immediate action), Warning (a device requires attention), or Normal (no device alarms are detected).
- **Name**—The name of the device. Click the device name to view or configure its settings.
- **Location**—The physical location of the device.
- **Type**—The type of device connected to the system.
- **Module Name**—The name of the module to which the device is connected. Click the name of a module to view or configure its settings.

By default, all information is sorted by status. A small arrow in the column heading indicates that information is being sorted in ascending or descending order. To sort by another column heading, click on its name.

To filter information, click **Create Filter**. On the filter configuration page, enter the information to filter, and click **Apply**. To modify the filter, click the filter icon in the column heading of the information being filtered, or click **Create Filter** again. Critical alarms that are filtered out will not display on the interface. The filter settings are valid for one user session only.
Module View page

The Home tab’s top menu bar option Module View displays the following module information about the devices installed on the system:

- Status—Critical (a device connected to this module is reporting an alarm that requires immediate action), Warning (a device requires attention), or Normal (no device alarms are detected).
- Module Name—The name of the module.
- Module ID—The number displayed on the Identifier # LED of the TH Module.
- Location—The physical location of the module.

By default, all information is sorted by status. A small arrow in the column heading indicates that information is being sorted in ascending or descending order. To sort by another column heading, click on its name.

To filter information, click Create Filter. On the filter configuration page, enter the information to filter, and click Apply. To modify the filter, click the filter icon in the column heading of the information being filtered, or click Create Filter again. Critical alarms that are filtered out will not display on the interface. The filter settings are valid for one user session only.

To configure the module: Click the name of the module to configure its name and location, view module factory information, and view the devices connected to the module. Configure the Identifier # LED of a TH Module, or blink the Identifier # LED for up to ten minutes.
Alarm Status page

The Home tab’s top menu bar option Alarm Status displays all active alarms for the relay output, the switched outlet, temperature/humidity sensors, user input sensors, and beacons connected to the system. For each device category, an icon reports the status of connected devices:

- 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.

Sensors Tab

Temperature & Humidity page

The Sensors tab’s top menu bar option Temperature & Humidity lists all temperature and temperature/humidity sensors connected to the network.

To change the temperature units from the default setting, click the thermometer icon. To permanently change the temperature units, select the Administration tab, then General, then Temp Scale.

By default, all sensors are sorted by status. A small arrow in the column heading indicates that the sensors are being sorted in ascending or descending order. To sort by another column heading, click on its name.

To configure a sensor: Click on the name of the sensor to modify. Enter the name and location in the appropriate fields and enable or disable Alarm Generation. Click Threshold Settings or Rate of Change Settings, alter the settings, and click Apply.

When Alarm Generation is disabled, the sensor continues to monitor the temperature of the air surrounding it, but does not generate an alarm if the temperature violates a threshold setting. Temperature alarms are recorded in the data log.
<table>
<thead>
<tr>
<th><strong>Threshold Settings</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Temperature Threshold</td>
<td>Set the minimum temperature threshold for this sensor. If the temperature drops below this threshold, an alarm occurs.</td>
</tr>
<tr>
<td>Low Temperature Threshold</td>
<td>Set the low temperature threshold for this sensor. If the temperature drops below this threshold, an alarm occurs. This threshold must be greater than <strong>Minimum Temperature Threshold</strong>.</td>
</tr>
<tr>
<td>High Temperature Threshold</td>
<td>Set the high temperature threshold for this sensor. If the temperature rises above this threshold, an alarm occurs. This threshold must be greater than the sum of <strong>Low Temperature Threshold</strong> and <strong>Temperature Threshold Hysteresis</strong>.</td>
</tr>
<tr>
<td>Maximum Temperature Threshold</td>
<td>Set the maximum temperature threshold for this sensor. If the temperature rises above this threshold, an alarm occurs. This threshold must be greater than <strong>High Temperature Threshold</strong>.</td>
</tr>
<tr>
<td>Temperature Threshold Hysteresis</td>
<td>The difference between the temperature threshold violation and the clearing point. Increasing this value prevents frequent alarms if temperature wavers slightly above and below the threshold before corrective actions restore the temperature to the clearing point.</td>
</tr>
<tr>
<td>Minimum Humidity Threshold</td>
<td>Set the minimum humidity threshold for this sensor. If the humidity drops below this threshold, an alarm occurs.</td>
</tr>
<tr>
<td>Low Humidity Threshold</td>
<td>Set the low humidity threshold for this sensor. If the humidity drops below this threshold, an alarm occurs. This threshold must be higher than <strong>Minimum Humidity Threshold</strong>.</td>
</tr>
<tr>
<td>High Humidity Threshold</td>
<td>Set the high humidity threshold for this sensor. If the humidity rises above this threshold, an alarm occurs. This threshold must be higher than the sum of <strong>Low Humidity Threshold</strong> and <strong>Humidity Threshold Hysteresis</strong>.</td>
</tr>
<tr>
<td>Maximum Humidity Threshold</td>
<td>Set the maximum humidity threshold for this sensor. If the humidity rises above this threshold, an alarm occurs. This threshold must be greater than <strong>High Humidity Threshold</strong>.</td>
</tr>
<tr>
<td>Humidity Threshold Hysteresis</td>
<td>The difference between the humidity threshold violation and the clearing point. Increasing this value prevents frequent alarms if humidity wavers slightly above and below the threshold before corrective actions restore the humidity to the clearing point.</td>
</tr>
</tbody>
</table>
To configure a filter: Click **Create Filter**. On the filter configuration page, enter the information to filter, and click **Apply**. To modify the filter, click the filter icon in the column heading of the information being filtered, or click **Create Filter** again. Critical alarms that are filtered out will not display on the interface. The filter settings are only valid for one user session.

**To configure a defined group of sensors:** Create a filter for the sensors to configure, then follow steps 2–4 of the procedure **To configure all sensors**.

**To configure all sensors:**

1. Remove any filters by clicking **Clear Filter** (skip this step if you are configuring a defined group of sensors).
2. Click **Mass Configuration**. Select the general information, temperature and humidity thresholds, and rate-of-temperature changes to mass-configure, and click **Next**.
3. Enter the settings, including a descriptive name and location. The following wildcard characters can be used:

<table>
<thead>
<tr>
<th>Rate of Change Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short-term Increasing Temperature Rate of Change</td>
<td>Set the maximum short-term increase in temperature that you want your system to allow. An alarm will occur if the temperature increases at a rate that is greater than the rate you have set.</td>
</tr>
<tr>
<td>Short-term Decreasing Temperature Rate of Change</td>
<td>Set the maximum short-term decrease in temperature that you want your system to allow. An alarm will occur if the temperature decreases at a rate that is greater than the rate you have set.</td>
</tr>
<tr>
<td>Long-term Increasing Temperature Rate of Change</td>
<td>Set the maximum long-term increase in temperature that you want your system to allow. An alarm will occur if the temperature increases at a rate that is greater than the rate you have set.</td>
</tr>
<tr>
<td>Long-term Decreasing Temperature Rate of Change</td>
<td>Set the maximum long-term decrease in temperature that you want your system to allow. An alarm will occur if the temperature decreases at a rate that is greater than the rate you have set.</td>
</tr>
</tbody>
</table>
4. Click **Apply**, then click **Finish** to view configured sensors.

