Environmental Monitoring Unit

AP9312TH
AP9312THi

User's Guide

APC®

Environmental Monitoring Unit

Contents

Contents

Contents

Environmental Monitoring Unit

Managing the Unit

Introduction

Available interfaces

The stand-alone Environmental Monitoring Unit performs continuous temperature and humidity sensing and contact monitoring. You can manage the unit through Web, Control Console, or SNMP interfaces.

- Remotely, you can manage the unit with a Web browser using the Web interface or with Telnet using the Control Console interface.
- Locally, you can manage the unit through a serial interface, using the Control Console.

Note: For information on using SNMP to manage the Environmental Monitoring Unit, see **page 23**.

Configuring network settings

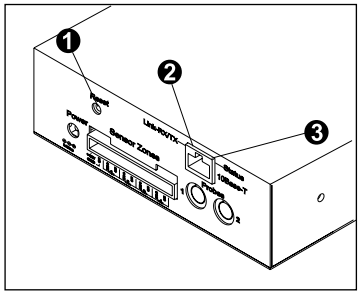
Before you manage the Environmental Monitoring Unit remotely, you must configure it with the proper network settings. See the *Environmental Monitoring Unit Installation and Quick Start Manual*, included in printed form and on this CD in PDF.

Managing the Unit

LEDs and the Reset Button

Front Panel Features

The reset button and two LEDs are on the front panel of the Environmental Monitoring Unit.



Descriptions

No.	Feature	Description
❶	Reset button	Reinitializes the unit's network interface.
❷	Link-RX/TX LED	*Off:* The device that connects the unit to the network (a router, hub, or concentrator) is off or not operating correctly.
		Flashing green: The unit is receiving data packets from the network.
❸	Status LED	*Off:* The unit has no power.
		Solid green: The unit has valid network settings.
		Flashing green: The unit does not have valid network settings.
		Solid red: A hardware failure has been detected in the unit.
		Blinking Red (Slowly): The unit is making BOOTP requests.

Managing the Unit

Web Interface

System requirements

To access the Web interface, you need one of the following supported Web browsers:

- Internet Explorer 3.0.2 and later
- Netscape 3.0 and later

Note: Some Web interface features (data verification, APC Interactive Assistant, and MD5 authentication) require that you enable Java Script and/or Java. For MD5 to function properly, you must also have cookies enabled on your Web browser.

Access to the Web interface

Only one user at a time may access the Environmental Monitoring Unit. Serial interface users have precedence over Telnet users and Telnet users have precedence over Web users.

In the URL Location field of your Web browser, type `http://` followed by your unit's IP address. For example:

```
http://170.241.17.51
```

Note: Alternatively, you can enter the DNS name (if a DNS server entry is configured for the unit's management card).

If the unit's Web port is set to a value other than 80, enter the System IP address, a colon and the port value (in this example 8000).

```
http://170.241.17.51:8000
```

Logging in

After entering the Environmental Monitoring Unit's IP address, press ENTER. At the prompts, enter your user name and password (**apc** by default for both).

Note: To change the user name, password, or time-out value, see **User Manager on page 16**.

Managing the Unit

Control Console

Options for using the Control Console

The Control Console provides comprehensive management of the unit by one of the following modes of access:

- Telnet, for remote management
- A serial interface for local management

Access to the Control Console

Only one user at a time may access the Environmental Monitoring Unitt. Serial interface users have precedence over Telnet users, and Telnet users have precedence over Web users.

Use a serial interface to access the Control Console:

1. Use the supplied configuration cable (APC part number 940-0120) to connect the terminal port to one of the Probe Ports on the Environmental Monitoring Unit.
2. Set the terminal port for the following communication settings:

Baud Rate	2400
Data Bits	8
Stop Bits	1
Parity	None
Handshaking	None
Local Echo	Off
Terminal Type	ANSI (VT100)

3. To change the communications settings using HyperTerminal:
   a. Make the needed changes.
   b. Select **Disconnect** in the **Call** menu.
   c. Select **Connect** in the **Call** menu.
   d. Press ENTER
4. Log into the Control Console. (See **Logging in on this page**.)

