

Contents

Introduction 1

Product Description	1
Access Procedures	3
How to Recover from a Lost Password	6
Upgrading Firmware	8
Front Panel	9
Rear Panel.	10
Optional Temperature and Humidity Sensors	13
Watchdog Features	14

Hardware Alarms 15

Alarm Messages	15
Clearing the Hardware Alarms	16

Web Interface 17

How to Log On	17
Summary Page.	21
Navigation Menu	24

Control Console 29

How to Log On	29
Main Screen	32
Control Console Menus.	35

Environmental Monitoring Unit Menus 38

Environment Menu.	38
Input Contacts	43
Output Relay	44
Alarm Beacon	45
Custom Events.	46
Device Info	49

Event-Related Menus 53

Introduction 53
Event Log 56
Event Actions (Web Interface Only) 61
Event Recipients 64
E-mail Feature 65
How to Configure Individual Events 70

Data Menu (Web Interface Only) 71

Log Option 71
Configuration Option 72

Network Menu 73

Introduction 73
Option Settings 75

System Menu 100

Introduction 100
Option Settings 102

Boot Mode 112

Introduction 112
DHCP Configuration Settings 115

Security 121

Security Features 121
Encryption 126
Creating and Installing Digital Certificates 130
Firewalls 137

Using the APC Security Wizard 138

Overview 138
Create a Root Certificate & Server Certificates 142

Create a Server Certificate and Signing Request 147
Create an SSH Host Key 151

APC Device IP Configuration Wizard 153

Purpose and Requirements 153
Install the Wizard. 154
Use the Wizard 155

How to Export Configuration Settings 158

Retrieving and Exporting the .ini file 158
The Upload Event and its Error Messages 163
Using the Device IP Configuration Wizard 165

File Transfers 166

Introduction 166
Upgrading Firmware 167
Verifying Upgrades and Updates 176

Product Information 177

Warranty and Service 177
Life-Support Policy 178

Index 179

Introduction

Product Description

Features of the Environmental Monitoring Unit

The APC® Environmental Monitoring Unit is a rack-mountable product that monitors and controls the essential functions needed to ensure the availability of the racks in a room. It provides the following features:

- Network wiring consolidation for all Web-enabled APC products
- Temperature, humidity, Air Removal Unit (ARU), beacon, output relay, and custom event monitoring
- Input contact monitoring for use with dry contact sensors
- Event and data logs accessible by Telnet, FTP, Secure CoPy (SCP), serial connection, or a Web browser
- E-mail notifications and SNMP traps based on the severity level of events.



Note

The Environmental Monitoring Unit does not provide battery backup or surge protection. To ensure that any devices connected to the two outlets on the Environmental Monitoring Unit are protected from power failure or power surges, connect the Environmental Monitoring Unit to an APC UPS.

Initial setup

You must define the following three TCP/IP settings for the Environmental Monitoring Unit before it can operate on the network:

- IP address of the Environmental Monitoring Unit
- Subnet mask
- IP address of the default gateway



See also

To configure the TCP/IP settings, see the Environmental Monitoring Unit *Installation and Quick Start Manual*, provided in printed form, and in PDF form on the APC *Utility CD*.

Access Procedures

Overview

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



For more information about the internal user interfaces, see [Control Console](#) and [Web Interface](#).

The SNMP interface allows you to use an SNMP browser with the PowerNet[®] Management Information Base (MIB) to manage the Environmental Monitoring Unit.



See also

To use the PowerNet MIB with an SNMP browser, see the *PowerNet SNMP Management Information Base (MIB) Reference Guide*, which is provided on the APC *Utility CD* that came with your Environmental Monitoring Unit.

Access priority for logging on

Only one user at a time can log on to the Environmental Monitoring Unit to use its internal user interface features. The priority for access is as follows:

- Local access to the control console from a computer with a direct serial connection to the Environmental Monitoring Unit always has the highest priority.
- Telnet or Secure SHell (SSH) access to the control console from a remote computer has priority over Web access.
- Web access, either directly or through the InfraStruXure Manager, has the lowest priority.

Types of user accounts

The Environmental Monitoring Unit has three levels of access (Administrator, Device Manager, and Read-Only User), all of which are protected by user name and password requirements.

Account Type	Default User Name	Default Password	Access
Administrator	apc	apc	All of the management menus available in the control console and the Web interface.
Device Manager	device	apc	<ul style="list-style-type: none">• The Device Manager menu and its sub-menus in the control console, and all menus in the top section of the navigation panel of the Web interface.• The Log option in the Events menu in the Web interface. A Device Manager can also access the event log in the control console by pressing CTRL-L.• The Data Log option in the Data menu on the Web interface.
Read-Only User	readonly	apc	<ul style="list-style-type: none">• Access through the Web interface only.• Access to the same menus as a Device Manager, but without the capability to change configurations, control devices, delete data, or use FTP-related options. Links to configuration options are visible but disabled, and the event and data logs display no Delete button.



Note

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 [User manager](#).



Note

APC recommends changing the default user name and password for security reasons.

How to Recover from a Lost Password

You can use a local computer that connects to the Environmental Monitoring Unit 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 configuration port at the Environmental Monitoring Unit.



Note

Modbus and the Control Console share a common serial port. You can use either one or the other, one at a time, to access the Environmental Monitoring Unit.

3. Run a terminal program (such as HyperTerminal®) on your computer and configure the selected port as follows:
 - 9600 bps (or 19200 bps, if you are using Modbus configured at that rate)
 - 8 data bits
 - no parity
 - 1 stop bit
 - no flow control



Note

Modbus runs at 9600 or 19200 bps. To use the Control Console when Modbus is enabled, your computer's serial port must communicate at the same serial protocol rate as Modbus.

4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
 - The serial port is not in use by another application.
 - The terminal settings are correct as specified in step 3.
 - The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
6. Press ENTER 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. Press CTRL-C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Upgrading Firmware

Firmware file transfer method

You can use FTP or SCP to upgrade the firmware of one or more Environmental Monitoring Units over the network.

You can use XMODEM to upgrade the firmware for an Environmental Monitoring Unit that is not on the network.

When you use FTP or XMODEM to upgrade the firmware for an Environmental Monitoring Unit, the APC Operating System (AOS) module must be transferred to the Environmental Monitoring Unit before you transfer the application module.

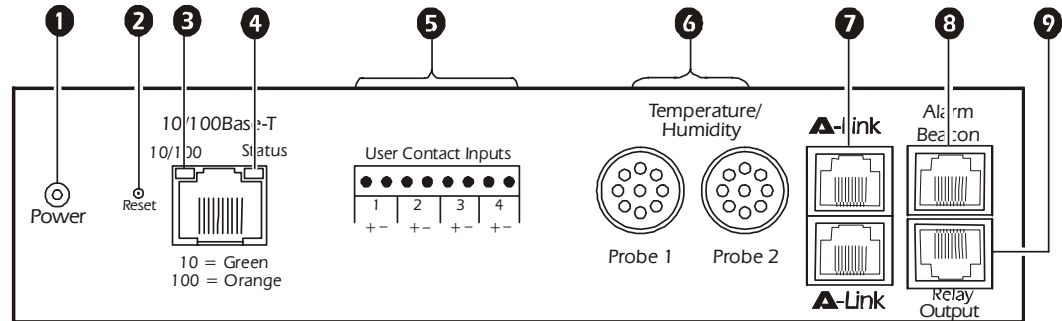


To download a firmware upgrade for your Environmental Monitoring Unit, see [File Transfers](#).

Front Panel

The front panel of the Environmental Monitoring Unit has an RS-232 console port that connects the unit to a local computer, using the configuration cable (APC part number 940-0103). Through the serial connection, you can access all setup, status, maintenance, and diagnostic information for the unit.

Rear Panel



	Item	Description
1	Power LED	Indicates whether the Environmental Monitoring Unit is receiving power (green: receiving power; dark: not receiving power).
2	Reset Button	Resets the Environmental Monitoring Unit. This button will not affect the operation of any connected devices.
3 4	10/100 and Status LEDs	10/100 LEDs: indicate traffic on the network (green: operating at 10 mbps; orange: operating at 100 mbps). Duplex LEDs: indicate how data are being transmitted over the network (off: operating at half duplex; on: operating at full duplex).
5	User Connections	Provides four user input connections for connecting normally open or normally closed input contacts.
6	Local Temperature and Humidity Probe Connections	Connects up to two local temperature/humidity sensors.
7	A-Link Ports	Connects to APC temperature/humidity probes and air distribution products. A-Link is the device communication protocol used by APC.
8	Alarm Beacon Port	Connects to the rack beacon.
9	Relay Output	Connects to other equipment for mapping APC Environmental Monitoring Unit events to outside devices.

Link-RX/TX (10/100) LED

These LEDs indicate the network connection status of products connected through the Ethernet Switch, with one LED for each available connection.

Condition	Description
Off	The device connected to this port is off or not operating correctly.
Flashing Green	The device connected to this port is receiving data packets from the network at 10 Megabits per second (mbps).
Flashing Orange	The device connected to this port is receiving data packets from the network at 100 Megabits per second (mbps).

Duplex LEDs

Condition	Description
Off	The corresponding port is operating at half duplex.
On	The corresponding port is operating at full duplex.

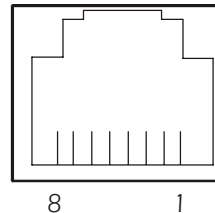
Status LED

This LED indicates the network status of the Environmental Monitoring Unit.

Condition	Description
Off	The Environmental Monitoring Unit has no power.
Solid Green	The Environmental Monitoring Unit has valid TCP/IP settings.
Flashing Green	The Environmental Monitoring Unit does not have valid TCP/IP settings. [†]
Solid Orange	A hardware failure has been detected in the Environmental Monitoring Unit. Contact APC Worldwide Customer Support .
Flashing Orange	The Environmental Monitoring Unit is making BOOTP requests.

[†] If you do not use a BOOTP server, see the Environmental Monitoring Unit *Installation and Quick Start Manual* provided in printed format and in PDF on the APC *Utility* CD that came with your Environmental Monitoring Unit to configure the TCP/IP settings.

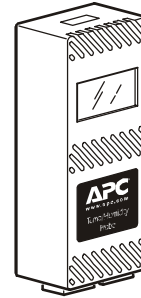
Connector pinout descriptions



Relay output pinouts	
Pinout	Description
2, 3	Relay normally closed
4, 5	Relay common
6, 7	Relay normally open

Optional Temperature and Humidity Sensors

The temperature and relative humidity sensor kit is provided as an option available for purchase with your unit. Additional sensors can be purchased and connected together with A-Link cables.



See also

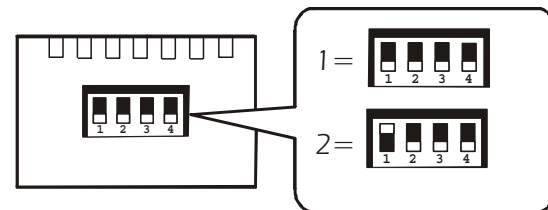
See the Temperature and Humidity Sensor installation sheet, supplied with the kit, for installation instructions.