If you change the module ID LED, DIP switch, or location after using wildcard characters, you must re-apply the same wildcard mass configuration settings for the changes to appear on the interface.

## User Inputs page

The **Sensors** tab’s top menu bar option **User Inputs** lists all user input sensors connected to the network. By default, all user inputs are sorted by status. A small arrow in the column heading indicates that the user inputs are being sorted in ascending or descending order. To sort by another column heading, click on its name.

**To configure a sensor:** Click on the name of the sensor to modify. Enter the name, location, and input type of the sensor, and click **Next**. See Analog sensor or Digital sensor/dry contact for configuration information specific to your device.

**To configure a filter:** Click **Create Filter**. On the filter configuration page, enter the information to filter, and click **Apply**. To modify the filter, click the filter icon in the column heading of the information being filtered, or click **Create Filter** again. Critical alarms that are filtered out will not display on the interface. The filter settings are valid for one user session only.

<table>
<thead>
<tr>
<th>Wildcard Characters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%m</td>
<td>Use to identify the LED ID of the module to which the sensor is connected. If the sensor is connected to the Main Module, this wildcard displays <strong>MM</strong>.</td>
</tr>
<tr>
<td>%p</td>
<td>Use to identify the sensor’s port number. A temperature or temperature/humidity sensor will display a number from 1 to 6, depending on the sensor port to which it is connected. A remote temperature or temperature/humidity sensor will display a number from 1 to 8, as defined by the remote sensor’s DIP switch settings.</td>
</tr>
<tr>
<td>%l</td>
<td>Use to identify the location of the module to which the sensor is connected.</td>
</tr>
</tbody>
</table>
To configure a defined group of sensors: Click Create Filter. On the filter configuration page, enter the information to filter, and click Apply, then follow the instructions for steps 2–5 of the procedure To configure all sensors.

To configure all sensors:

You can mass-configure the name, location, and alarm generation settings of all input sensors, but it is not possible to mass-configure analog-specific sensor settings. To mass-configure input sensor settings when you have analog sensors, you must first filter the table to display only discrete (digital and dry contact) sensors.

1. Remove any filters by clicking Clear Filter (disregard this step if you are configuring a defined group of sensors or if analog sensors are connected to the system).
2. Click Mass Configuration.
3. Select the general information and input settings to mass-configure, and click Next.
4. Enter the settings, including a descriptive name and location. The following wildcard characters can be used:

<table>
<thead>
<tr>
<th>Wildcard Characters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%m</td>
<td>Use to identify the LED ID of the module to which the sensor is connected. If the sensor is connected to the Main Module, this wildcard displays MM.</td>
</tr>
<tr>
<td>%p</td>
<td>Use to identify the sensor’s port number. A temperature or temperature/humidity sensor will display a number from 1 to 6, depending on the sensor port to which it is connected. A remote temperature or temperature/humidity sensor will display a number from 1 to 8, as defined by the remote sensor’s DIP switch settings.</td>
</tr>
<tr>
<td>%l</td>
<td>Use to identify the location of the module to which the sensor is connected.</td>
</tr>
</tbody>
</table>

5. Click Apply, then click Finish to view configured sensors.

If you change the module ID LED, DIP switch, or location after using wildcard characters, you must re-apply the same wildcard mass configuration settings for the changes to appear on the interface.
To change a sensor’s input type: Click on the sensor’s name, then click Change Input Type.

Analog sensor. Select the analog sensor option appropriate for your device (Analog mA or Analog V), then click Next. Enable or disable alarm generation, enter the Calibration information, and click Next. Click Thresholds to configure the thresholds that will cause an alarm, and select Apply.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calibration</td>
<td></td>
</tr>
<tr>
<td>Points</td>
<td>Enter the number of conversion points for the conversion map.</td>
</tr>
<tr>
<td>Units</td>
<td>Enter the sensor’s measurement units (for example, psi).</td>
</tr>
<tr>
<td>Conversion Map</td>
<td>Used to convert sensor data to mA or V; enter up to five voltages and their values converted to the sensor’s unit of measurement.</td>
</tr>
<tr>
<td>Thresholds</td>
<td></td>
</tr>
<tr>
<td>Minimum Threshold</td>
<td>Set the minimum threshold for this sensor. If the configured measurement drops below this number, an alarm occurs.</td>
</tr>
<tr>
<td>Low Threshold</td>
<td>Set the low threshold for this sensor. If the configured measurement drops below this number, an alarm occurs. This threshold must be greater than Minimum Threshold.</td>
</tr>
<tr>
<td>High Threshold</td>
<td>Set the high threshold for this sensor. If the configured measurement rises above this number, an alarm occurs. This threshold must be greater than the sum of Low Threshold and Threshold Hysteresis.</td>
</tr>
<tr>
<td>Maximum Threshold</td>
<td>Set the maximum threshold for this sensor. If the configured measurement rises above this number, an alarm occurs. This threshold must be greater than High Threshold.</td>
</tr>
<tr>
<td>Threshold Hysteresis</td>
<td>This difference between the threshold violation and the clearing point. Increasing this value prevents frequent alarms if the measurement wavers slightly above and below the threshold before corrective actions restores the measurement to the clearing point.</td>
</tr>
</tbody>
</table>
Digital sensor/dry contact. Configure the normal state, severity level, and alarm generation capabilities of your sensor, and click Apply.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal State</td>
<td>Set this contact to either normally open or normally closed.</td>
</tr>
<tr>
<td>Severity</td>
<td>Informational, Warning (device status requires attention), or Critical (device status requires immediate attention). Selecting the Informational severity setting causes all devices to display a status of Normal, even if devices are in an alarm state.</td>
</tr>
<tr>
<td>Alarm Generation</td>
<td>Enable or disable this sensor’s ability to send alarms.</td>
</tr>
</tbody>
</table>

Outputs Tab

Beacons page

To view the status of the beacons, select the Outputs tab and then select the top menu item Beacons. By default, all beacons are sorted by status. A small arrow in the column heading indicates that the beacons are sorted in ascending or descending order. To sort by another column heading, click on its name.

To configure or to change the name, location, or status of a beacon, click its name. Enter or revise the name and location in the appropriate fields, and click the status, Warning or Normal.

To configure a filter: Click Create Filter. On the filter configuration page, enter the information to filter, and click Apply. To modify the filter, click the filter icon in the column heading of the information being filtered, or click Create Filter again. Critical alarms that are filtered out will not display on the interface. The filter settings are only valid for one user session.

To configure a defined group of beacons: Click Create Filter, enter the information to filter, click Apply, then follow the instructions for the option To configure all beacons.
To configure all beacons:
1. Click **Clear Filter** (skip this step if you are configuring a defined group of sensors), then **Mass Configuration**.
2. Select the general information and settings to mass-configure, and click **Next**.
3. Enter the settings, including a descriptive name and location. The following wildcard characters can be used:

<table>
<thead>
<tr>
<th>Wildcard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%m</td>
<td>Use to identify the LED ID of the module to which the beacon is connected. If the beacon is connected to the Main Module, this wildcard displays <strong>MM</strong>.</td>
</tr>
<tr>
<td>%p</td>
<td>Use to identify the beacon’s port number. (For the beacon, this wildcard will always display 1.)</td>
</tr>
<tr>
<td>%l</td>
<td>Use to identify the location of the module to which the beacon is connected.</td>
</tr>
</tbody>
</table>

4. Click **Apply**, then click **Finish** to view configured beacons.

   ! Warning: If you change the module ID LED, DIP switch, or location after using wildcard characters, you must re-apply the same wildcard mass configuration settings for the changes to appear on the interface.