Logging in

When prompted, enter the Administrator user name and password (**apc**, by default, for both).

To change the user name, password, or timeout value, see **User Manager on page 16**.

Continued on next page

Managing the Unit

Control Console *continued*

Navigating the menus

Within the menu structure:

- To select a menu item, type the item number, then press ENTER.
- To save changes to configurable values, use the **Accept Changes** menu option.
- To refresh the current menu, Press ENTER.
- To go to the previous menu, Press ESC.
- to access brief descriptions of the current menu items, Type ? and then press ENTER (if the menu has help available).
- To return to the main Control Console menu, use CTRL-C.

Managing the Unit

Password-Protected User Accounts

Types of accounts

The Environmental Monitoring Unit provides two password-protected accounts, Administrator and Device Manager, that allow you to control access to the device. To configure the accounts, see **User Manager on page 16**

Account access to management menus

Management Menus	Account Type	
	Administrator	Device Manager
Environmental Monitoring	Yes	Yes
Event Log	Yes	Yes
Network	Yes	No
System	Yes	No
Logout	Yes	Yes
Help	Yes	Yes
Link	Yes	Yes

Menu Items

Introduction

Interface similarities and differences

The information in this section is based on the Web interface. The Control Console interface varies slightly, but offers the same capabilities for managing the Environmental Monitoring Unit.

Your access to menus is determined by the account under which you logged in. See **Password-Protected User Accounts on page 6**.

Contents of this section

This section provides information on the following menus:

Note: To manage the unit with SNMP, see **page 23**.

Menu Items

Environmental Monitoring

Purpose

Use the Environmental Monitoring menu to configure settings for monitoring contact closures and for obtaining information about the temperature and humidity sensed by up to two probes.

Status: probes

Item	Definition
Temperature	Reports the temperature (Celsius) sensed by the unit's probes.
High Temperature Violation	Reports whether current temperature exceeds the high temperature threshold (**Yes** or **No**) or reports that the threshold is disabled.
Low Temperature Violation	Reports whether current temperature violates the low temperature threshold (**Yes** or **No**) or reports that the threshold is disabled.
Humidity	Reports the relative humidity (as a percentage) sensed by the unit's probes.
High Humidity Violation	Reports whether current humidity exceeds the high humidity threshold (**Yes** or **No**) or reports that the threshold is disabled.
Low Humidity Violation	Reports whether current humidity violates the low humidity threshold (**Yes** or **No**) or reports that the threshold is disabled.
Trap Thresholds	Defines the thresholds for high and low temperature (in Celsius) and for relative humidity (as a percentage) that the unit uses to identify a trap condition.
Send Traps On	Enables or disables sending traps for each threshold.

Continued on next page

Menu Items

Environmental Monitoring *continued*

Status: contacts

Item	Definition
Device 1 (Contact Zone 1) Alarm through Device 4 (Contact Zone 4) Alarm:	For each contact by number and name, reports whether the contact senses an alarm condition (**Yes** or **No**) or that the alarm is disabled .

Status: firmware version

The status section also reports the firmware version of the Environmental Monitoring Unit.

Configuration

Item (for each probe)	Definition
Trap Threshold Options	Defines the thresholds for high and low temperature (in Celsius) and relative humidity (as a percentage) that the unit uses to identify a trap condition. (You must enable the **Send Traps** item for the unit to react to the alarm.)
Contact Name 1–4	Defines a name of up to 16 characters for each contact.
Contact Zone 1–4	Enables or disables the contacts.

Menu Items

Events

Viewing the Event Log directly

The Event Log displays information for the Environmental Monitoring Unit's last 300 events.

Item	Description
Date	The date on which the event occurred (*DD*/*MM*/*YYYY*)
Time	The time at which the event occurred (*HH*:*MM*:*SS*)
Event	Description of the event. For detailed descriptions of event codes, select APC Interactive Assistant from the Navigation Bar on the Web interface and read the page about event codes.