Note

Use no more than a total of two temperature sensors (APC part number AP9520T) or temperature/humidity sensors (APC part number AP9520TH). Each sensor must have a unique DIP switch address setting to ensure proper operation.

Set the DIP switches on each sensor to a unique A-Link address.



Watchdog Features

Overview

To detect internal problems and recover from abnormal inputs, the Environmental Monitoring Unit uses internal, system-wide watchdog mechanisms. When it reboots itself to recover from an internal problem, a **System: Warmstart** event is recorded in the event log.

Network interface watchdog mechanism

The Environmental Monitoring Unit implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Environmental Monitoring Unit 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 itself.

Resetting the network timer

To ensure that the Environmental Monitoring Unit does not reboot if the network is quiet for 9.5 minutes, the Environmental Monitoring Unit attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the Environmental Monitoring Unit, 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 Environmental Monitoring Unit from restarting.

Hardware Alarms

Alarm Messages

An audible alarm sounds when there is a hardware problem with the Environmental Monitoring Unit. The problem could be caused by either an improper A-Link or sensor connection, or by damaged hardware.

A-Link alarms

The audible alarm is accompanied by the following messages.

A-Link Interface	Message
Control Console or Web (front status display)	ALINK
Event Log	Alink Power Overload
Display Interface	ALINK: Curr Lim Alarm

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

Clearing the Hardware Alarms

To clear an A-Link alarm, disconnect the appropriate connectors to the Environmental Monitoring Unit. This will turn off power to the system.

If the alarm stops, reconnect the devices one at a time to determine what device caused the alarm condition.



See also

For information on A-Link connections, see the Environmental Monitoring Unit *Installation and Quick Start Manual*, provided in printed form, and in PDF on the APC *Utility CD*.

If everything is properly connected and the alarm persists, contact [APC Worldwide Customer Support](#).

If the alarm sounds and nothing is plugged into either the A-Link or sensor ports, turn off the Environmental Monitoring Unit and return the unit to APC.

Web Interface

How to Log On

Overview

You can use the DNS name or System IP address of the Environmental Monitoring Unit for the URL address of the Web interface. Use your case-sensitive **User Name** and **Password** settings to log on. The default user name differs by account type:

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

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



Note

If you are using HTTPS (SSL/TSL) 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, you must use an IP address to log on to the Environmental Monitoring Unit if an IP address was specified as the common name in the certificate, or you must use a DNS name to log on if a DNS name was specified as the common name in the certificate.



For information about the Web page that appears when you log on to the Web interface, see [Summary Page](#).

Supported Web browsers

You can use the Microsoft® Internet Explorer (IE) browser (5.0 and higher) or the Netscape® browser (7.0 and higher) to access the Environmental Monitoring Unit through its Web interface.

Some Web interface features (data verification, data log, and event log) require that you enable the following for your Web browser:

- JavaScript
- Java
- Cookies

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

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

URL address formats

Type the DNS name or IP address of the Environmental Monitoring Unit in the Web browser's URL address field and press ENTER. Except as noted below, `http://` is automatically added by the browser.



Note

If the error "You are not authorized to view this page" occurs (Internet Explorer only), someone is logged onto the Web interface or control console. If the error "No Response" (Netscape) or "This page cannot be displayed" (Internet Explorer) occurs, Web access may be disabled, or the Environmental Monitoring Unit may use a non-default Web-server port that you did not specify correctly in the address. (For Internet Explorer, you must type `http://` or `https://` as part of the address when any port other than 80 is used.)

- For a DNS name of Web1, the entry would be one of the following:
 - `http://Web1` if HTTP is your access mode
 - `https://Web1` if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 198.168.6.133, when the Environmental Monitoring Unit uses the default port (80) at the Web server, the entry would be one of the following:
 - `http://198.168.6.133` if HTTP is your access mode
 - `https://198.168.6.133` if HTTPS (SSL/TLS) is your access mode

- For a System IP address of 198.168.6.133, when the Environmental Monitoring Unit uses a non-default port (5000, in this example) at the Web server, the entry would be one of the following:
 - `http://198.168.6.133:5000` if HTTP is your access mode
 - `https://198.168.6.133:5000` if HTTPS (SSL/TLS) is your access mode

Summary Page

When you log on to the Web interface at the Environmental Monitoring Unit, the status view is displayed at the right side of the screen, the quick status tab is displayed at the upper right, and the navigation menu is displayed at the left.

Status

The **Status** view has these sections:

- **Device Overview** reports any active alarm or warning conditions and displays a status for each device or custom event connected to your Environmental Monitoring Unit.



Note

Device or custom event states displayed in red text indicate an abnormal (fault) condition.

- **Input Contacts** lists the available input contacts and their present state.
- **Output Relay** shows the state of the output relay, which can be connected to outside monitoring devices.
- **Beacon** shows the status of the alarm beacon.
- **Environment –Environmental Probes** shows the status of up to two local temperature/humidity sensors directly connected to the Environmental Monitoring Unit, and up to two remote sensors connected through the A-Link ports.







Note

To change the temperature units on any status page from Fahrenheit (F) to Celsius (C), click the C. To change them from Celsius to Fahrenheit, click the F.

- **Environment – Rack Air Removal Units** displays the status of up to eight Rack Air Removal Units.
- **Status** shows the following:
 - **Name, Contact,** and **Location** information for the Environmental Monitoring Unit.
 - Date and time the screen was last refreshed.
 - Type of user (**Administrator, Device Manager,** or **Read-Only User**).
 - How long (**Up Time**) the Environmental Monitoring Unit has been running since it was last started or reset.

Quick status tab

The quick status tab is displayed in the upper right of every screen in the Web interface. The tab displays a warning of any alarms and provides a link to the online help.

	Access the online help for the displayed page.
	Click the green “device operating normally” icon to return to the status screen where the status for attached devices is displayed.
	Click the “attention required” icon to return to the status screen where active warnings and alarms are displayed.
	Click the “device status requires critical attention” icon to return to the status screen where the active warnings and alarms are displayed.

Navigation Menu

Overview

When you log on to the Web interface, the navigation menu (left frame) includes the following elements:

- IP address of the Environmental Monitoring Unit
- Environmental Monitoring Unit menus to manage the Environmental Monitoring Unit and its components:
 - **Environment**
 - **Input Contacts**
 - **Output Relay**
 - **Beacon**
 - **Custom Events**
 - **Device Info**
- Menus to manage the event log, data log, network connection, and system parameters
 - **Events**
 - **Data**
 - **Network**
 - **System**



Note

When you log on as a Device Manager or Read-Only User, the **Network** and **System** menus do not appear in the navigation menu. Options to make any changes are not available for the Read-Only User.

- **Logout**
- **Help**
- **Links**

Select a menu to perform a task

To do the following, see [Environment Menu](#):

- Configure the local and remote environmental probes.
- Configure Rack Air Removal Units connected to the Environmental Monitoring Unit.

To do the following, see [Input Contacts](#):

- Rename or change the normal state of a contact.
- Change the alarm map for each input contact.

To do the following, see [Output Relay](#):

- Rename or change the normal state of a relay.
- Change the state of each output relay.

To activate the beacon, see [Alarm Beacon](#).

To do the following, see [Custom Events](#):

- Configure signals to be used in custom event configuration.
- Configure custom event settings.

To change the elements shown on the summary page, see [Device Info](#).

To do the following, see [Event-Related Menus](#):

- Access the event log.
- Configure the actions to be taken based on an event's severity level.
- Configure SNMP Trap Receiver settings for sending event-based traps.
- Define who will receive e-mail notifications of events.
- Test e-mail settings.

To do the following, see [Data Menu \(Web Interface Only\)](#):

- View log.
- Configure data logging.

To do the following, see [Network Menu](#):

- Configure new TCP/IP settings for the Environmental Monitoring Unit.
- Identify the Domain Name System (DNS) Server and test the network connection to that server.
- Define settings that affect FTP, Telnet, Secure SHell (SSH), the Web interface, Secure Sockets Layer (SSL), SNMP, and e-mail.

To do the following, see [System Menu](#):

- Control **Administrator**, **Device Manager**, and **Read-Only User** access.
- Define the system **Name**, **Contact**, and **Location** values.
- Set the date and time used by the Environmental Monitoring Unit.
- Restart the Environmental Monitoring Unit interface.
- Reset control console settings to default settings.
- Define the URL addresses of the user links and APC logo links in the Web interface, as described in [Links menu](#).

Help menu

When you click **Help**, the **Contents** for all of the online help is displayed. However, from any Web interface page, you can use the question mark (?) in the quick status bar to link to the section of the online help for that page.

The **Help** menu also has an **About System** option you use to view information about the Environmental Monitoring Unit's **Model Number**, **Serial Number**, **Hardware Revision**, **Manufacture Date**, **MAC Address**, **Application Module** and **APC OS (AOS) Module**, including the date and time each of the two modules were created.



Note

In the control console, the **About System** option, which is a **System** menu option, identifies the **Flash Type** used.

Links menu

Provides three user-definable URL link options. By default, these links access the following APC Web pages:

- **APC's Web Site** accesses the APC home page.
- **Testdrive Demo** accesses a demonstration page where you can use samples of APC web-enabled products.
- **APC Monitoring** accesses the "APC Remote Monitoring Service" page about pay-for-monitoring services available from APC.

To redefine these links so that they point to other URL addresses:

1. Click on **Links** in the **System** menu.
2. Define any new names for **User Links**.
3. Define any new URL addresses that you want **User Links** to access. Only HTTP links may be defined.
4. Click **Apply**.



Note

The link associated with the APC logo is also definable.

Control Console

How to Log On

Overview

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection 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). A Read-Only User has no access to the control console.



If you cannot remember your user name or password, see [How to Recover from a Lost Password](#).

Remote access to the control console

You can access the control console through Telnet or SSH, depending on which is enabled. (An Administrator can enable these access methods through the **Telnet/SSH** option of the **Network** menu.) By default, Telnet is enabled. Enabling SSH automatically disables Telnet.

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 from any computer on the same subnet:

1. At a command prompt, type `telnet` and the System IP address for the Environmental Monitoring Unit (when the Environmental Monitoring Unit uses the default Telnet port of 23), and press ENTER. For example:

```
telnet 198.168.6.133
```



Note

If the Environmental Monitoring Unit uses a non-default port number (between 5000 and 32768), you need to 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 SSH for access to the control console. SSH encrypts user names, passwords, and transmitted data.

The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

Local access to the control console

You can use a local computer that connects to the Environmental Monitoring Unit through the serial port on the front panel of the unit.

1. Select a serial port at the local computer, and disable any service which uses that port.
2. Use the supplied serial cable (APC part number 940-0103) to connect the selected port to the serial port on the front panel of the Environmental Monitoring Unit.



Note

Modbus and the control console share a common serial port. You can use either one or the other, one at a time, to access the Environmental Monitoring Unit.

3. Run a terminal program (such as HyperTerminal) and configure the selected port for 9600 bps (or 19200 bps, if you use Modbus configured at that rate), 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.