Mapping a device alarm to activate a beacon: The beacon connected to the TH Module can only be activated by the alarm states of sensors on that module. The beacon connected to the Main Module can be activated by an alarm state in any temperature/humidity sensor or remote temperature/humidity sensor connected to the system.

1. In the section **Mapping: Alarm Reaction**, select the alarm states that will activate the beacon.
2. By default, all sensors are mapped to activate the beacon when in an abnormal state. Click the name of the abnormal state to view the sensors connected to the module. If you are configuring the beacon connected to the Main Module, all sensors connected to the system are displayed.
3. Select devices to include in the alarm. Any selected device, in its abnormal state, activates the beacon.

4. Click **Apply**.

To start the beacon for testing purposes, select **Turn Beacon On**. To stop the beacon when it is active, select **Turn Beacon Off**.

**Relay Output page**

Select the **Outputs** tab and then the top menu item **Relay Output** to configure the relay output. Enter the name and location in the appropriate fields. Set the normal state of the output, open or closed.

To change the state of the output manually, check-mark the setting in the **Control** field.

**Mapping a device alarm to activate a relay**: The relay can be activated only by the alarm states of sensors connected to the Main Module.

1. In the section **Mapping: Alarm Reaction**, select the alarm states that will activate the relay.
2. By default, all sensors connected to the Main Module are mapped to activate the relay output when in an abnormal state. Click the name of the abnormal state to view the sensors connected to the module.
3. Select devices to include in the alarm. Any selected device, in its abnormal state, activates the relay.
4. Click **Apply**.
Switched Outlet page

Select the Outputs tab and then the top menu item Switched Outlet to configure the switched outlet. Enter the name and location in the appropriate fields. Set the normal state of the outlet, on or off.

To change the state of the outlet manually, check-mark the setting in the Control field.

Mapping a device alarm to activate a outlet: The outlet can only be activated by the alarm states of sensors on the Main Module.

1. In the section Mapping: Alarm Reaction, select the alarm states that will activate the outlet.
2. By default, all sensors connected to the Main Module are mapped to activate the switched outlet when in an abnormal state. Click the name of the abnormal state to view the sensors connected to the module.
3. Select devices to include in the alarm. Any selected device, in its abnormal state, activates the outlet.
4. Click Apply.
Local Users

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

You set the user name and password for each of the account types in the same manner. The maximum length of the user name is 10 characters; the maximum length of the password is 32 characters. Blank passwords (passwords with no characters) are not allowed.

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

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Default User Name</th>
<th>Default Password</th>
<th>Permitted Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>apc</td>
<td>apc</td>
<td>Web interface and control console</td>
</tr>
<tr>
<td>Device User</td>
<td>device</td>
<td>apc</td>
<td>Web interface only</td>
</tr>
<tr>
<td>Read-Only User</td>
<td>readonly</td>
<td>apc</td>
<td>Web interface only</td>
</tr>
</tbody>
</table>
Remote Users

Authentication (Administration>Security>Remote Users>Authentication)

Use this option to select how to administer remote access to this Main Module.

For information about local authentication (authentication that can be administered without the centralized authentication provided by a RADIUS server), see the Security Handbook provided on the Utility CD and available 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 Main Module 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 Main Module are limited to 32 characters.

Select one of the following:

• **Local Authentication Only**: RADIUS is disabled. Local authentication is enabled.

• **RADIUS, then Local Authentication**: RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used.

• **RADIUS Only**: RADIUS is enabled. Local authentication is disabled.

If **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 Main Module, 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

<table>
<thead>
<tr>
<th>RADIUS Setting</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Server</td>
<td>The server name or IP address of the RADIUS server.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>Secret</td>
<td>The shared secret between the RADIUS server and the Main Module.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time, in seconds, that the Main Module waits for a response from the RADIUS server.</td>
</tr>
<tr>
<td>Test Settings</td>
<td>Enter the Administrator user name and password to test the RADIUS server path that you have configured.</td>
</tr>
<tr>
<td>Skip Test and Apply</td>
<td>Do not test the RADIUS server path.</td>
</tr>
<tr>
<td>Switch Server Priority</td>
<td>Change which RADIUS server will authenticate users if two configured servers are listed and <strong>RADIUS, then Local Authentication</strong> or <strong>RADIUS Only</strong> is the enabled authentication method.</td>
</tr>
</tbody>
</table>
Configuring the RADIUS Server

Summary of the configuration procedure

You must configure your RADIUS server to work with the Main Module.

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 Main Module to the RADIUS server client list (file).

   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.

2. Users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined. If no Service-Type attributes are configured, the user 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. Vendor Specific Attributes (VSA) 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.

   For examples of the RADIUS users file with VSAs and an example of an entry in the dictionary file on the RADIUS server, see the APC Security Handbook.
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.
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 Main Module.

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

For information on DHCP and DHCP options, see RFC2131 and RFC2132.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>The IP address, subnet mask, and default gateway must be configured manually. Click <strong>Next&gt;&gt;</strong>, and enter the new values.</td>
</tr>
</tbody>
</table>
| BOOTP | A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Main Module requests network assignment from any BOOTP server:  
  • If the Main Module receives a valid response, it starts the network services.  
  • If the Main Module finds a BOOTP server, but the request to that server fails or times out, the Main Module stops requesting network settings until it is restarted.  
  • By default, if previously configured network settings exist, and the Main Module 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 Main Module requests network assignment from any DHCP server. By default, the number of retries is unlimited.  
  • If the Main Module 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 the Main Module finds a DHCP server, but the request to that server fails or times out, the Main Module stops requesting network settings until it is restarted.  
  
To change these values, click **Next>>** to access 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 Main Module, which uniquely identifies it on the local area network (LAN)  
• **User Class**: The name of the application firmware module
DHCP & BOOTP

The default setting. The Main Module 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 Main Module.

Click Next>> to configure the same settings that are on the BOOTP Configuration and DHCP Configuration pages¹ 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 Main Module, 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 Main Module needs to operate on a network, and other information that affects the Main Module’s operation.

**Vendor Specific Information (option 43).** The Main Module 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 Main Module that a DHCP server is configured to service APC devices. By default, this DHCP response option must contain the APC Cookie for the Main Module 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 the option *Remain in DHCP & BOOTP mode after accepting TCP/IP settings*, which, by default, is disabled.
  - A data value of 1 enables the option *Remain in DHCP & BOOTP mode after accepting TCP/IP settings*. Whenever the Main Module 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 option *Remain in DHCP & BOOTP mode after accepting TCP/IP settings*. The *TCP/IP Configuration* setting option switches to DHCP when the Main Module accepts the DHCP response. Whenever the Main Module 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 Main Module 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 Main Module.
- **Subnet Mask** (option 1): The Subnet Mask value that the Main Module needs to operate on the network.
- **Router**, i.e., Default Gateway (option 3): The default gateway address that the Main Module needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the Main Module.
- **Renewal Time, T1** (option 58): The time that the Main Module 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 Main Module must wait after an IP address lease is assigned before it can seek to rebind that lease.