To view the Event Log, select the **Log** option of the **Events** menu in the Web interface or press CTRL + L in the Control Console.

Retrieving the Event Log using FTP

To retrieve the Event Log using client side FTP:

1. From an MS-DOS prompt, type `ftp` *`card-ip`*, where *`card-ip`* is the IP address of the Environmental Monitoring Unit.
2. Log in to the unit's FTP server
3. type `dir` to list files.
4. To retrieve the Event Log, type `get event.txt`. The Environmental Monitoring Unit transmits the Event Log, which includes at least the last 300 events, to your local drive. A confirming message simiar to the following is displayed.

   ```
   ftp: 3694 bytes received in 0.11 Seconds
   33.58Kbytes/sec.
   ```

Viewing the event.txt file

You can use a spreadsheet program to view the ***event.txt*** file. The file is TAB-delimited to appear in columns in the spreadsheet.

Note: To display the year in 4-digit format in the spreadsheet, be sure to select that date format in the spreadsheet application.

The ***event.txt*** file contains the following information that is not displayed in the Web and Control Console Event Log screens.

- The version of the ***event.txt*** file format (first field).
- The Date and Time the ***event.txt*** file was retrieved.
- The Name, Contact, Location, and IP address of the unit's management card.
- An unique Event Code for every type of event.

Continued on next page

Menu Items

Events *continued*

Deleting the Event Log in the FTP interface

To delete the Event Log, type `del event.txt`. FTP confirms the deletion:

```
Requested file action okay, completed.
```

A new ***event.txt*** file is immediately created to record the Deleted Log event.

Recipients (Web interface only)

Use the **Recipients** option of the **Events** menu to configure email recipients who will be notified when an event occurs. See **Configuring Email Recipients on page 21**. (In the Control Console, use the **Email** option on the **Network** menu instead.)

Menu Items

Network

Purpose

The **Network** menu provides access to the configurable network settings. Only the Administrator can access the **Network** menu.

TCP/IP

The TCP/IP section lists the Environmental Monitoring Unit's start-up settings for network service and allows you to configure TCP/IP settings.

Item	Definition
System IP	The unit's Internet Protocol address, which is a numeric address that the domain name server translates into a domain name.
Subnet Mask	A 32-bit character string used to select some of the bits from an Internet address to route it to the subnet.
Default Gateway	A device that connects two computer networks that use different protocols so that the connected networks can exchange data. Default: Router address
BOOTP	A protocol used to enable a diskless workstation to find its own logical IP address at startup. Settings: Enabled/Disabled

TFTP/FTP

Use the TFTP/FTP section to control file transfers through the settings for the TFTP and FTP Client and FTP Server.

Client or Server	Item	Definition
TFTP Client	Remote Server IP:	The network address of the TFTP server used for downloads.
FTP Client	Remote Server IP:	The network address of the FTP server used for downloads.
	User Name	The user name for access to the FTP server.
	Password:	The password for access to the FTP server.
FTP Server	Access:	Enables or disables FTP server access.
	Port:	The TCP/IP port on which the FTP server for the unit's management card is located. Default: port 21

Continued on next page

Menu Items

Network *continued*

Telnet/Web

Item	Definition
Telnet	
Access	Enables or disables Telnet access.
Port	The TCP/IP port where the Telnet server for the unit is located. Default: port 23
Web	
Access	Enables or disables Web access.
Port	The TCP/IP port where the Web server for the unit is located. Default: port 80

Continued on next page

Menu Items

Network *continued*

SNMP

The SNMP section displays the SNMP access control and trap receiver Settings.

Item	Definition
SNMP Access	Enables or disables SNMP access.
Access Control	Controls access to each of the four SNMP channels.
Trap Receiver	Defines the NMSs (up to 4) to which traps are sent.