Note

Modbus runs at 9600 or 19200 bps. To use the control console when Modbus is enabled, your computer's serial port must communicate at the same serial protocol rate as Modbus.

4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.
5. Enter your user name and password.

Main Screen

Example main screen

The following is an example of the screen that appears when you log on to the control console at an Environmental Monitoring Unit.

```
American Power Conversion          Network Management Card AOS v2.6.4
(c) Copyright 2005 All Rights Reserved EMS & EMU2 APP                v2.6.6
-----
Name      : Env Monitor                      Date : 01/09/2005
Contact   : Eileen Jenson                    Time : 12:43:17
Location  : Testing lab 1                    User : Administrator
Up Time   : 0 Days 23 Hours 06 Minutes       Stat : P+ N+ A+
```

Environmental Monitoring Unit

```
-----
Env Probes : Fault                          ARUs      : No ARUs found
Contacts   : OK                             Relays    : Fault
Beacon     : Off                            Custom Events : Inactive
```

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

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

<ESC>- Main Menu, <ENTER>- Refresh, <CTRL-L>- Event Log

Information and status fields

Main screen information fields.

- Two fields identify the APC operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the type of device that connects to the network. On the [Example main screen](#), the application firmware for the Environmental Monitoring Unit is displayed.

```
Network Management Card AOS          v2.6.4
```

```
EMS & EMU2 APP                      v2.6.6
```

- Three fields identify the system **Name**, **Contact**, and **Location** values.

```
Name       : Env Monitor  
Contact    : Eileen Jenson  
Location   : Testing lab 1
```



To set the **Name**, **Contact**, and **Location** values, see [System Menu](#).

- An **Up Time** field reports how long the Environmental Monitoring Unit has been running since it was last reset or since power was applied.

```
Up Time    : 0 Days 23 Hours 06 Minutes
```

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

```
Date : 01/09/2005  
Time : 12:43:17
```

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

```
User : Administrator
```

Main screen status fields.

- A **Stat** field reports the Environmental Monitoring Unit status.

Stat : P+ N+ A+

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



Note

If the AOS status is not P+, contact [APC Worldwide Customer Support](#), even if you can still access the Environmental Monitoring Unit.

Environmental Monitoring Unit status fields.

The status fields display the status of each of the devices that the Environmental Monitoring Unit can control or monitor. **OK**, **Fault Present**, or **No Device Found** is displayed.

Control Console Menus

Menu structure

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.

For menus that allow you to change a setting you must use the **Accept Changes** option to save the changes you made.

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

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



For information about the event log, see [Event-Related Menus](#).

Main menu

The main control console menu has options that provide access to the management features of the control console:

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



Note

When you log on as Device Manager, you do not have access to the **System** or **Network** menus.

Device Manager option

This option accesses the **Device Manager** menu. Select the components you want to manage. For example:

- 1- Environment
- 2- Input Contacts
- 3- Output Relay
- 4- Beacon
- 5- Device Info
- 6- Modbus

Network option

To do any of the following tasks, see [Network Menu](#):

- Configure the TCP/IP settings for the Environmental Monitoring Unit.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet, SSH, Web interface, SSL, TLS, SNMP, e-mail, Syslog, and DNS features of the Environmental Monitoring Unit.

System option

To do any of the following tasks, see [System Menu](#):

- Control **Administrator** and **Device Manager** access. (You can control **Read-Only User** access by using the Web interface only.)
- Define the system **Name**, **Contact**, and **Location** values.
- Set the **Date** and **Time** used by the Environmental Monitoring Unit.
- Through the **Tools** menu:
 - Restart the Environmental Monitoring Unit interface.
 - Reset parameters to their default values.
 - Delete SSH host keys and SSL certificates.
 - Upload an initialization file.
 - Perform a file transfer through a serial connection.
- 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 Environmental Monitoring Unit.

Environmental Monitoring Unit Menus

Environment Menu

Environmental sensors

Web interface. To set the sensor's name and its temperature and humidity thresholds, select **Env Probes** from the **Environment** menu, and then select the sensor you want to modify. Click **Configure** to change the sensor name, environmental thresholds, and rate of change, and click **Apply** below the list.

On the same screen, set the alarm map for each threshold. Under the **Environmental Probe Alarm Map Configuration** heading, select the check boxes for the alarm behaviors next to each threshold. Click **Apply** below the list.

Control console. Select **Environment** from the **Device Manager** menu, and select the **Temp/Humidity** option to display a list of sensors and their settings. Choose either **Local Env Probes** or **Remote Env Probes** and select an individual sensor to modify. After you make changes, select **Accept Changes** to confirm them.

Setting	Description
Probe Name	Set the name for each environmental sensor.
Maximum Temperature Threshold	Set the maximum high temperature threshold for this sensor. If the temperature rises above this threshold, an alarm occurs. This threshold must be greater than High Temperature Threshold .

Setting	Description
High Temperature Threshold	Set the high temperature threshold for this sensor. If the temperature rises above this threshold, an alarm occurs. This temperature must be greater than the sum of Low Temperature Threshold and Temperature Threshold Delta .
Low Temperature Threshold	Set the low temperature threshold for this sensor. If the temperature drops below this threshold, an alarm occurs. This threshold must be greater than Minimum Temperature Threshold .
Minimum Temperature Threshold	Set the minimum low temperature threshold for this sensor. If the temperature rises below this threshold, an alarm occurs.
Temperature Threshold Delta	This difference between the temperature threshold violation and the clearing point.
Short-term Increasing Temperature Rate of Change	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.
Short-term Decreasing Temperature Rate of Change	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.
Long-term Increasing Temperature Rate of Change	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.
Long-term Decreasing Temperature Rate of Change	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.

Setting	Description
Maximum Humidity Threshold	Set the maximum humidity threshold for this sensor. If the humidity rises above this threshold, an alarm occurs. This threshold must be greater than High Humidity Threshold .
High Humidity Threshold	Set the high humidity threshold for this sensor. If the humidity rises above this threshold, an alarm occurs. This temperature must be greater than the sum of Low Humidity Threshold and Humidity Threshold Delta .
Low Humidity Threshold	Set the low humidity threshold for this sensor. If the humidity drops below this threshold, an alarm occurs. This threshold must be greater than Minimum Humidity Threshold .
Minimum Humidity Threshold	Set the minimum humidity threshold for this sensor. If the humidity rises above below threshold, an alarm occurs.
Humidity Threshold Delta	This difference between the humidity threshold violation and the clearing point.
Maximum Temperature Alarm map	Map the maximum temperature alarm threshold to a beacon or relay.
High Temperature Alarm Map	Map the high temperature alarm threshold to a beacon or relay.
Low Temperature Alarm Map	Map the low temperature alarm threshold to a beacon or relay.
Minimum Temperature Alarm Map	Map the minimum temperature alarm threshold to a beacon or relay.
Short-term Increasing Temperature Rate of Change Alarm Map	Map the short-term increasing rate of change to a beacon or relay.
Short-term Decreasing Temperature Rate of Change Alarm Map	Map the short-term decreasing rate of change to a beacon or relay.

Setting	Description
Long-term Increasing Temperature Rate of Change Alarm Map	Map the long-term decreasing rate of change to a beacon or relay.
Long-term Decreasing Temperature Rate of Change Alarm Map	Map the long-term decreasing rate of change to a beacon or relay.
Maximum Humidity Alarm Map	Map the maximum humidity alarm threshold to a beacon or relay.
High Humidity Alarm Map	Map the high humidity alarm threshold to a beacon or relay.
Low Humidity Alarm Map	Map the low humidity alarm threshold to a beacon or relay.
Minimum Humidity Alarm Map	Map the minimum humidity alarm threshold to a beacon or relay.

Alarm map types

Events can be mapped to a behavior. When the event occurs, the Environmental Monitoring Unit can take one or more of these actions:

Alarm Map	Description
Beacon	Activate the alarm beacon.
Relay 1	Change the state of Relay 1 to its fault state.

Rack Air Removal Units (Rack ARUs)

Web interface. Select **Environment** and then **Air Removal** from the navigation menu. The Rack Air Removal Unit Status and Rack Air Removal Unit Alarms are displayed. To configure one of the ARUs, select its name to display the **Rack Air Removal Unit Configuration** and **Rack Air Removal Unit Alarm Map Configuration** screen. Make changes to the temperature setpoints and the alarm map settings from this screen. Click the **Apply** button for each section to confirm your changes.

Control console. On the **Device Manager** menu select **Environment**, and then **Rack ARUs**. Configure any of the displayed ARUs or select **Alarm Details** for a list of the firmware revisions and active alarms for each ARU.

Setting	Description
ARU Name	Set a name for this Rack ARU.
Setpoint	Set the temperature remote setpoint for this Rack ARU. The setpoint can be set to the heat load in the rack (kW) or the exhaust temperature of the air leaving equipment in the rack. When the ARU is in remote mode, it uses the remote setpoint.
Temperature Override	Enable or disable the temperature override. If the setpoint for the ARU is in kW mode (and the override is enabled), the fan speed will increase in response to a rise in temperature.
Override Setpoint	When the setpoint dial for the ARU is in kW mode, the fans will increase speed when the air in the rack reaches this temperature.
Alarm Map	Map the change of state for this Rack ARU to an alarm type, relay, or outlet. See Alarm map types for the specific behaviors to which events can be mapped.

Input Contacts

Web interface

To view the status of the input contacts, select **Input Contacts** from the navigation menu. Click **Configure** to change input contact settings.

Control console

To change the input contact settings, select **Input Contacts** from the **Device Manager** menu and select a contact to modify.

Setting	Descriptions
Name	Set the name for this input contact.
Normal State	Set this contact to either normally open or normally closed.
Alarm Map	Map the change of state for this contact to an alarm type, relay, or outlet. See Alarm map types for the specific behaviors to which events can be mapped.

Output Relay

Control relay

Web interface. To control the output relay, select **Output Relays** from the navigation menu. Click **Control/Configure** to change the output relay settings. To change the state of a relay manually, choose an action from the **Action** drop-down list and click **Apply**.

Control console. To control the output relay from the control console, select **Output Relays** from the **Device Manager** menu and then select **Control Relay 1**.

Setting	Description
Action (Web) Immediate Open or Immediate Close (Control Console)	Manually open or close this relay.

Configure relay

Web interface. To configure the output relay, select **Output Relays** from the navigation menu, and then click **Control/Configure**. Under **Output Relay Configuration**, change the **Name** and **Normal State** for this output relay.

Control console. To configure the output relay from the control console, select **Output Relays** from the **Device Manager** menu and select **Configure Relay 1** from the **Output Relays** menu.

Setting	Description
Name	Set the name for this output relay.
Normal State	Set this relay to either normally open or normally closed.

Alarm Beacon

Control the alarm beacon

Web interface. To start or stop the beacon, select **Beacon** from the navigation menu and then click **Control**. Choose an action from the **Action** drop-down list and click **Apply**.