**Other options.** The Main Module also uses the following 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 Main Module can use.
- **Time Offset** (option 2): The offset of the Main Module'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 Main Module can use.
- **Host Name** (option 12): The host name that the Main Module will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the Main Module 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 APC user configuration file (.ini file) to download. The `siaddr` field of the DHCP response specifies the IP address of the server from which the Main Module will download the .ini file. After the download, the Main Module 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 either 10 Mbps or 100 Mbps, each with the option of half-duplex (for communication in only one direction at a time) or full-duplex (for communication simultaneously in both directions on the same channel).
DNS (Administration>Network>DNS>options)

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

Servers. Select servers to specify the IP addresses of the primary and optional secondary DNS server. For the Main Module to send e-mail, at least the IP address of the primary DNS server must be defined.

The Main Module 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 Main Module does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the Main Module or on a nearby segment (but not across a wide-area network [WAN]).

![Book Icon] To verify that DNS is working correctly after you define the IP addresses of the DNS servers, see Test.

Naming. Select naming to define the host name and domain name of the Main Module:

- **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 Main Module 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 Main Module interface (except e-mail addresses) that accept domain names, the Main Module adds this domain name when only a host name is entered.
  - To override all instances of the expansion of a specified host name by the addition of the domain name, set the domain name field to its default, somedomain.com, or to 0.0.0.0.
  - To override the expansion of a specific host name entry (for example, when defining a trap receiver) include a trailing period. The Main Module 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.
Test. 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

- In the **Query Question** field, identify the value to be used for the selected query type:

<table>
<thead>
<tr>
<th>Query Type Selected</th>
<th>Query Question to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>by Host</td>
<td>the URL</td>
</tr>
<tr>
<td>by FQDN</td>
<td>the fully qualified domain name, my_server.my_domain.</td>
</tr>
<tr>
<td>by IP</td>
<td>the IP address</td>
</tr>
<tr>
<td>by MX</td>
<td>the Mail Exchange address</td>
</tr>
</tbody>
</table>

- View the result of the test DNS request in the **Last Query Response** field.
Web (Administration>Network>Web>options)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| access                  | To activate changes to any of these selections, log off from the Main Module:  
  • **Disable**: Disables access to the Web interface. (You must use the control console to re-enable access. Select **Network** and **Web/SSL/TLS**. For HTTP access, 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 over Secure Sockets Layer (HTTPS) to provide Web access. Secure Sockets Layer (SSL) encrypts user names, passwords, and data during transmission, and authenticates the Main Module 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 **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 Main Module.  

  **HTTPS Port**: The TCP/IP port (443 by default) used to communicate by HTTPS with the Main Module.  

  For either of these ports, you can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114:  

  `http://152.214.12.114:5000`
  `https://152.214.12.114:5000`

| ssl 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.  

|
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 Main Module.

- **Generating:** The Main Module is generating a certificate because no valid certificate was found.

- **Loading:** A certificate is being activated on the Main Module.

- **Valid certificate:** A valid certificate was installed or was generated by the Main Module. 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 Main Module 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 Utility CD to choose a method for using digital certificates created by the Security Wizard or generated by the Main Module.

**Remove:** Delete the current certificate.
## Console (Administration>Network>Console>options)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| access | Choose one of the following for access by Telnet or Secure SHeIl (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/v2**: Do not enable both versions 1 and 2 of Secure SHeIl (SSH) unless you require both. (Security protocols 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 TCP/IP ports to be used by these protocols:  
  - **Telnet Port**: The Telnet port used to communicate with the Main Module (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 these commands:  
    - `telnet 152.214.12.114:5000`  
    - `telnet 152.214.12.114 5000`  
  - **SSH Port**: The SSH port used to communicate with the Main Module (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**). |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 Main Module is creating a host key because no valid host key was found.  
  - **Loading:** A host key is being activated on the Main Module.  
  - **Valid:** One of the following valid host keys is in the /sec directory (the required location on the Main Module):  
    - A 1024-bit host key created by the APC Security Wizard  
    - A 768-bit RSA host key generated by the Main Module  

  **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 *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 Main Module 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. SSH 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 Main Module on the public network of an InfraStruXure system, you must have SNMP enabled in the Main Module interface. Read access will allow InfraStruXure Manager to receive traps from a Main Module, but Write access is required while you use the interface of the Main Module 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 *Utility CD* or from the APC Web site, [www.apc.com](http://www.apc.com).
### Option Description

**access**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access</td>
<td><strong>Enable SNMPv1 Access:</strong> Enables SNMP version 1 as a method of communication with this device.</td>
</tr>
</tbody>
</table>

**access control**

You can configure up to four access control entries to specify which Network Management Systems (NMSs) have access to this device. The opening page for access control, by default, assigns one entry to each of the four available SNMPv1 communities, but you can edit these settings to apply more than one entry to any community to grant access by several specific IP addresses, host names, or IP address masks. To edit the access control settings for a community, click its community name.

- If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network.
- If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device.

**Community Name:** The name that an NMS must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are `public`, `private`, `public2`, and `private2`.

**NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contains 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 Main Module supports only MD5 authentication and DES encryption.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access</td>
<td><strong>SNMPv3 Access:</strong> Enables SNMPv3 as a method of communication with this device.</td>
</tr>
<tr>
<td>user profiles</td>
<td>By default, lists the settings of four user profiles, configured with the user names <strong>apc snmp profile1</strong> through <strong>apc snmp profile4</strong>, and no authentication and no privacy (no encryption). To edit the following settings for a user profile, click a user name in the list.</td>
</tr>
</tbody>
</table>

**User Name:** The identifier of the user profile. SNMPv3 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.
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access control</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>

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 for communication with the Main Module. 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 the 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.

Related topics

See these related topics:
• Console (Administration>Network>Console>options) to configure SSH.
• Using FTP or SCP to retrieve log files to obtain a text version of the event or data log.
Types of notification

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

- Active, automatic notification. The following actions notify specified users or monitoring devices directly:
  - E-mail notification
  - SNMP traps
  - Syslog notification

To set up other types of active notification not included in the Event Action options, see Beacons page and Relay Output page.

- Indirect notification through the event log. Users must check the log to determine which events have occurred.

Other methods of indirect notification, not included in the Event Action options, are informational queries. See Serial Modbus (Administration>General>Serial Modbus) to configure and use the request/response structure of Modbus. See SNMP for SNMP access types that enable 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.