Access Control . The Access Control section of SNMP displays the current settings for all four SNMP channels and lets you configure values for a selected channel.

Item	Definition
Community Name	Password that the NMS specified by the **NMS IP** option must use for SNMP access to the unit. The **Access Type** option defines the allowed access. Note: Allows a maximum of 15 characters.
NMS IP	Configures the channel to allow only one NMS (using a specific NMS IP address), or all NMSs (using 0.0.0.0 for the NMS IP value), to have access to the channel.
Access Type	Defines whether the NMS identified by the NMS IP option can write (use GETs and SETs) or read (use only GETs) or is disabled (cannot use GETs or SETs).

Trap Receiver. The Trap Receiver section of SNMP displays and lets you configure the current settings for all four trap receivers.

Item	Definition
Community Name	The password that the unit uses when it sends traps to the NMS identified by the **Receiver NMS IP** option. Maximum length: 15 characters.
Receiver NMS IP	The specific NMS (defined by its IP address) to receive traps sent by the unit. Note: To send no traps to any NMS, set the Trap Receiver IP to 0.0.0.0
Trap Generation	Enables or disables the sending of traps to the NMS identified by the **Receiver NMS IP** option.
Authentication Traps	Enables or disables the sending of authentication traps to the NMS identified by the **Receiver NMS IP** option.

Continued on next page

Menu Items

Network *continued*

Email (Control Console only)

Use the **Email** option of the **Network** menu to configure email recipients who will be notified when an event occurs. See **Configuring Email Recipients on page 21**. (In the Web interface, use the **Recipients** option of the **Events** menu instead.)

Menu Items

System

Purpose

Use the **System** menu to configure accounts, system identification, file transfers, and links. Only the Administrator has access to the **System** menu.

User Manager

Use this section to configure the properties of the Administrator and Device Manager accounts. The Administrator has unrestricted access, but the Device Manager can configure only the Environmental Monitoring Unit; not the network and system parameters.

Item	Definition
Auto Logout	How long you can be inactive before the system automatically logs you out. Default: 3 minutes.
Authentication	**Basic** (the default) causes the Web Interface to use standard HTTP 1.1 login (base64 encoded passwords) **MD5** causes the Web Interface to use an MD5-based authentication login. (For MD5 to function properly, you must have cookies enabled on your browser.)
Administrator	
User Name	User name (10 characters maximum). Default: **apc**
Password	Password only for HTTP 1.1 authentication (10 characters maximum). Default: **apc**
Authentication Phrase	Authentication phrase (only for MD5). The phrase must be from 15 to 32 characters. Default: **admin user phrase**
Device Manager User	
User Name	User name (10 characters maximum). Default: **apc**
Password	Password only for HTTP 1.1 authentication (10 characters maximum). Default: **apc**
Authentication Phrase	Authentication phrase for MD5. The phrase must be from 15 to 32 characters. Default: **device user phrase**

Continued on next page

Menu Items

System *continued*

Identification

Use this section to display and configure the unit's system identification values. The following items are configurable:

Item	Definition
Name	The unit's system name (used as the SNMP MIB-II **sysName** OID).
Contact	The unit's contact or owner (used as the SNMP MIB-II **sysContact** OID.
Location	The unit's physical location (used as the SNMP MIB-II **sysLocation** OID

Date/Time

Item	Definition
Date	The date for the system in the form of *MM/DD/YYYY*.
Time	The time for the system in the form of *HH:MM:SS* (24 hour time).

Continued on next page

Menu Items

System *continued*

File Transfer

Item	Description
Display the current transfer settings	
Remote TFTP Server IP	IP address of the remote TFTP server defined in the **Network** menu's TFTP/FTP settings. TFTP: Remote Server IP
Remote FTP Server IP	IP address of the remote FTP server defined in the **Network** menu's TFTP/FTP settings. FTP: Remote Server IP
Remote FTP ServerUser Name	User name of the FTP server defined in the **Network** menu's TFTP/FTP settings. FTP Client: User Name
Remote FTP Server Password	Password of the FTP server defined in the **Network** menu's TFTP/FTP settings. FTP Client: Password
Configure the Name of the File to Download	
Filename	The name of the file to be downloaded
Initiate the Transfer	
Result of Last File Transfer	Display the results of the last file transfer.
Initiate File Transfer Via	Choose to transfer the file by TFTP or FTP.