Control console. To control the beacon from the control console, select **Beacon** from the **Device Manager** menu. Select **Immediate On** or **Immediate Off** from the **Beacon** menu.

Custom Events



Note

Custom events can be defined only from the Web interface.

Custom Events allows you to create events that are not already monitored by the Environmental Monitoring Unit. First, define signals for the Environmental Monitoring Unit to monitor, then configure events based on combinations of your signals. If an alarm state occurs, you will receive notification based on the alarm map settings you chose.

Signal Config

Web interface only. It is possible to configure up to ten signals by specifying data for the Environmental Monitoring Unit to monitor. To configure custom event signals, select **Custom Events** from the navigation menu; the Signal Configuration List is displayed. Select the number of the signal you wish to configure. Select the parameters of the signal from the drop-down lists that are activated by the input category you select. Define time requirements, and click **Apply**.

Event Config

Web interface only. It is possible to create five custom events. Each event can monitor up to three configured signals. Select **Event Config** from the **Custom Events** menu, then select the event that you want to configure. Edit the event definition and click **Apply**.

On the same screen, set the alarm map for each event. Check the box of the desired alarm type and click **Apply** below the list.

Setting	Description
Event	Enable or disable the event.
State	Status of the event, active or inactive.
Event Active Text	Text to be displayed if the event becomes active.
Event Inactive Text	Text to be displayed if the event become inactive.
Configured Signal Reference List	Displays the list of signals you have configured.
Event Definition	Define the parameters of the event by selecting the number of signals that will be used, the names of the signals to be monitored, and the frequency of event evaluation.
Alarm Map	Select the alarm types that will be activated when the event occurs.

Administrators only. Select **Configure 'Active' Notification** or **Configure 'Inactive' Notification** to configure the event severity and actions. Select the severity of the warning from the **Event Security** drop-down menu. To designate an item as a recipient of an alert, select the check-box next to the item. The events can also be reset to **Default**.

Setting	Description
Event Severity	Define the severity of the event. <ul style="list-style-type: none"> • None—The severity of this event is intentionally undefined. • Informational—The event requires no action. • Warning—The event requires your action, but not immediately. • Severe—The event requires your immediate action.
Actions	Perform one or several actions when a custom event activates. Record it in the event log and as a Syslog event, and send it to SNMP trap receivers and e-mail recipients. Specify which events will take place by checking the box next to the desired option.

Device Info

Detailed status (control console only)

Control console. The **Detailed Status** screen displays the status of the following:

- Contacts
- Relay
- Beacon
- Local Environmental Probes
- Remote Environmental Probes
- Rack Air Removal Units
- Custom Events Status

Select **Device Info** from the **Device Manager** menu and then select **Detailed Status**.



For similar information on the Web interface, see [Summary Page](#).

Device parameter configuration

Web interface. To configure device parameters, select **Device Info** from the navigation menu, and click **Configure** in the **Parameters** field.

Control console. To configure the Environmental Monitoring Unit, select **Device Info** from the **Device Manager** menu, then select **Device Configuration**.

Setting	Description
Device Name	Set the name for the Environmental Monitoring Unit.
Clear Alarms	Clear active alarms and reestablish based on the current state of the devices. This setting is useful for clearing Lost Communications alarms when reconfiguring the device.
Status Display Presentation (Web only)	<p>Shows any active alarms and the status of each category of monitored devices connected to the Environmental Monitoring Unit. Set the fields to be displayed only on the main Status page of the Web interface, or on all Status pages.</p> <p>If the monitored devices of a category are not installed, that category will not appear on the status page.</p> <p>Display options include the current status of inputs, relays, probes, and Air Removal Units. Select the check-box next to each option you wish to display, then select Apply to confirm the changes.</p>

Alarm Maps

Alarm Maps, in the **Device Info** field, allows you to view all possible alarm maps, and displays the status of alarms for Environmental Probes, Input Contact Status, Air Removal Units, and Custom Events. Click **Control/Configure** to modify alarm maps for Input Contacts. The alarm maps for all other items can be configured by clicking on the name of the item you wish to configure, then navigating to its configuration page.

Modbus

Modbus lets you view the Environmental Monitoring Unit through your building management services interface. It is read-only.



Note

Modbus and the control console share a common serial port. You can use either one or the other, one at a time, to access the Environmental Monitoring Unit.

The Modbus interface supports 2-wire RS-485 using a RS-485 to RS-232 converter with its own power source. This converter is not included. The RS-232 port on the Environmental Monitoring Unit has the following pin-out:

- Pin 2: RX
- Pin 3: TX
- Pin 5: GND



Note

Modbus runs at 9600 or 19200 bps. To use the control console when Modbus is enabled, the console serial port must communicate at the same serial protocol rate settings as Modbus.

To configure Modbus using the Web interface, do the following:

- Select **Modbus** from the **Device Info** menu.
- Select **Configure**, then enter your settings.

To configure Modbus using the control console, do the following:

- Select **Device Manager**.
- Select **Modbus**.
- Enter settings by selecting **Access**, **Unique Target ID**, or **Baud Rate** from the menu list.
- Apply changes by selecting **Accept changes**.



See also

The Modbus register map for the Environmental Monitoring Unit, a spreadsheet (`.\doclen\AP9320MBRegMapxxx.xls`) provided on the Environmental Monitoring Unit *Utility* CD, defines the data (type, location, and valid responses) available through Modbus. To see if an update to this register map is available, go to the Web page www.apc.com/search/index.cfm, search the APC Web site for the part number **AP9319**, click on the link to the register map in the list of documentation, and check the publication date at the start of the file.

Event-Related Menus

Introduction

Overview

The **Events** menu provides access to the options that you use to do the following tasks:

- Access the event log.
- Define the actions to be taken when an event occurs, based on the severity level of that event.
 - Event logging
 - Syslog message notification
 - SNMP trap notification
- E-mail notification



Note

You can only use the Web interface to define which events will use which actions, as described in [Event Log](#) and [How to Configure Individual Events](#).

- Define up to four Network Management Stations (NMSs) as trap receivers by their IP addresses or domain names.
- Define up to four recipients for event notifications by e-mail.

Menu options

In the Web interface, all of the events options are accessed through the **Events** menu.

In the control console, access the available events-related options as follows:

- Use the **Email** option in the **Network** menu to define the SMTP server and e-mail recipients.
- Use the **SNMP** option in the **Network** menu to define the SNMP trap receivers.
- Use CTRL-L to access the event log from any menu.

For information on the following topics, use these links:

- [Event Log](#)
- [Event Actions \(Web Interface Only\)](#)
- [Event Recipients](#)
- [E-mail Feature](#)
- [How to Configure Individual Events](#)

Event Log

Overview

The Environmental Monitoring Unit supports event-logging for all embedded management card application firmware modules. To view embedded management card and Environmental Monitoring Unit (Device) events, use any of the following to access the event log:

- Web interface
- Control console
- FTP
- SCP

Logged events

By default, abnormal internal system events and any event which causes an SNMP trap will be logged, except for SNMP authentication failures. However, you can use the **Actions** option in the Web interface's **Events** menu to disable the logging of events based on their assigned severity level, as described in [Event Actions \(Web Interface Only\)](#).



Some System (embedded management card) events do not have a severity level. Even if you disable the event log for all severity levels, events with no severity level will still be logged.



To access a list of the System (embedded management card) and Environmental Monitoring Unit (Device) events, see [Event list page](#).

Web interface

The **Log** option in the **Events** menu accesses the event log. This log displays all of the events, in reverse chronological order, that have been recorded since the log was last deleted. The **Delete Log** button clears all events from the log.

Control console

Press CTRL-L to display all the events that have been recorded since the log was last deleted, in reverse chronological order. Use the SPACE BAR to scroll through the recorded events. While viewing the log, type d and press ENTER to clear all events from the log.



Note

After events are deleted, they cannot be retrieved.

How to use FTP or SCP to retrieve log files

You can use FTP or SCP to retrieve a tab-delimited event log (*event.txt*) or data log (*data.txt*) that you can import into a spreadsheet application, or a configuration file (*config.ini*) that you can export to another Environmental Monitoring Unit or to multiple Environmental Monitoring Units.



For more information about user configuration files, see [Retrieving and Exporting the .ini file](#).



For more information about the data log, see [Data Menu \(Web Interface Only\)](#).

- The file reports all of the events (*event.txt*) or data (*data.txt*) recorded since the log was last deleted.
- The file includes information that the event 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 the IP address of the Environmental Monitoring Unit
 - In the *event.txt* file, the unique event code for each recorded event

If you are using the encryption-based security protocols for your system, use SCP to retrieve the log file. (You should have FTP disabled.)

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



See [Security](#) for information on the available protocols and methods for setting up the type of security appropriate for your needs.



Note

The Environmental Monitoring Unit 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.

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 *event.txt* or *data.txt* file:

1. At a command prompt, type `ftp` and the IP address of the Environmental Monitoring Unit, and press ENTER. If the **Port** setting for **FTP Server** in the **Network** menu has been changed from its default value (21), you must use the non-default value in the FTP command. For some FTP clients, you must use a colon to add the port number to the end of the IP address. For Windows FTP clients, use the following command (including spaces):

```
ftp>open ip_address port_number
```

2. Use your case-sensitive user name and password to log on as either an Administrator or a Device Manager user.
 - For Administrator, **apc** is the default user name and password.
 - For Device Manager, **device** is the default user name, and **apc** is the default password.
3. Use the **get** command to transmit the text version of the event 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 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.

Event Actions (Web Interface Only)

Overview

The **Actions** option, available only on the Web interface's **Events** menu, allows you to select which actions will occur for events that have a specified severity level:

- **Event Log** selects which severity levels cause an event to be recorded in the event log.



See [Event log action](#).

- **SNMP Traps** selects which severity levels cause SNMP traps to be generated.



See [SNMP traps action](#).

- **Email** selects which severity levels cause e-mail notifications to be sent.



See [Email action](#).

Click **Details** to access a complete list of the System (embedded management card) and Environmental Monitoring Unit (Device) events that can occur, and then edit the actions that will occur for an individual event, as described in [How to Configure Individual Events](#). Click **Hide Details** to return to the **Actions** option.



Note

Modifying events on the **Configure Event Action by Severity Level** page will override any changes you have made to individual events on the **Details** page.

Severity levels

Except for some System (embedded management card) events that do not have a severity level, events are assigned a default severity level based on their seriousness:

- **Informational:** Indicates an event that requires no action, such as a notification of a return from an abnormal condition.
- **Warning:** Indicates an event that may need to be addressed if the condition continues, but does not require immediate attention.
- **Severe:** Indicates an event that requires immediate attention. Unless resolved, severe Device and System events can cause incorrect operation of the Environmental Monitoring Unit or its embedded management card.

Event log action

You can disable the recording of events in the event log. By default, all events are recorded, even events that have no severity level assigned.



Note

Even if you disable the event log action for all severity levels, System (embedded management card) events that have no severity level assigned will still be logged.



For more information about this log, see [Event Log](#).

SNMP traps action

By default, the **SNMP Traps** action is enabled for all events that have a severity level. However, before you can use SNMP traps for event notification, you must identify the NMSs (by their IP addresses or domain names) that will receive the traps.