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

**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, of the secondary Domain Name System (DNS) servers

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

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

  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).**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local SMTP Server</td>
<td>The IP address (or if DNS is configured, the DNS name) of the local SMTP server. <strong>NOTE:</strong> This definition is required only when SMTP Server is set to Local when e-mail recipients are being configured. See E-mail recipients (Administration&gt;Notification&gt;E-mail&gt;recipients).</td>
</tr>
<tr>
<td>From Address</td>
<td>The contents of the From field in the format user@[IP_address] (if an IP address is specified as Local SMTP Server) or <a href="mailto:user@domain.com">user@domain.com</a> (if DNS is configured and the DNS name is specified as Local SMTP Server) in the e-mail messages sent by the Main Module. <strong>NOTE:</strong> The local SMTP server’s configuration may require that you use a valid user account on the server for this setting. See the server’s documentation for more information.</td>
</tr>
</tbody>
</table>
**E-mail recipients (Administration>Notification>E-mail>recipients).** Use this option to identify up to four e-mail recipients.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Address</td>
<td>Defines the user and domain names of the recipient. To use e-mail for paging, use the e-mail address for that recipient’s pager gateway account (for example, <a href="mailto:myacct100@skytel.com">myacct100@skytel.com</a>). The pager gateway will generate the page. You can bypass the DNS lookup of the mail server’s IP address by using the IP address in brackets instead of the e-mail domain name. For example, use jsmith@[xxx.xxx.x.xxx] instead of <a href="mailto:jsmith@company.com">jsmith@company.com</a>. This is useful when DNS lookups are not working correctly. <strong>NOTE:</strong> The recipient’s pager must be able to use text-based messaging.</td>
</tr>
</tbody>
</table>
| SMTP Server   | Selects one of the following methods for routing e-mail:  
• **Local:** Through the Main Module’s SMTP server (the recommended setting). This option ensures that the e-mail is sent before the Main Module’s 20-second time-out, and, if necessary, is retried several times. Also do one of the following:  
• Enable forwarding at the Main Module’s SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Always check with the administrator of your SMTP server before changing the configuration of the SMTP server to allow forwarding.  
• Set up a special e-mail account for the Main Module to forward e-mail to an external mail account.  
• **Recipient:** Directly to the recipient’s SMTP server. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent because, with this option, the Main Module tries to send the e-mail only once.  
When the recipient uses the Main Module’s SMTP server, this setting has no effect. |
| E-mail Generation | Enables (by default) or disables sending e-mail to the recipient.                                                                                       |

**E-mail test (Administration>Notification>E-mail>test).** Use this option to 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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap Generation</td>
<td>Enable (the default) or disable trap generation for this trap receiver.</td>
</tr>
<tr>
<td>NMS IP/Host Name</td>
<td>The IP address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.</td>
</tr>
</tbody>
</table>

SNMPv1 option.

<table>
<thead>
<tr>
<th>Item</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Name</td>
<td>The name (public by default) used as an identifier when SNMPv1 traps are sent to this trap receiver.</td>
</tr>
<tr>
<td>Authenticate Traps</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 Main Module 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).**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Server</td>
<td>Uses IP addresses or host names to identify from one to four servers to receive Syslog messages sent by the Main Module.</td>
</tr>
<tr>
<td>Port</td>
<td>The user datagram protocol (UDP) port that the Main Module will use to send Syslog messages. The default is 514, the UDP port assigned to Syslog.</td>
</tr>
</tbody>
</table>
**Syslog Settings (Logs>Syslog>settings).**

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

**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 Main Module.
– The Header: A time stamp and the IP address of the Main Module.
– 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>**

**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 upper 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 that you do not select from the Filter By Severity list never display in the filtered event log, even if the event occurs in a category you selected from the Filter by Category list.

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

• **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 that stores periodic measurements of the ambient temperature and relative humidity for each sensor managed by the Main Module and its TH Modules. 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 then 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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graph Data</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Graph Time      | Specify the time period for which the data items will be graphed. <br>• **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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Log Rotation</td>
<td>Enable or disable (the default) data log rotation.</td>
</tr>
<tr>
<td>FTP Server Address</td>
<td>The location of the FTP server where the data repository file is stored.</td>
</tr>
<tr>
<td>User Name</td>
<td>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.</td>
</tr>
<tr>
<td>Password</td>
<td>The password required to send data to the repository file.</td>
</tr>
<tr>
<td>File Path</td>
<td>The path to the repository file.</td>
</tr>
<tr>
<td>Filename</td>
<td>The name of the repository file (an ASCII text file).</td>
</tr>
<tr>
<td>Delay X hours between uploads.</td>
<td>The number of hours between uploads of data to the file.</td>
</tr>
<tr>
<td>Upload every X minutes</td>
<td>The number of minutes between uploads of data to the file.</td>
</tr>
</tbody>
</table>
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 of the 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 Main Module
  - The unique Event Code for each recorded event (*event.txt* file only)

The Main Module 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 of the year.

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 Utility CD and on the APC Web site (www.apc.com) for information on the available protocols and methods for setting up the type of security you need.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Retries</td>
<td>The maximum number of times the upload will be attempted after initial failure.</td>
</tr>
<tr>
<td>Failure Wait Time</td>
<td>How long in minutes before an attempt to upload data times out.</td>
</tr>
</tbody>
</table>
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 Main Module’s IP address, and press ENTER.

   If the Port setting for the FTP Server option (which you select on the Network menu of the Administration tab) has been changed from its default value (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-version of the event log or data 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 the event log or data 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 is created to record the deleted-log event.

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

**Queries (Modbus requests and SNMP GETs)**

See Serial Modbus (Administration>General>Serial Modbus) for information on configuring and using the request/response structure of Modbus, and 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 the **Name** (the device name), **Location** (the physical location), and **Contact** (the person responsible for the device) used by the Main Module’s SNMP agent. These settings are the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifications (OIDs).

For more information about the MIB-II OIDs, see the *PowerNet SNMP Management Information Base (MIB) Reference Guide* provided on the Utility CD and on the APC Web site, [www.apc.com](http://www.apc.com).

Set the Date and Time

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

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

- **Manual**: Do one of the following:
  - Enter the date and time for the Main Module.
  - Mark the checkbox **Apply Local Computer Time** to match the date and time settings of the computer you are using, and click **Apply**.

- **Synchronize with NTP Server**: Have an NTP Server define the date and time for the Main Module.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary NTP Server</td>
<td>Enter the IP address or domain name of the primary NTP server.</td>
</tr>
<tr>
<td>Secondary NTP Server</td>
<td>Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.</td>
</tr>
<tr>
<td>Setting</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Time Zone</td>
<td>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.</td>
</tr>
<tr>
<td>Update Interval</td>
<td>Define how often, in hours, the Main Module accesses the NTP Server for an update. <em>Minimum: 1; Maximum: 8760 (1 year).</em></td>
</tr>
<tr>
<td>Update Using NTP Now</td>
<td>Initiate an immediate update of date and time by the NTP Server.</td>
</tr>
</tbody>
</table>

**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 Daylight Saving Time (DST):
- If the local DST always starts or ends on the fourth occurrence of a specific weekday of a month (for example, 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 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.
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.

<table>
<thead>
<tr>
<th>Text Color</th>
<th>Alarm Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Critical: A critical alarm exists, which requires immediate action.</td>
</tr>
<tr>
<td>Orange</td>
<td>Warning: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.</td>
</tr>
<tr>
<td>Green</td>
<td>Normal: No alarms are present. The Main Module and all connected devices are operating normally.</td>
</tr>
</tbody>
</table>

Changing the default temperature scale

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

Configuring the default Home page

To change the Web page that displays by default at login, select a Web page from the Log On Start Page drop-down menu.
Serial Modbus (Administration>General>Serial Modbus)

To configure Modbus, select the Administration tab, General on the top menu bar, and Serial Modbus on the left navigation menu. You can enable or disable Modbus, choose a baud rate, and specify a unique identifier.