Menu Items

System *continued*

Tools

Item	Description
No Action	Causes no action.
Reboot Card	Re-initializes the unit's management card.
Reset Card to Defaults	Restores all configuration settings to their defaults, including user accounts, and enables BOOTP.
Reset Card to Defaults Except TCP/IP	Restores all configuration settings (except TCP/IP) to their defaults.

Links (Web Interface only)

Use this section to configure URL links that appear on the Navigation menu at the left. (The APC Links are pre-defined, but can be changed.)

Item	Definition
Configure the User Links	
Name	For each link, the name that will appear on the menu bar.
URL	The HTTP link in URL form: **http://mysite.com/mypage.com**.
Configure the APC Links	
Name	View the names of the APC links.
URL	Define the URL of each APC link.

Menu Items

Help

Help options

In the Web interface:

- The **Help** menu is at the lower left.
- The Contents page provides an overview of parameters that you can display and configure.
- To access help about a page, click the ? at the end of the black title bar of that page.

In the Control Console, type ? for help about the current menu.

Interactive Assistant

Interactive Assistant brings APC Customer Service to the Web. When you select Interactive Assistant, the Environmental Monitoring Unit transmits information about the Environmental Monitoring Unit's management card to APC's Interactive Assistant server. The server informs you if a newer version of firmware is available and can link you to extensive context-sensitive help.

About Card

About Card displays information about the Environmental Monitoring Unit's hardware, application module, and APC OS, including the serial number, hardware revision, and the date and time at which the AOS was loaded.

Configuring and Using Email Notification

Configuring Email Recipients

Menu options

To identify up to four email recipients, use one of the following:

- The **Recipients** option of the Web interface's **Events** menu
- The **Email** option of the Control Console's **Network** Menu

Settings

Setting	Description
To Address	Defines the user and domain names of the recipient. To use email for paging, use the email address for the recipient's pager gateway account (for example, **myacct100@skytel.com**). The pager gateway generates the page. **Note:** The recipient's pager must be able to use text-based messaging.
Send via	Lets you choose one of the following methods for routing email: • Send email through the Environmental Monitoring Unit's SMTP server. Selecting **Local SMTP Server**, which is the recommended option, ensures that the email is sent before the unit's 20-second timeout, and, if necessary, is retried several times. • Send email directly to the recipient's remote SMTP server. If you select the **Recipient's SMTP Server** option, and the remote SMTP server is busy, the timeout may prevent some email from being sent, With this option, the management card tries to send the email only once. When the recipient uses the Environmental Monitoring Unit's SMTP server, this setting has no effect.
Email Generation	Enables (by default) or disables sending email to the defined recipient.

Configuring the local SNMP server

When you select the **Local SNMP Server** option for the **Send via** setting, you must do one of the following:

- Make sure that forwarding is enabled at that server so that the server can route email to external SMTP servers.

  Note: Always see your SMTP-server administrator before changing the configuration of your SMTP server.
- Set up a special email account for the Environmental Monitoring Unit. This account then forwards the Email to an external email account.

Testing Email

In the Web interface, use the **Email Test** option to send a test email message to a configured recipient.

Configuring and Using Email Notification

Configuring SMTP and DNS Settings

Requirements for using SMTP

To use the Simple Mail Transfer Protocol (SMTP) to send email when an event occurs, you must define the following settings:

- The IP address of the Domain Name Service (DNS) server.
- The DNS name of the SMTP server and the **From Address** settings for SMTP.
- The email addresses for a maximum of four recipients.