To define up to four NMSs as trap receivers, see [Event Recipients](#).

Email action

By default, the **Email** action is enabled for all events that have a severity level assigned. However, before you can use e-mail for event notifications, you must define the e-mail recipients.



See [E-mail Feature](#).

Event Recipients

Overview

The Web interface and control console both have options that allow you to define up to four trap receivers and up to four e-mail addresses to be used when an event occurs that has the SNMP traps or e-mail enabled.



See [Event Actions \(Web Interface Only\)](#)

Trap receiver settings

To define the **Trap Receiver** settings that determine which NMSs receive traps:

- In the Web interface, use the **Recipients** option in the **Events** menu.
- In the control console, use the **SNMP** option in the **Network** menu.

Item	Definition
Community Name	The password (maximum of 15 characters) used when traps are sent to the NMS identified by the Receiver NMS IP/Domain Name setting.
Receiver NMS IP/ Domain Name	The IP address or domain name of the NMS that will receive traps. 0.0.0.0 (the default value) causes traps not to be sent to any NMS.
Generation (Web interface) Trap Generation (control console)	Enables (by default) or disables the sending of any traps to the NMS identified by the Receiver NMS IP/Domain Name setting.
Authentication Traps	Enables or disables the sending of authentication traps to the NMS identified by the Receiver NMS IP/Domain Name setting.

E-mail Feature

Overview

You can 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 Domain Name System (DNS) server. (Optionally, you can also define a secondary DNS server.)



See [DNS servers](#).

- The DNS name of the SMTP server and the **From Address** setting for SMTP.



See [SMTP settings](#).

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



See [Email recipients](#).

DNS servers

The Environmental Monitoring Unit cannot send any e-mail messages unless the IP address of the primary DNS server is defined.

The Environmental Monitoring Unit will wait a maximum of 15 seconds for a response from the primary or (if specified) the secondary DNS server. If the Environmental Monitoring Unit does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers that are on the same segment as the Environmental Monitoring Unit or on a nearby segment (but not across a WAN).

Once you define the IP addresses of the DNS servers, verify that DNS is working correctly. Enter the DNS name of a computer on your network to test whether you can look up the IP address for that DNS name.

SMTP settings

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

Setting	Description
SMTP Server	Defines the SMTP server by its DNS name. NOTE: This definition is required only when the SMTP Server option (see Email recipients) is set to Local .
From Address	Defines the contents of the From field in the e-mail messages sent by the Environmental Monitoring Unit. NOTE: The 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.

Email recipients

In the Web interface, use the **Recipients** option in the **Events** menu or the **Configure the Email recipients** link in the “Email Configuration” page to identify up to four e-mail recipients. Use the **Email Test** option to send a test message to a configured recipient.

In the control console, use the **Email** option in the **Network** menu to access the e-mail recipient settings.

Setting	Description
To Address	<p>Defines the user and domain names of the recipient.</p> <ul style="list-style-type: none">• To bypass the DNS lookup of the mail server’s IP address, use the IP address in brackets instead of the e-mail domain name. For example, use <code>jsmith@[xxx.xxx.xxx.xxx]</code> instead of <code>jsmith@company.com</code>. This is useful when DNS lookups are not working correctly.• To use e-mail for paging, use the e-mail address for that recipient’s pager gateway account (for example, <code>myacct100@skytel.com</code>). The pager gateway pages the recipient. The recipient’s pager must be able to use text-based messaging.

Setting	Description
SMTP Server	<p>Selects one of the following methods for routing e-mail.</p> <ul style="list-style-type: none"> • Through the SMTP server provided with the Environmental Monitoring Unit (the recommended option, Local). This option ensures that the e-mail is sent before the 20-second time-out for the Environmental Monitoring Unit, and, if necessary, is retried several times. Also do one of the following: <ul style="list-style-type: none"> • Enable forwarding at the SMTP server provided with the Environmental Monitoring Unit 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 its configuration to allow forwarding. • Set up a special e-mail account for the Environmental Monitoring Unit to forward e-mail to an external mail account. • Directly to the recipient's SMTP server (the Recipient's option). On a busy remote SMTP server, the time-out may prevent some e-mail from being sent, and with this option the Environmental Monitoring Unit tries to send the e-mail only once. <p>When the recipient uses the SMTP server provided with the Environmental Monitoring Unit, the Recipient's setting has no effect.</p>
Generation	Enables (by default) or disables sending e-mail to the recipient.

Setting	Description
Format	<p>Selects the format used for e-mail messages:</p> <p>Short: Identifies only the event that occurred. For example: Environmental Monitoring Unit: Output Relay abnormal condition</p> <p>Long: Includes information about the Environmental Monitoring Unit and the event. For example:</p> <p>Name: TestLab Location: Building 3 Contact: DonAdams http://139.225.6.133 Environmental Monitoring Unit Ser #: WS0131005294 Date: 01/03/2005 Time: 16:09:48 Code: 0x1015</p> <p>Warning - Environmental Monitoring Unit: Output Relay abnormal condition</p>

How to Configure Individual Events

Event list page

The **Actions** option in the **Events** menu opens the Event Action Configuration page on the Web interface. Use the **Details** button in this page to access a complete list of the events that can be reported by your Environmental Monitoring Unit.



Note

Modifying events on the **Configure Event Action by Severity Level** page will override any changes you have made to individual events on the **Details** page.

Each event is identified by its unique code, its description, and its assigned severity level. For example:

Code	Description	Severity
0x0002	System: Warmstart	Severe
0x0F15	Environmental Monitoring Unit: Output Relay abnormal condition	Warning



For information about severity levels and how they define the actions associated with events, see [Event Actions \(Web Interface Only\)](#).

Detailed Event Action Configuration page

The event codes provide a link to a page that allows you to do the following:

- Change the selected event's severity level
- Enable or disable whether the event uses the event log, Syslog messages, SNMP traps, or e-mail notifications

Data Menu (Web Interface Only)

Log Option

Use this option to access a log that stores readings taken by the temperature and humidity probes at regular intervals.

The information in the data log is sampled and stored based on the log interval defined by the **Data** menu's **Configuration** option. Each entry is listed by the date and time the data was recorded, and provides the data in a column format.



See [Configuration Option](#).



For information about how you can retrieve the Data Log as a text file, see [How to use FTP or SCP to retrieve log files](#).



See also

For descriptions of the recorded data specific to your Environmental Monitoring Unit, see the online help in your Environmental Monitoring Unit's Web interface.

Configuration Option

Use this option to access the **Data Log Configuration** page. This page reports how much data can be stored in the data log based on the **Log Interval** setting, which defines how often data will be sampled and recorded in the data log. If you change the **Log Interval**, the report updates to reflect the effect of the new setting.



Note

The minimum interval is one minute; the maximum interval is 18 hours, 12 minutes, and 15 seconds.

Network Menu

Introduction

Overview

Use the **Network** menu to do the following tasks:

- Define TCP/IP settings, including BOOTP server settings, when a BOOTP server is used to provide the needed TCP/IP values.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet, SSH, Web interface, SSL, SNMP, E-mail, DNS, and Syslog features of the Environmental Monitoring Unit.



Note

Only an Administrator has access to the **Network** menu.

Menu options

Unless noted, the following menu options are available in the control console and Web interface:

- TCP/IP
- DNS
- Ping utility (control console)
- FTP server
- Telnet/SSH
- SNMP
- Email
- Syslog
- Web/SSL

Option Settings

TCP/IP

This option accesses the following settings:

- A Boot mode setting selects the method used to define the three TCP/IP values that an Environmental Monitoring Unit needs to operate on the network:
 - **System IP**: The IP address of the Environmental Monitoring Unit
 - **Subnet Mask**: The subnet mask value
 - **Default Gateway**: The IP address of the default gateway



For information about the watchdog role the default gateway plays, see [Resetting the network timer](#).



See also

For information about how to configure the initial TCP/IP settings when you install the Environmental Monitoring Unit, see the Environmental Monitoring Unit *Installation and Quick Start Manual* (`.\doc\en\insguide.pdf`), provided on the *Utility CD* that came with your Environmental Monitoring Unit and in printed form.

- Advanced settings define the Environmental Monitoring Unit's host and domain names, as well as TCP/IP port, BOOTP, and DHCP settings used by the Environmental Monitoring Unit.

Current TCP/IP settings fields. The current **System IP**, **Subnet Mask**, and **Default Gateway** values, along with the Environmental Monitoring Unit's **MAC Address**, **Host Name**, **Domain Name**, and **Ethernet Port Speed** values are displayed above the TCP/IP settings in the control console and the Web interface.

Boot mode setting. This setting selects which method will be used to define the Environmental Monitoring Unit's TCP/IP settings whenever the Environmental Monitoring Unit starts, resets, or reboots:

- **Manual:** Three settings (**System IP**, **Subnet Mask**, and **Default Gateway**) that are only available when **Manual** is used to define the needed TCP/IP settings.
- **BOOTP only:** A BOOTP server provides the TCP/IP settings.
- **DHCP only:** A DHCP server provides the TCP/IP settings.
- **DHCP & BOOTP:** The Environmental Monitoring Unit will attempt to get its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server.



Note

An **After IP Assignment** setting will, by default, switch **Boot mode** from its default **DHCP & BOOTP** setting to **BOOTP only** or **DHCP only**, depending on the type of server that supplied the TCP/IP settings to the Environmental Monitoring Unit. For information about the **After IP Assignment** setting, and other settings that affect how the Environmental Monitoring Unit uses BOOTP and DHCP, see [Advanced settings](#); For more information about how to use DHCP, see [Boot Mode](#).

Advanced settings. The **Boot mode** affects which settings are available:

- Two settings are available for all **Boot mode** selections to define the Environmental Monitoring Unit's **Host Name** and **Domain Name** values.
 - **Host Name:** When an Administrator configures a host name here and a domain name in the **Domain Name** field, users can then enter a host name in any field in the Environmental Monitoring Unit interface (except e-mail addresses) that accepts a domain name as input.
 - **Domain Name:** An Administrator needs to configures the domain name here only. In all other fields in the Environmental Monitoring Unit interface (except e-mail addresses) that accept domain names, the Environmental Monitoring Unit will add this domain name when only a host name is entered.



Note

- To override the expansion of a specified host name by the addition of the domain name, do one of the following:
- To override the behavior in all instances, set the domain name field in **Configure General Settings** to its default `somedomain.com` or to `0.0.0.0`.
 - To override the behavior for a particular host name entry — for example when defining a trap receiver — include a trailing period. The Environmental Monitoring Unit recognizes a host name with a trailing period (such as *mySnmpServer.*) as if it were a fully qualified domain name and therefore does not append the domain name.
- A **Port Speed** setting is available for all **Boot mode** selections to define the TCP/IP port's communication speed (**Auto-negotiate**, by default).

- Three settings are available for all **Boot mode** selections, except **Manual**, to identify the Environmental Monitoring Unit in BOOTP or DHCP communication:
 - **Vendor Class**: Uses **APC**, by default.
 - **Client ID**: Uses the Environmental Monitoring Unit's MAC address, by default.