Modbus defines a request/response message structure for a client/server environment. The APC implementation of Modbus uses Remote Terminal Unit (RTU) mode. You can use Modbus to view the Environmental Manager through your building management system interface. It is read-only.

• The Modbus interface supports 2-wire RS-485.
• Modbus runs at 9600 or 19200 bps.

The Modbus register map for the Environmental Manager defines the data (type, location, and valid responses) available through Modbus. To download the Modbus register map or any updates to this register map, go to the APC Web site (www.apc.com), search by part number for AP9340, and click the link to the register map in the list of documentation. Check the publication date at the start of the file.

For more information on Modbus, see the Modbus Standard Library at www.modbus.org.

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

Use this option to perform any of the following actions:

<table>
<thead>
<tr>
<th>Action</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot Management Interface</td>
<td>Restarts the interface of the Main Module.</td>
</tr>
<tr>
<td>Reset to Defaults</td>
<td>Resets all configuration settings.</td>
</tr>
</tbody>
</table>

**NOTE:** For information about how this affects the TCP/IP configuration settings, see this table’s description of **Reset Only TCP/IP to Defaults**.
Configuring Links (Administration>General>Quick Links)

Select the Administration tab, the General option on the top menu bar, and the Quick Links option on the left navigation menu to view the three URL links displayed at the bottom left of each page of the interface.

By default, these links access the following Web pages:

- **APC’s Web Site**: The APC home page.
- **Testdrive Demo**: A demonstration page where you can use samples of APC Web-enabled products.
- **APC Monitoring**: The home page of the APC Remote Monitoring Service.

To reconfigure a link, click on that link in the Display column, and change any of the following:

- **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 and server

**NOTE:** With the TCP/IP configuration method set to **DHCP & BOOTP**, its default setting, the Main Module’s TCP/IP settings must be defined by a DHCP or BOOTP server. See **TCP/IP settings (Administration>Network>TCP/IP)**.

<table>
<thead>
<tr>
<th>Action</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset to Defaults Except TCP/IP</td>
<td>Resets all configuration settings except the TCP/IP settings.</td>
</tr>
<tr>
<td>Reset Only TCP/IP to Defaults</td>
<td>Resets the TCP/IP settings only. <strong>NOTE:</strong> With the TCP/IP configuration method set to <strong>DHCP &amp; BOOTP</strong>, its default setting, the Main Module’s TCP/IP settings must be defined by a DHCP or BOOTP server. See <strong>TCP/IP settings (Administration&gt;Network&gt;TCP/IP)</strong>.</td>
</tr>
<tr>
<td>Reset Only Event Configuration</td>
<td>Resets all events to their default configuration. Any configuration changes, by event or by group, revert to default settings.</td>
</tr>
<tr>
<td>Reset All Lost Comms Alarms</td>
<td>Resets alarms caused when devices are removed from the system.</td>
</tr>
</tbody>
</table>
About the Main Module (Administration>General>About)

The hardware information is especially useful to APC Customer Support in helping to troubleshoot problems with the Main Module. The serial number and MAC address accessible through the About menu option are also available on the Main Module itself.

Firmware information, listed under Application Module and APC OS (AOS), indicates the name, firmware version number, and the date and time each firmware module was created. This information may also be useful in troubleshooting and enables you to determine quickly if updated firmware is available to download from the APC Web site.
APC Device IP Configuration Wizard

Capabilities, Requirements, and Installation

How to use 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 Network Management Cards or devices on the same network segment as the computer running the Wizard.
• Through a direct connection from a serial port of your computer to a Network Management Card or device to configure or reconfigure it.

System requirements


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:

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 or devices.

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 Network Management Card or device) 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 6, you can now configure other parameters through the Web interface of the card or device.
Retrieving and Exporting the .ini File

Summary of the procedure

An Administrator can retrieve the .ini file of a Main Module and export it to another Main Module or to multiple Main Modules.

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

Each receiving Main Module 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 Main Module 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 Main Module 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 Main Module) 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 Main Module 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 Main Module:
   a. Open a connection to the Main Module, 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 Main Module’s settings:
      ```
      ftp> get config.ini
      ```
      The file is written to the folder from which you launched FTP.

To retrieve configuration settings from multiple Main Modules and export them to other Main Modules, see Release Notes: ini File Utility, version 1.0, available on the 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 Main Modules can access a Network Time Protocol server, configure enabled for NTPEnable:
      ```
      NTPEnable=enabled
      ```
Alternatively, reduce transmission time by exporting the \([\text{SystemDate/Time}]\) 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 Main Module.** To transfer the .ini file to another Main Module, do either of the following:

- From the Web interface of the receiving Main Module, select the **Administration** tab, **General** on the top menu bar, and **User Config File** on the left navigation menu. Enter the full path of the file, or use **Browse**.
- Use any file transfer protocol supported by Main Modules (i.e., FTP, FTP Client, SCP, or TFTP). The following example uses FTP:
  a. From the folder containing the copy of the customized .ini file, use FTP to log in to the Main Module 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 Main Module:
     
     ```
     ftp> put filename.ini
     ```

**Exporting the file to multiple Main Modules.** To export the .ini file to multiple Main Modules:

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single Main Module.
- 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 **Utility CD**.
The Upload Event and Error Messages

The event and its error messages

The following event occurs when the receiving Main Module 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 Main Module succeeds, and additional event text states the error.

<table>
<thead>
<tr>
<th>Event text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration file warning: Invalid keyword on line</td>
<td>A line with an invalid keyword or value is ignored.</td>
</tr>
<tr>
<td>number.</td>
<td></td>
</tr>
<tr>
<td>Configuration file warning: Invalid value on line</td>
<td></td>
</tr>
<tr>
<td>number.</td>
<td></td>
</tr>
<tr>
<td>Configuration file warning: Invalid section on line</td>
<td>If a section name is invalid, all keyword/value pairs in that section are ignored.</td>
</tr>
<tr>
<td>number.</td>
<td></td>
</tr>
<tr>
<td>Configuration file warning: Keyword found outside of</td>
<td>A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.</td>
</tr>
<tr>
<td>a section on line number.</td>
<td></td>
</tr>
<tr>
<td>Configuration file warning: Configuration file exceeds</td>
<td>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.</td>
</tr>
<tr>
<td>maximum size.</td>
<td></td>
</tr>
</tbody>
</table>
Messages in config.ini

A device associated with the Main Module 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 Main Modules, 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 Main Modules 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 Main Module:

• 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 Main Modules support the same features in the same manner.

Firmware files (Main Module)

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

The APC Operating System (AOS) and application module files used with the Main Module 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 Main Module.
• `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](http://www.apc.com/tools/download). At this Web page, find the latest firmware release for your APC product (in this case, the Environmental Manager Main Module) 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 Main Modules by using the separate AOS and application firmware modules.

Obtain the firmware modules from [www.apc.com/tools/download](http://www.apc.com/tools/download).

**Firmware File Transfer Methods**

To upgrade the firmware of a Main Module, 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 Main Module that is not on your network, use XMODEM through a serial connection to transfer the individual firmware modules from your computer to the Main Module.