Note: To page an email recipient who uses a text-based pager gateway, see the description of the **To Address** setting in **Settings on page 21**.

DNS server

To enable the Environmental Monitoring Unit to send email messages, you must use the **TCP/IP & DNS** option (Web interface) or **DNS** option (Control Console) in the **Network** menu to identify the Domain Name Service (DNS) server by its IP address.

If the unit does not receive a response from the DNS server within five seconds, email cannot be sent. Therefore, use a DNS server on the same segment as the unit or on a nearby segment (but not across a WAN).

After you define the DNS server's IP address, verify that DNS is working correctly by entering the DNS name of a computer on your network to obtain the IP address for that DNS name.

SMTP settings

The **Email** option in the **Network** menu accesses the following SMTP settings:

Setting	Description
SMTP Server	The DNS name of the SMTP server.
From Address	The contents of the **From** field in the email messages sent by the Environmental Monitoring Unit. **Note:** See the documentation for your SMTP server to determine whether you must you use a valid user account on the server for this setting.

Managing the Unit with SNMP

SNMP Interface

Purpose

You can use PowerNet MIB OIDs to manage (monitor, configure, and control) your Environmental Monitoring Unit.

PowerNet MIB OID categories

Use your MIB browser to locate the PowerNet MIB OIDs that you can use to manage the Environmental Monitoring Unit:

1. Select **[product]** under **[apc]**.
2. Select **[hardware]**.
3. Select **[measureUps]** to list the following two OID categories:

OID	Function
[mUpsEnviron]	Displays information about the ambient temperature and relative humidity.
[mUpsContact]	Defines contact values.

Managing the Unit with SNMP

Using the OIDs

Using monitoring OIDs

Use the read-only **[mUpsEnviron]** OIDs to view temperature and humidity values.

OID	Function
mUpsRelativeHumidity	Reports the relative humidity sensed by the probes.
mUpsAmbientTmperature	Reports the ambient temperature in Celsius, sensed by the probes.

Using contact OIDs

Use the **[mUpsContact]** OIDs to view and configure the current contact sensor values.

OID	Function
mUpsContactNumContacts	Lists how many contact sensors the unit uses.
{mUpsContactTable}	Lists the OIDs for each contact sensor: **contactNumber**: Identifies the contact sensor for which the other OIDs apply. **normalState**: Defines the contact sensor's normal condition (unknown, open, or closed). **description**: Defines the purpose of the contact sensor **monitoringStatus**: Defines whether the contact sensor is being monitored **currentStatus**: Identifies the sensor's current condition (unknown, noFault, or fault).

Security

Security Features

Planning and implementing security features

As a network device that passes information across the network, the Environmental Monitoring Unit is subject to the same exposure as other devices on the network.

Use the information in this section to plan and implement the security features appropriate for your environment.

Port assignments

If a Telnet, FTP, or Web server uses a non-standard port, a user must specify the port when using the client interface, such as a Web browser. The non-standard port address becomes an extra "password," hiding the server to provide an additional level of security. The TCP ports for which the Telnet, FTP, and Web servers listen are initially set at the standard "well known ports" for the protocols.To hide the interfaces, use any port numbers from 5000 to 65535.

For an example of how to access a client interface for which the port is non-standard, see **Access to the Web interface on page 3**.

User names, passwords, community names

All user names, passwords, and community names for SNMP are transferred over the network as plain text. A user who is capable of monitoring the network traffic can determine the user names and passwords required to log into the Environmental Monitoring Unit's Control Console or Web interface as an Administrator or Device Manager. This security limitation of the protocols affects any device using Telnet, a Web server, or an SNMP version 1 agent.

Security

Authentication

Authentication versus encryption

The Environmental Monitoring Unit controls access by providing basic authentication through user names, passwords, and IP addresses, but provides no type of encryption. These basic security features are sufficient for most environments, in which sensitive data is not being transferred. To ensure that data and communication between the Environmental Monitoring Unit and the client interfaces, such as Telnet and the Web browser, cannot be captured, you can provide a greater level of security by enabling MD5 authentication for the Web interface. See **MD5 authentication (Web interface) on this page**.