If the **Client ID** is changed from the Environmental Monitoring Unit's MAC address, the new value must be unique on the LAN. Otherwise, the DHCP or BOOTP server may act incorrectly.

- **User Class**: Uses the Environmental Monitoring Unit's application module type, by default. For example, the Environmental Monitoring Unit module sets the **User Class** to **EMU**.
- Two settings are available when **BOOTP only** is the Boot mode selection:
 - **Retry Then Fail**: Defines how many times the Environmental Monitoring Unit will attempt to discover a BOOTP server before it stops (**4**, by default).
 - **On Retry Failure**: Defines what TCP/IP settings will be used by the Environmental Monitoring Unit when it fails to discover a BOOTP server (**Use Prior Settings**, by default).



For information about the **Advanced** settings (**DHCP Cookie Is** and **Retry Then Stop**) that directly affect how DHCP is used, see [Boot Mode](#)

DNS

Configure Domain Name Service Settings fields. Use these fields to define the IP addresses of the primary and secondary Domain Name System (DNS) Servers used by the Environmental Monitoring Unit e-mail feature.



See [E-mail Feature](#) and [DNS servers](#).

Send DNS query (Web interface). Use this option, available only through the **DNS** menu in the Web interface, to send a DNS query that tests the setup of your DNS servers.

Use the settings listed below to define the parameters for the test DNS request. View the result of the test DNS request in the **Last Query Response** field (which displays **No last query** or text describing the query result of the last test).

- Use the **Query Type** setting to select the method to use for the DNS query:
 - The URL name of the server (**Host**)
 - The IP address of the server (**IP**)
 - The fully qualified domain name (**FQDN**)
 - The Mail Exchange used by the server (**MX**)
- Use the **Query Question** text field to identify the value to be used for the selected **Query Type**:
 - For **Host**, identify the URL
 - For **IP**, identify the IP address
 - For **FQDN**, identify the fully qualified domain name, formatted as `myserver.mydomain.com`
 - For **MX**, identify the Mail Exchange address

- Enable or disable **Reverse DNS Lookup**, which is disabled by default. Enable this feature unless you do not have a DNS server configured or have poor network performance because of heavy network traffic. With **Reverse DNS Lookup** enabled, when a network-related event occurs, reverse DNS lookup logs in the event log both the IP address and the domain name for the networked device associated with the event. If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change much less frequently than IP addresses, enabling reverse DNS lookup can improve the ability to identify addresses of networked devices that are causing events to occur.

Ping utility (control console)

Select this option, available only in the control console, to check the network connection by testing whether a defined IP address or domain name responds to the Ping network utility.

By default, the IP address of the default gateway is used. However, you can use the IP address or domain name of any device known to be running on the network.

FTP server

Use the **Access** setting to enable or disable the FTP server. The server is enabled by default.



Note

FTP transfers files without using encryption. For higher security, use SCP for file transfers. When you select and configure SSH, SCP is enabled automatically. To configure SSH, see [Telnet/SSH](#). If you decide to use SCP for file transfer, be sure to disable the FTP server.

Use the **Port** setting to identify the TCP/IP port that the FTP server uses for communications with the Environmental Monitoring Unit. The default **Port** setting is **21**.

You can change the **Port** setting to any unused port from **5000** to **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port. For example, for a port number of 5000 and a Environmental Monitoring Unit IP address of 159.215.12.114, you would use this command:

```
ftp 159.215.12.114:5000
```



To access a text version of the Environmental Monitoring Unit's event or data log, see [How to use FTP or SCP to retrieve log files](#).

Telnet/SSH

Use the **Telnet/SSH** option to perform the following tasks:

- Enable or disable Telnet or the Secure SHell (SSH) protocol for remote control console access.
 - While SSH is enabled, you cannot use Telnet to access the control console.
 - Enabling SSH enables SCP automatically.



Note

When SSH is enabled and its port and encryption ciphers are configured, no further configuration is required to use SCP. (SCP uses the same configuration as SSH.)

- Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.)



Note

To use SSH, you must have an SSH client installed. Most Linux and other UNIX[®] platforms include an SSH client as part of their installation, but Microsoft Windows operating systems do not. SSH clients are available from various vendors.

- Configure the port settings for Telnet and SSH.
- Select one or more data encryption algorithms for SSH, version 1, version 2, or both.
- In the Web interface, specify a host key file previously created with the APC Security Wizard and load it to the Environmental Monitoring Unit.



Note

From a command line interface, such as the command prompt on Windows operating systems, you can use FTP or SCP to transfer the host key file. You must transfer the file to location `/sec` on the Environmental Monitoring Unit.

If you do not specify a host key file, the Environmental Monitoring Unit generates an RSA host key of 768 bits, instead of the 1024-bit RSA host key that the Wizard creates.

The Environmental Monitoring Unit can take up to 5 minutes to create this host key, and SSH is not accessible during that time.

- Display the *fingerprint* of the SSH host key for SSH versions 1 and 2. Most SSH clients display the fingerprint at the start of a session. Compare the fingerprint displayed by the client to the fingerprint that you recorded from the Web interface or control console of the Environmental Monitoring Unit.



Note

If you are using SSH version 2, expect a noticeable delay when logging on to the control console of the Environmental Monitoring Unit. Although the delay is not long, it can be mistaken for a problem because there is no explanatory message.

Option	Description
Telnet/SSH Network Configuration	
Access	<p>Enables or disables the access method selected in Protocol Mode.</p> <p>NOTE: Enabling SSH automatically disables Telnet. To enable SSH, change the setting and then click Next>> in the Web interface or choose Accept Changes in the control console. You must then agree to the license agreement that is displayed.</p>
Protocol Mode	<p>Choose one of the following:</p> <ul style="list-style-type: none"> • Telnet: User names, passwords, and data are transmitted without encryption. • Secure SHell (SSH), version 1: User names, passwords, and data are transmitted in encrypted form. There is little or no delay when you are logging on. • Secure SHell (SSH), version 2: User names, passwords, and data are transmitted in encrypted form, but with somewhat more protection than version 1 from attempts to intercept, forge, or alter data during data transmission. There is a noticeable delay when you are logging on to the Environmental Monitoring Unit. • Secure SHell (SSH), versions 1 and 2: Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.)

Option	Description
Telnet/SSH Port Configuration	
Telnet Port	<p>Identifies the TCP/IP port used for communications by Telnet with the Environmental Monitoring Unit. The default is 23.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings. Then, according to the requirements of your Telnet client program, you must use either a colon (:) or a space in the command line to specify the non-default port number. For example, for a port number of 5000 and a Environmental Monitoring Unit IP address of 159.215.12.114, your Telnet client would require one or the other of the following commands:</p> <pre>telnet 159.215.12.114:5000 telnet 159.215.12.114 5000</pre>
SSH Port	<p>Identifies the TCP/IP port used for communications by the Secure SHell (SSH) protocol with the Environmental Monitoring Unit. The default is 22.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings. See the documentation for your SSH client for information on the command line format required to specify a non-default port number when starting SSH.</p>

Option	Description
SSH Server Configuration	
SSHv1 Encryption Algorithms	<p>Enables or disables DES, and displays the status (always enabled) of Blowfish, two encryption algorithms (block ciphers) compatible with SSH version 1 clients.</p> <ul style="list-style-type: none"> • DES: The key length is 56 bits. • Blowfish: The key length is 128 bits. You cannot disable this algorithm. <p>NOTE: Not all SSH clients can use every algorithm. If your SSH client cannot use Blowfish, you must also enable DES.</p>
SSHv2 Encryption Algorithms	<p>Enables or disables the following encryption algorithms (block ciphers) that are compatible with SSH version 2 clients.</p> <ul style="list-style-type: none"> • 3DES (enabled by default): The key length is 168 bits. • Blowfish (enabled by default): The key length is 128 bits. • AES 128: The key length is 128 bits. • AES 256: The key length is 256 bits. <p>NOTE: Not all SSH clients can use every algorithm. Your SSH client selects the algorithm that provides the highest security from among the enabled algorithms that it is able to use. (If your SSH client cannot use either of the default algorithms, you must enable an AES algorithm that it can use.)</p>

Option	Description
SSH User Host Key File	
Status:	<p>The Status field Indicates the status of the host key (<i>private</i> key). In the control console, display host key status by selecting Advanced SSH Configuration.</p> <ul style="list-style-type: none"> • SSH Disabled: No host key in use: No host key has been transferred to the Environmental Monitoring Unit or a host key has been transferred improperly. <p>NOTE: A host key must be installed to the /sec directory of the Environmental Monitoring Unit.</p> <ul style="list-style-type: none"> • Generating: The Environmental Monitoring Unit is generating a host key because no valid host key was installed in its /sec directory. • Loading: A host key is being loaded (i.e., being activated on the Environmental Monitoring Unit). • Valid: The host key is valid. (If you install an invalid host key, the Environmental Monitoring Unit discards it and generates a valid one. However, a host key that the Environmental Monitoring Unit generates is only 768 bits in length. A valid host key created by the APC Security Wizard is 1024 bits.)
Filename:	<p>You can create a host key file with the APC Security Wizard and then upload it to the Environmental Monitoring Unit by using the Web interface. Use the Browse button for the Filename field to locate the file, then click Apply.</p> <p>Alternatively, you can use FTP or SCP to transfer the host key file to the Environmental Monitoring Unit.</p> <p>NOTE: Creating and uploading a host key in advance reduces the time required to enable SSH. If no host key is loaded when you enable SSH, the Environmental Monitoring Unit creates one when it reboots. The Environmental Monitoring Unit takes up to 5 minutes to create this key, and the SSH server is not accessible during that time.</p>

Option	Description
SSH Host Key Fingerprint	
SSH v1:	Displays the SSH version 1 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose Advanced SSH Configuration and then Host Key Information to display the fingerprint.
SSH v2:	Displays the SSH version 2 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose Advanced SSH Configuration and then Host Key Information to display the fingerprint.

SNMP

An **Access** option (the **Settings** option in the control console) enables (by default) or disables SNMP. When SNMP is enabled, the **Access Control** settings allow you to control how each of the four available SNMP channels is used.



To define up to four NMSs to serve as trap receivers, see [Trap receiver settings](#).

Setting	Definition	
Community Name	This setting defines the password (maximum of 15 characters) which an NMS that is defined by the NMS IP/Domain Name setting uses to access the channel.	
NMS IP/ Domain Name	Limits access to the NMS specified by a domain name or to the NMSs specified by the format used for the IP address: <ul style="list-style-type: none"> • A domain name allows only the NMS at that location to have access. • 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. 	
Access Type	Selects how the NMS defined by the NMS IP setting can use the channel, when that NMS uses the correct Community Name .	
	Read	The NMS can use GETs at any time, but it can never use SETs.
	Write	The NMS can use GETs at any time, and can use SETs when no one is logged on to the control console or Web interface.
	Disabled	The NMS cannot use GETs or SETs.
	Write+	The NMS can use GETs and SETs at any time, even when someone is logged on to the control console or Web interface.