When you transfer individual firmware modules, **you must** transfer the APC Operating System (AOS) module to the Main Module before you transfer the application module.
Using FTP or SCP to upgrade one Main Module

FTP. For you to use FTP to upgrade one Main Module over the network:

• The Main Module 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 Main Module.

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:\>ftp

3. Type **open** and the Main Module’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.** To use Secure CoPy (SCP) to upgrade firmware for a Main Module:

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 Main Module. 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 Main Module.

**Upgrading multiple Main Modules**

**Export configuration settings.** You can create batch files and use an APC utility to retrieve configuration settings from multiple Main Modules and export them to other Main Modules.

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

**Use FTP or SCP to upgrade multiple Main Modules.** To upgrade multiple Main Modules using an FTP client or using SCP, write a script which automatically performs the procedure.
Using XMODEM to upgrade one Main Module

To upgrade the firmware for a Main Module 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 provided serial cable to the selected port and to the serial port at the Main Module.

4. Run a terminal program such as HyperTerminal, and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.

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 9600. The Main Module 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 (Main Module).
Verifying Upgrades

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 Last Transfer Result, or use an SNMP GET to the mfiletransferStatusLastTransferResult OID.

Last Transfer Result codes

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

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.
Product Information

Two-Year Factory Warranty

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

Terms of warranty

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

Non-transferable warranty

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

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

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, BY OPERATION OF LAW OR OTHERWISE, OF PRODUCTS SOLD, SERVICED OR FURNISHED UNDER THIS AGREEMENT OR IN CONNECTION HEREWITH. APC DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTION AND FITNESS FOR A PARTICULAR PURPOSE. APC EXPRESS WARRANTIES WILL NOT BE ENLARGED, DIMINISHED, OR AFFECTED BY AND NO OBLIGATION OR LIABILITY WILL ARISE OUT OF, APC RENDERING OF TECHNICAL OR OTHER ADVICE OR SERVICE IN CONNECTION WITH THE PRODUCTS. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES AND REMEDIES. THE WARRANTIES SET FORTH ABOVE CONSTITUTE APC’S SOLE LIABILITY AND PURCHASER’S EXCLUSIVE REMEDY FOR ANY BREACH OF SUCH WARRANTIES. APC WARRANTIES EXTEND ONLY TO PURCHASER AND ARE NOT EXTENDED TO ANY THIRD PARTIES.
IN NO EVENT SHALL APC, ITS OFFICERS, DIRECTORS, AFFILIATES OR EMPLOYEES BE LIABLE FOR ANY FORM OF INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, ARISING OUT OF THE USE, SERVICE OR INSTALLATION, OF THE PRODUCTS, WHETHER SUCH DAMAGES ARISE IN CONTRACT OR TORT, IRRESPECTIVE OF FAULT, NEGLIGENCE OR STRICT LIABILITY OR WHETHER APC HAS BEEN ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES. SPECIFICALLY, APC IS NOT LIABLE FOR ANY COSTS, SUCH AS LOST PROFITS OR REVENUE, LOSS OF EQUIPMENT, LOSS OF USE OF EQUIPMENT, LOSS OF SOFTWARE, LOSS OF DATA, COSTS OF SUBSTITUENTS, CLAIMS BY THIRD PARTIES, OR OTHERWISE.

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

Warranty claims

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

General policy

American Power Conversion (APC) does not recommend the use of any of its products in the following situations:

- In life-support applications where failure or malfunction of the APC product can be reasonably expected to cause failure of the life-support device or to affect significantly its safety or effectiveness.
- In direct patient care.

APC will not knowingly sell its products for use in such applications unless it receives in writing assurances satisfactory to APC that (a) the risks of injury or damage have been minimized, (b) the customer assumes all such risks, and (c) the liability of APC is adequately protected under the circumstances.

Examples of life-support devices

The term *life-support device* includes but is not limited to neonatal oxygen analyzers, nerve stimulators (whether used for anesthesia, pain relief, or other purposes), autotransfusion devices, blood pumps, defibrillators, arrhythmia detectors and alarms, pacemakers, hemodialysis systems, peritoneal dialysis systems, neonatal ventilator incubators, ventilators (for adults and infants), anesthesia ventilators, infusion pumps, and any other devices designated as “critical” by the U.S. FDA.

Hospital-grade wiring devices and leakage current protection may be ordered as options on many APC UPS systems. APC does not claim that units with these modifications are certified or listed as hospital-grade by APC or any other organization. Therefore these units do not meet the requirements for use in direct patient care.
# Index

## A

About option, Main Module information
- in control console 17
- in Web interface 80

Access
- account types 4
- method determined by SSL certificate 19
- priority for logging on 3
- to control console 51
- to event log from control console 15
- to FTP server 57
- to Web interface 49

Alarm mapping
- beacons 34
- relay outputs 35

A-Link
- alarm messages 9
- clearing alarms 10
- ports 7

Analog sensors 32
- calibration 32
- not mass-configurable 31
- thresholds 32

Apply Local Computer Time 75

Authenticate Traps setting 64

Authenticate users through RADIUS 38

Automatic log-off for inactivity 41

## B

Beacons
- alarm mapping 34, 35, 36
- configuring 33
- mass-configuration 34
- testing 35
- viewing status 33

BOOTP
- request cycle in progress 14
- using server to provide TCP/IP settings 42

Browsers supported 18

## C

Calibrating analog sensors 32

Certificate
- adding, replacing, or removing 50
- viewing 50

Community Name
- for trap receivers 64
- config.ini file. See User configuration files.

Configuring
- proxy server before using Web interface 18
- RADIUS authentication 38

Contact information (whom to contact) 75

Control console
- configuring access 51
- Device Manager menu 16
- navigating menus 15
- Network menu 17
- refreshing menus 15
- System menu 17

## D

Data log
- displaying and using 69
- graphing data records 69
- importing into spreadsheet 72
- rotation (archiving) 71
- using FTP or SCP to retrieve 72

Date & Time settings 75

Date format 75
Daylight Saving Time configuration 76
Device configuration 24
Device IP Configuration Wizard
   installation and system requirements 81
   using the wizard
      for local configuration 83
      for remote configuration 82
Device Manager menu in control console 16
DHCP
   APC cookie 44
   response options 44
   using server to provide TCP/IP settings 42
Digital sensors, configuring 33
Disable
   access to FTP server 57
   alarm generation, digital sensors 33
   alarm generation, dry contact sensors 33
   alarm generation, temperature sensor 27
   e-mail to a recipient 63
   encryption algorithms for SSH 51
   reverse lookup 68
Telnet 51
   use of a proxy server 18
   Web interface 49
DNS
   defining host and domain names 47
   query types 48
   specifying DNS servers by IP address 47
Dry contacts, configuring 33

E
E-mail
   configuring notification parameters 61
   configuring recipients 63
   test message 63
   using for paging 63
Enable
   access to FTP server 57
   alarm generation, digital sensors 33
   alarm generation, dry contact sensors 33
   alarm generation, temperature sensor 27
   e-mail forwarding to external SMTP servers 63
   e-mail to a recipient 63
   encryption algorithms for SSH 51
   JavaScript for your Web browser 18
   reverse lookup 68
Telnet 51
   versions of SSH 51
   Web interface 49
Encryption algorithms, SSH 51
Error messages
   for firmware file transfer 94
   for Web access attempts 20
   from overridden values in .ini file 88
Ethernet port speed 46
Event actions 58
   configuring by event 59
   configuring by group 60
Event log
   accessing from control console 15
   displaying and using 67
   errors from overridden values in .ini file 88
   using FTP del command 74
   using FTP or SCP to retrieve 72
   event.txt file
      contents 72
      importing into spreadsheet 72