MD5 authentication (Web interface)

The Web interface option for MD5 authentication enables a higher level of access security than the basic HTTP authentication scheme. The MD5 scheme is similar to CHAP and PAP remote access protocols. Enabling MD5 implements the following security features:

- The Web server requests a user name and a password phrase (distinct from the password). The user name and password phrase are not transmitted over the network, as they are in basic authentication. Instead, a Java login applet combines the user name, password phrase, and a unique session challenge number to calculate an MD5 hash number. Only the hash number is returned to the server to verify that the user has the correct login information; MD5 authentication does not reveal the login information.
- In addition to the login authentication, each form post for configuration or control operations is authenticated with a unique challenge and hash response.
- After the authentication login, subsequent page access is restricted by IP addresses and a hidden session cookie. (You must have cookies enabled in your browser.) Pages are transmitted in their plain-text form, with no encryption.

If you use MD5 authentication, which is available only for the Web interface, disable the less secure interfaces, including Telnet, FTP, and SNMP. For SNMP, you can disable write-only access so that read access and trap facilities are still available. For additional information on MD5 authentication, see RFC document #1321 at the Web site of the Internet Engineering Task Force. For CHAP, see RFC document #1994.

Firewalls

Although MD5 authentication provides a much higher level of security than the plain-text access methods, complete protection from security breaches is almost impossible to achieve. Well-configured firewalls are an essential element in an overall security scheme.

Continued on next page

Security

Authentication *continued*

Summary of access methods

The following table describes interfaces and its access methods.

Interface	Security Access	Notes
Serial Control Console	Access is by user name and password.	Always enabled.
Telnet Control Console	These methods are available: • User name and password • Selectable server port • Server Enable/Disable	The user name and password are transmitted as plain text.
SNMP	These methods are available: • Community Name • NMS IP filters • Agent Enable/Disable • Four access communities with read/write/disable capability	The NMS IP filters allow access from designated IP addresses. • 159.215.12.1 allows only the NMS with that IP address to have access. • 159.215.12.255 allows access for any NMS on the 159.215.12 segment. • 159.215.255.255 allows access for any NMS on the 159.215 segment. • 159.255.255.255 allows access for any NMS on the 159 segment. • 0.0.0.0 or 255.255.255.255 allows access for any NMS.
FTP Server	These methods are available: • User name and password • Selectable server port • Server Enable/Disable	Only the Administrator account has access.
Web Server	These methods are available: • User name and password • Selectable server port • Server Enable/Disable • MD5 Authentication option	In basic HTTP authentication mode, the user name and password are transmitted base-64 encoded (with no encryption). MD5 authentication mode uses a user name and password phrase.

www.apcc.com

APC Worldwide Customer Support

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

- Use an APC web page to find answers to frequently asked questions (FAQs), to access documents in the APC Knowledge Base, and to submit customer support requests.
  - http://www.apcc.com (Corporate Headquarters)
    Connect by links to APC web pages for specific countries and regions, each of which provides customer support information.
  - http://www.apcc.com/support/
    Submit customer support requests.
- Contact local or regional APC Customer Support by telephone or e-mail.
  - For e-mail addresses and local, country-specific, customer support telephone numbers worldwide, go to http://www.apcc.com/support/contact.
  - For e-mail addresses and technical support telephone numbers of major APC regional customer support centers, use the following list:

APC Headquarters (U.S. and Canada)	(1) (800) 800-4272 (toll free)
Latin America	(1) (401) 789-5735 (United States) apctchla@apcc.com
Europe, Middle East, Africa	(353) (91) 702020 (Ireland) apceurtech@apcc.com
Japan	(03) 5434-2021 jsupport@apcc.com

- Contact the APC representative or other distributor from whom you purchased your APC hardware device or APC software application for information on how to obtain local customer support.

990-0815B 01/2001