Email

Use this option to define two SMTP settings (**SMTP Server** and **From Address**) used by the e-mail feature of the Environmental Monitoring Unit.



See [SMTP settings](#) and [E-mail Feature](#).

Syslog

By default, the Environmental Monitoring Unit can send messages to up to four Syslog servers whenever Environmental Monitoring Unit or embedded management card events occur. The Syslog servers, which must be specifically identified by their IP addresses or domain names, record the events in a log that provides a centralized record of events that occur at network devices.



See also

This user's guide does not describe Syslog, or the Syslog configuration values, in detail. For more information about Syslog, see RFC3164, a copy of which is available at www.ietf.org/rfc/rfc3164.

Syslog settings. Leave the Syslog settings, except the **Server IP** settings, set to their defaults unless otherwise specified by the Syslog network or system administrator.

General Settings	
Setting	Definition
Syslog	Enables (by default) or disables the Syslog feature.
Facility	Selects the facility code assigned to the Environmental Monitoring Unit's Syslog messages (User , by default). NOTE: Although other selections are available, User is the selection that best defines the Syslog messages sent by an Environmental Monitoring Unit.

Syslog Server Settings	
Server IP/ Domain Name	<p>Uses specific IP addresses or domain names to identify which of up to four servers will receive Syslog messages sent by the Environmental Monitoring Unit.</p> <p>NOTE: To use the Syslog feature, the Server IP/Domain Name setting must be defined for at least one server.</p>
Port	<p>Identifies the user datagram protocol (UDP) port that the Environmental Monitoring Unit will use to send Syslog messages. The default is 514, the number of the UDP port assigned to Syslog.</p>
Local Priority (Severity Mapping)	
Map to Syslog's Priorities	<p>Maps each of the severity levels (Local Priority settings) that can be assigned to embedded management card and Environmental Monitoring Unit events to the available Syslog priorities. The following definitions are from RFC3164:</p> <ul style="list-style-type: none"> • Emergency: The system is unusable • Alert: Action must be taken immediately • Critical: Critical conditions • Error: Error conditions • Warning: Warning conditions • Notice: Normal but significant conditions • Informational: Informational messages • Debug: Debug-level messages <p>The following are the default settings for the four Local Priority settings:</p> <ul style="list-style-type: none"> • Severe is mapped to Critical • Warning is mapped to Warning • Informational is mapped to Info • None (for events which have no severity level assigned) is mapped to Info <p>NOTE: To disable sending Syslog messages for Severe, Warning, or Informational events, see Event Actions (Web Interface Only).</p>

Syslog test (Web interface). This option allows you to send a test message to the Syslog servers configured in the **Syslog Server** section.

1. Select the **Priority** to assign to the test message.
2. Define the **Test Message** using any text in the format described in **Syslog message format**. For example, EMU: Communications Established 0x0F01 meets the required message format.
3. Click **Apply** to have the Environmental Monitoring Unit send a Syslog message that uses the defined **Priority** and **Test Message** settings.

Syslog message format. A Syslog message has three parts:

- The priority (PRI) part identifies the Syslog priority assigned to the message's event and the facility code assigned to messages sent by the Environmental Monitoring Unit.
- The Header includes a time stamp and the IP address of the Environmental Monitoring Unit.
- The message (MSG) part has two fields:
 - A TAG field, which is followed by a colon and a space, identifies the event type (System or EMU, for example)
 - A CONTENT field provides the event text, followed by a space and the event code

Web/SSL

Use the **Web/SSL** menu to perform the following tasks.

- Enable or disable the two protocols that provide access to the Web interface of the Environmental Monitoring Unit:
 - Hypertext Transfer Protocol (HTTP) provides access by user name and password, but does not encrypt user names, passwords, and data during transmission.
 - Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS). Secure Sockets Layer (SSL) encrypts user names, passwords, and data during transmission and provides authentication of the Environmental Monitoring Unit by means of digital certificates.



See [Creating and Installing Digital Certificates](#) to choose among the several methods for using digital certificates.


- Configure the ports that each of the two protocols will use.
- Select the encryption ciphers that SSL will use.
- Identify whether a server certificate is installed on the Environmental Monitoring Unit. If a certificate has been created with the APC Security Wizard but is not installed:
 - In the Web interface, browse to the certificate file and upload it to the Environmental Monitoring Unit.
 - Alternatively, use the SCP protocol or FTP to upload it to the location **lsec** on the Environmental Monitoring Unit.



Note

Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL). If no server certificate is loaded when you enable HTTPS (SSL), the Environmental Monitoring Unit creates one when it reboots. **The Environmental Monitoring Unit can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.**

- Display the configured parameters of a digital server certificate, if one is installed.

Option	Description
Web/SSL Network Configuration	
Access	Enables or disables the access method selected in Protocol Mode .
Protocol Mode	<p>Choose one of the following:</p> <ul style="list-style-type: none">• HTTP: User names, passwords, and data are transmitted without encryption.• HTTPS (SSL): User names, passwords, and data are transmitted in encrypted form, and digital certificates are used for authentication. <p>NOTE: To enable HTTPS (SSL), change the setting and then click Next>> in the Web interface, or choose Accept Changes in the control console. You must then agree to the license agreement that is displayed. To activate the changes you must log off and log back on to the interface. When SSL is activated, your browser displays a lock icon, usually at the bottom of the screen.</p> 

Option	Description
HTTP/HTTPS Port Configuration	
HTTP Port	<p>Identifies the TCP/IP port used for communications by HTTP with the Environmental Monitoring Unit. The default is 80.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings.</p> <p>You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 5000 and a Environmental Monitoring Unit IP address of 159.215.12.114, you would use this command:</p> <pre>http://159.215.12.114:5000</pre>
HTTPS Port	<p>Identifies the TCP/IP port used for communications by HTTPS with the Environmental Monitoring Unit. The default is 443.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings.</p> <p>You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 6502 and a Environmental Monitoring Unit IP address of 159.215.12.114, you would use this command:</p> <pre>https://159.215.12.114:6502</pre>

Option	Description
SSL Server Configuration	
CipherSuite	<p>Enables or disables the following SSL encryption ciphers and hash algorithms. (To access these options in the control console, choose Web/SSL, then Advanced SSL Configuration.)</p> <p>NOTE: All of these encryption ciphers and hash algorithms use the RSA public key algorithm.</p> <ul style="list-style-type: none"> • DES (SSL_RSA_WITH_DES_CBC_SHA): a block cipher with a key length of 56 bits. A Secure Hash Algorithm (SHA) is used for authentication. • 3DES (SSL_RSA_WITH_3DES_EDE_CBC_SHA): a block cipher with a key length of 168 bits. A Secure Hash Algorithm (SHA) is used for authentication. • RC4 (SSL_RSA_WITH_RC4_128_SHA): a stream cipher with a key length of 128 bits. A Secure Hash Algorithm (SHA) is used for authentication. This selection is enabled by default. • RC4 (SSL_RSA_WITH_RC4_128_MD5): a stream cipher with a key length of 128 bits, with an RSA key exchange algorithm, and with a Message Digest 5 (MD5) hash algorithm used for authentication. This selection is enabled by default.

Option	Description
SSL Server Certificate	
Status	<p>The Status field indicates whether a server certificate is installed. (To display the status in the control console, choose Web/SSL, then Advanced SSL Configuration.)</p> <ul style="list-style-type: none"> • Not installed: No certificate is installed on the Environmental Monitoring Unit. <p>NOTE: If you install a certificate by using FTP or SCP, you must specify the correct location (/sec) on the Environmental Monitoring Unit.</p> <ul style="list-style-type: none"> • Generating: The Environmental Monitoring Unit is generating a certificate because no valid certificate was installed. • Loading: A certificate is being loaded (activated on the Environmental Monitoring Unit). • Valid: A valid certificate was installed to or generated by the Environmental Monitoring Unit. (If you install an invalid certificate, the Environmental Monitoring Unit discards it and generates a valid one. However, a certificate that the Environmental Monitoring Unit generates has some limitations. See Method 1: Use the auto-generated default certificate.)
SSL/TLS Server Certificate	
Filename:	<p>You can create a server certificate with the APC Security Wizard and then upload it to the Environmental Monitoring Unit by using the Web interface. Use the Browse button for the Filename field to locate the file, then click Apply. By default, the certificate is installed to the correct location.</p> <p>Alternatively, you can use FTP or SCP to transfer the server certificate to the Environmental Monitoring Unit. However, you must specify the correct location (/sec) on the Environmental Monitoring Unit.</p> <p>NOTE: Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL). If no server certificate is loaded when you enable HTTPS (SSL), the Environmental Monitoring Unit creates one when it reboots. The Environmental Monitoring Unit can take up to 5 minutes to create this certificate, and the SSL server is not available during that time.</p>

Parameter	Description
Current Certificate Details	
Issued To:	<p>Common Name (CN): The IP Address or DNS name of the Environmental Monitoring Unit, except if the server certificate was generated by default by the Environmental Monitoring Unit. For a default server certificate, the Common Name (CN) field displays the Environmental Monitoring Unit's serial number.</p> <p>NOTE: If an IP address was specified as the Common Name when the certificate was created, use an IP address to log on to the Web interface of the Environmental Monitoring Unit; if the DNS name was specified as the Common Name, use the DNS name to log on. When you log on, if you do not use the IP address or DNS name that was specified for the certificate, authentication fails, and you receive an error message asking if you want to continue.</p> <p>Organization (O), Organizational Unit (OU), and Locality Country: The name, organizational unit, and location of the organization that is using the server certificate. If the server certificate was generated by default by the Environmental Monitoring Unit, the Organizational Unit (OU) field displays "Internally Generated Certificate."</p> <p>Serial Number: The serial number of the server certificate.</p>
Issued By:	<p>Common Name (CN): The Common Name as specified in the CA root certificate, except if the server certificate was generated by default by the Environmental Monitoring Unit. For a default server certificate, the Common Name (CN) field displays the Environmental Monitoring Unit's serial number.</p> <p>Organization (O) and Organizational Unit (OU): The name and organizational unit of the organization that issued the server certificate. If the server certificate was generated by default by the Environmental Monitoring Unit, the Organizational Unit (OU) field displays "Internally Generated Certificate."</p>
Validity:	<p>Issued on: The date and time at which the certificate was issued.</p> <p>Expires on: The date and time at which the certificate expires.</p>

Parameter	Description
Current Certificate Details	
Fingerprint:	<p>Each fingerprint is a long string of alphanumeric characters punctuated by colons. A fingerprint is a unique identifier that you can use to further authenticate the server. Record the fingerprints to compare with the fingerprints contained in the certificate, as displayed in the browser.</p> <p>SHA1 Fingerprint: This fingerprint is created by a Secure Hash Algorithm (SHA).</p> <p>MD5 Fingerprint: This fingerprint is created by a Message Digest 5 (MD5) algorithm.</p>

System Menu

Introduction

Overview

Use the **System** menu to do the following tasks:

- Configure system identification, date and time settings, and access parameters for the Administrator, Device Manager, and Read-Only User accounts.
- Synchronize the real-time clock for the Environmental Monitoring Unit with a Network Time Protocol (NTP) server.
- Reset or restart the Environmental Monitoring Unit interface.
- Define the URL links available in the Web interface.
- Set the units (Fahrenheit or Celsius) used for temperature displays.
- Access hardware and firmware information about the Environmental Monitoring Unit.
- Download firmware files (control console only).
- Upload user configuration files to the Environmental Monitoring Unit.