F
Facility Code (Syslog setting) 66
Factory information 80
File transfers
   to upgrade firmware 89
   verification 94
Filters
   configuring 29
   for module view 26
   for system view 25
Firmware
  benefits of upgrading  89
  file transfer methods
    automated upgrade tool  90
    FTP or SCP  91
    XMODEM  93
  files for the Main Module  89
  obtaining the latest version  90
  upgrading multiple Main Modules  92
  verifying upgrades and updates  94
  versions displayed, control console main
    screen  13
  versions displayed, Web interface  80
From Address (SMTP setting)  62
FTP
  server settings  57
  transferring firmware files  91
  using to retrieve event or data log  72
G
Graphing logged data  69
H
Hardware
  alarms  9
  information  80
Help
  in control console  15
  in Web interface  22
Host keys
  adding or replacing  52
  status  52
Host name of trap receivers  64
Hysteresis  32
I
Identification fields on main screen  14
Inactivity timeout  41
ini files, See User configuration files
Inputs  30
J
JavaScript
  enabling for your Web browser  18
  required to launch log in new window  67
K
Keywords in user configuration file  84
L
Last Transfer Result codes  94
Launch Log in New Window, JavaScript
  requirement.  67
LED
  Identifier Number  24
  Link  7
  Power  7
  Status  7
Life support policy  98
Links, configuration  79
Local SMTP Server
  defining by IP address or DNS name  62
  recommended option for routing e-mail  63
Local Users, setting user access  37
Location (system value)  75
Logging on
  control console  11
  DNS Name or IP address matched to
    common name  19
  error messages for Web interface  20
  Web interface  18
Login date and time in control console  14
Loopback address, not allowed as default
gateway  2
Main screen information and status fields 14

Menus
  control console 16
  General 75
  Home 24
  Logs 58
  Network 42
  Outputs 33
  Security 37
  Sensors 27

Message Generation (Syslog setting) 66
MIB-II Identification variables 75

Modbus
  configuration 78
  register map 78

Module configuration 24
Module view 26

Network Time Protocol (NTP) 75
NMS IP/Host Name for trap receivers 64
Notification 58
  delaying or repeating 59

Outputs
  beacons 33
  relay output 35
  switched outlet 36

Override keyword, user configuration file 84

Paging by using e-mail 63
Passwords
  default for all account types 37
  defining for each account type 37
  for data log repository 71
  recovering from lost password 5
  shadow passwords with RADIUS on UNIX 41

Port speed, configuring for Ethernet 46
Ports
  FTP server 57
  HTTP and HTTPS 49
  RADIUS server 39
  Telnet and SSH 51

Primary NTP Server 75
Proxy servers
  configuring not to proxy the Main Module 18
  disabling use of 18

Quick Links, configuration 79

RADIUS
  server configuration 40
  settings 39
  supported servers 41

RADIUS Server setting 39
Rate of change settings for sensors 29
Rear panel components 6
Reboot Management Interface 78
Recipient SMTP server 63
Relay outputs, configuring 35
Remote Monitoring Service 79
Remote Users
  setting user access 40
Remote users 38
  authentication 38
Remote users, authentication 38
Reset Only Event Configuration 79
Reset Only TCP/IP to Defaults 79
Reset to Defaults 78
Reset to Defaults Except TCP/IP  79
Reverse lookup  68

S
SCP
   for high-security file transfer  57
   transferring firmware files  91
   using to retrieve event or data log  72
Secondary NTP Server  75
Section headings, user configuration file  84
Security menu  37
Sensor  27
   analog  32
   dry contact/digital sensor  33
   humidity  27
   temperature  27
Serial Modbus. See Modbus
Setup
   initial  2
Severity Mapping (Syslog setting)  66
SMTP server
   selecting for e-mail recipients  63
   settings  62
SNMP
   access and access control
      SNMPv1  54
      SNMPv3  55
   authentication traps  64
   disabling SNMPv1  53
SSH
   client programs  52
   encryption algorithms  51
   host key  52
   host keys  52
SSL
   adding, replacing, or removing
      a certificate  50
   certificates  50
   configuring cipher suites  49
Status
   beacons  33
      control console main screen  14
      Web interface  21
Switched outlet, configuring  36
Synchronize with NTP Server, (Date & Time)  75
Syslog
   identifying the Syslog server and port  65
   mapping event severity to Syslog priorities  66
   settings  66
      test  66
System Name  75
System view  25

T
TCP/IP
   configuration  42
      restoring default settings  79
TCP/IP and communication settings  42
Temperature scale (Fahrenheit or Celsius)  77
Temperature/Humidity Sensors
   configuring  27
      mass-configuration  29
      rate of change  29
      thresholds  28
Test
   DNS query  48
   e-mail recipient settings  63
   RADIUS server path  39
   Syslog  66
   trap receiver  65
Threshold settings
   analog sensors  32
   temperature/humidity sensors  28
Time setting  75
Time Zone, for synchronizing with NTP server 76
Timeout setting for RADIUS 39
To Address, E-mail Recipients 63
Trap generation, for trap receivers 64
Traps
  trap receivers 64
Troubleshooting
  problems logging on to Web interface 19
  proxy server problems 18
Types of user accounts 4

U
Up time on control console main screen 14
Update Interval, Date & Time setting 76
Update Using NTP Now, Date & Time setting 76
Upgrading firmware 89
Upload event 87
URL address formats 20
User access identification, control console main screen 14
User configuration files
  contents 84
  customizing 85
  exporting system time separately 85
  messages for undiscovered devices 88
  overriding device-specific values 84
  retrieving and exporting 84
  upload event and error messages 87
  using file transfer protocols to transfer 86
  using the APC utility to retrieve and transfer the files 85, 92
User Inputs
  analog 32
  configuring 30
  digital 33
  dry contact 33
User names
  defining for each account type 37
  maximum number of characters 37
  maximum number of characters for RADIUS 38
  maximum number of characters for RADIUS 38

V
Verifying firmware upgrades 94

W
Watchdog features 8
Web browsers supported 18
Web interface
  configuring access 49
  logging on 18
  logon error messages 20
  URL address formats 20
Wildcard characters 29, 31

X
XMODEM to transfer firmware files 93
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
    APC headquarters U.S., Canada Latin America
    (1)(877)537-0607 (1)(800)800-4272 (1)(401)789-5735
    (toll free) (toll free) (USA)
    Europe, Middle East, Africa
    Western Europe (inc. Scandinavia)
    Japan Australia, New Zealand, South Pacific area
    (353)(91)702000 +800 0272 0272 (0) 36402-2001 (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

Entire contents copyright 2007 American Power Conversion Corporation. All rights reserved. Reproduction in whole or in part without permission is prohibited. APC, the APC logo, InfraStruXure, and PowerNet are trademarks of American Power Conversion Corporation. All other trademarks, product names, and corporate names are the property of their respective owners and are used for informational purposes only.