Note

Only an Administrator has access to the **System** menu.

Menu options

Unless noted, the following menu options are available in the control console and Web interface:

- [User manager](#)
- [RADIUS](#)
- [Identification](#)
- [Date & Time](#)
- [Tools](#)
- [Preferences \(Web interface\)](#)
- [Links \(Web interface\)](#)
- [About System \(control console\)](#)



Note

The **About System** option is a **Help** menu option in the Web interface.

Option Settings

User manager

Use this option to define the access values shared by the control console and the Web interface, and the authentication used to access the Web interface.

Setting	Definition
Auto Logout	The number of minutes (3 , by default) before a user is automatically logged off because of inactivity.
Separate values for Administrator, Device Manager, and Read-Only User	
User Name	The case-sensitive name (maximum of 10 characters) used by Administrator and Device Manager users to log on at the control console or Web interface and by the Read-Only User to log on at the Web interface. Default values are apc for Administrator users, device for Device Manager users, and readonly for the Read-Only User .
Password	The case-sensitive password (maximum of 10 characters) always used to log on at the control console, but only used to log on to the Web interface when Basic is selected for the Authentication setting (apc is the default for the Password settings for the three account types). NOTE: A Read-Only User cannot log on through the control console.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization, and accounting service. Use this option to centrally administer remote access for each Environmental Monitoring Unit.

When a user accesses the Environmental Monitoring Unit, an authentication request is sent to the RADIUS server to determine the user's permission level.



Note

RADIUS user names are limited to 32 characters.



For more information on user permission levels, see [Types of user accounts](#).



Note

RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.

RADIUS Setting	Definition
Access	Local Only: RADIUS is disabled. Access to the Environmental Monitoring Unit is controlled by the local user manager only.
	RADIUS then Local: RADIUS is enabled. Contact the RADIUS server first. If the RADIUS server fails to authenticate the user, the local user manager will be used to authenticate access to the Environmental Monitoring Unit.
	RADIUS Only: RADIUS is enabled. Only the RADIUS server will be contacted. If the RADIUS server fails to authenticate the user, access will be denied. NOTE: If RADIUS only is selected, the only way to recover if the RADIUS server is unavailable is through a serial connection to the control console.
Primary Server	The server name or IP address of the main RADIUS server.
Primary Server Secret	The shared secret between the primary RADIUS server and the Environmental Monitoring Unit.
Secondary Server	The server name or IP address of the secondary RADIUS server.
Secondary Server Secret	The shared secret between the secondary RADIUS server and the Environmental Monitoring Unit.
Timeout	The time in seconds that the Environmental Monitoring Unit waits for a response from the RADIUS server.

Configuring the RADIUS server. You must configure your RADIUS server to work with the Environmental Monitoring Unit. The following example is specific to the APC RADIUS server.

1. Define an APC vendor in your RADIUS server; 318 is the APC Private Enterprise Number assigned by the Internet Assigned Numbers Authority (IANA).
2. Define a RADIUS vendor-specific attribute called `APC-Service-Type`. This is an integer with an attribute identifier of 1.
3. Configure RADIUS users. The `APC-Service-Type` attribute must be configured for each RADIUS user accessing the card. This attribute is set to one of the following values, which correspond to an access level on the Management Card.
 - 1 - Administrator
 - 2 - Device Manager
 - 3 - Read-Only User



For more information on user permission levels, see [Types of user accounts](#).

Identification

Use this option to define the System **Name**, **Contact**, and **Location** values used by the SNMP agent for the Environmental Monitoring Unit. The option's settings provide the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifications (OIDs).



See also

For more information about the MIB-II OIDs, see the PowerNet® *SNMP Management Information Base (MIB) Reference Guide* ([.\doclen\mibguide.pdf](#)) provided on the APC *Utility* CD that came with your Environmental Monitoring Unit.

Date & Time

Use this option to set the date and time used by the Environmental Monitoring Unit. The option displays the current settings, and allows you to change those settings manually, or through a Network Time Protocol (NTP) Server.

Set Manually. Use this option in the Web interface, or **Manual** in the control console, to define the date and time for the Environmental Monitoring Unit.



Note

An **Apply Local Computer Time to Environmental Monitoring Unit** option, which is available in the Web interface only, sets these values to match the date and time settings of the computer you are using to access the Web interface.

Synchronize with Network Time Protocol (NTP) Server. Use this option, or **Network Time Protocol (NTP)** in the control console, to have an NTP Server update the date and time for the Environmental Monitoring Unit automatically.



Note

In the control console, use the **NTP Client** option to enable or disable (the default) the NTP Server updates. In the Web interface, use the **Set Manually** option to disable the updates.

Setting	Definition
Primary NTP Server	Identifies the IP address or domain name of the primary NTP server.
Secondary NTP Server	Identifies the IP address or domain name of the secondary NTP server, when a secondary server is available.
GMT Offset (Time Zone)	Defines the offset from Greenwich Mean Time (GMT) based on the Environmental Monitoring Unit's time zone.
Update Interval	Defines how often, in hours, the Environmental Monitoring Unit accesses the NTP Server for an update. The minimum is 1 hour; the maximum is 8760 hours (1 year). Use Update Using NTP Now to initiate an immediate update as well.

Tools

Initiating an action. Use this drop-down list in the Web interface or the equivalent menu options in the control console to restart the interface of the Environmental Monitoring Unit, to reset some or all of its configuration settings to their default values, or to delete SSH Host Keys and SSL Certificates.

Action	Definition
Reboot Management Interface	Restarts the interface of the Environmental Monitoring Unit.
Reset to Defaults	Resets all configuration settings. NOTE: For information about how this affects the Boot mode setting, see this table's description of Reset Only TCP/IP to Defaults .
Reset to Defaults Except TCP/IP	Resets all configuration settings except the TCP/IP settings.
Reset Only TCP/IP to Defaults	Resets the TCP/IP settings only. NOTE: With Boot mode set to DHCP & BOOTP , its default setting, the Environmental Monitoring Unit's TCP/IP settings must be defined by a DHCP or BOOTP server. See TCP/IP .
Delete SSH Host Keys and SSL Certificates	Removes any SSH host key and server certificate on the Environmental Monitoring Unit so that you can reconfigure these components of your security system.

Uploading an initialization file (Web interface only). To transfer configuration settings from a configured Environmental Monitoring Unit to the current Environmental Monitoring Unit, export the .ini file from the configured Environmental Monitoring Unit, select the **Tools** menu on the current Environmental Monitoring Unit, browse to the file, and click **Upload**. The current Environmental Monitoring Unit imports the file and uses it to set its own configuration. The **Status** field reports the progress of the upload.



See [How to Export Configuration Settings](#) for information on the content of the .ini file, how to preserve comments you add to the file, and how to export settings to multiple Environmental Monitoring Units.

File Transfer (control console only). The **File Transfer** option of the **Tools** menu provides two methods for file transfer over the network and one for file transfer through a serial connection to the Environmental Monitoring Unit.

Option	Description
XMODEM	Allows you to transfer either an .ini file or a firmware upgrade file to a Environmental Monitoring Unit using a terminal-emulation program. This option is available only when you use a local connection to the control console. See Local access to the control console .
FTP Client	Use one of these two options to transfer either an .ini file or a firmware upgrade file from an FTP or TFTP server of your organization (company, agency, or department) to the current Environmental Monitoring Unit. These options assume that your organization has a centralized system for configuring or upgrading APC Environmental Monitoring Units. For FTP Client , you are prompted for a user name and password. For either option, you are then prompted for the server address and the file to transfer. After you supply that required information, the Environmental Monitoring Unit transfers the file.
TFTP Client	

Preferences (Web interface)

Use this option to define whether temperature values are displayed as **Fahrenheit** or **Celsius** in the Web interface and the control console.

Links (Web interface)

Use this option to modify the links to APC Web pages.

Setting	Definition
User Links	
Name	Defines the link names that appear in the Links menu (by default, APC's Web site , Testdrive Demo , and Remote Monitoring).
URL	Defines the URL addresses used by the links. By default, the following URL addresses are used: <ul style="list-style-type: none">• http://www.apc.com (APC's Web site)• http://testdrive.apc.com (Testdrive Demo)• http://rms.apc.com (Remote Monitoring) NOTE: Only links of type http:// can be used in these fields. For information about these pages see Links menu .
Access Links	
APC Home Page	Defines the URL address used by the APC logo at the top of all Web interface pages (by default, http://www.apc.com).

About System (control console)

This option identifies the following hardware information for the Environmental Monitoring Unit: **Model Number**, **Serial Number**, **Hardware Revision**, **Manufacture Date**, and **MAC Address**.

This screen also displays **Name**, **Version**, **Date**, and **Time** for the Application Module and AOS.

The **About System** menu also includes fields for system **Flash Type** and the **Type**, **Sector**, and **CRC 16** for each module.



Note

In the Web interface, except for **Flash Type**, this hardware information is reported by the **About System** option in the **Help** menu.

Boot Mode

Introduction

Overview

In addition to using a BOOTP server or manual settings, the Environmental Monitoring Unit can use a dynamic host configuration protocol (DHCP) server to provide the settings that it needs to operate on a TCP/IP network.

The method that is used to provide the network settings for the Environmental Monitoring Unit depends on **Boot mode**, a **TCP/IP** option in the **Network** menu. To use a DHCP server to provide the network assignment for the Environmental Monitoring Unit, **Boot mode** must be set to either **DHCP & BOOTP**, its default setting, or **DHCP only**.



See also

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

DHCP & BOOTP boot process

When **Boot mode** is set to its default **DHCP & BOOTP** setting, the following occurs when the Environmental Monitoring Unit is started or reset:

1. The Environmental Monitoring Unit makes up to five requests for its network assignment from any BOOTP server. If a valid BOOTP response is received, the Environmental Monitoring Unit starts the network services and sets **Boot mode** to **BOOTP Only**.
2. If the Environmental Monitoring Unit fails to receive a valid BOOTP response after five BOOTP requests, the Environmental Monitoring Unit makes up to five requests for its network assignment from any DHCP server. If a valid DHCP response is received, the Environmental Monitoring Unit starts the network services and sets **Boot mode** to **DHCP Only**.



Note

To configure the Environmental Monitoring Unit so that it always uses the **DHCP & BOOTP** setting for **Boot mode**, enable the **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** option, which is disabled by default.



See [Environmental Monitoring Unit settings](#).

3. If the Environmental Monitoring Unit fails to receive a valid DHCP response after five DHCP requests, it repeats BOOTP and DHCP requests until it receives a valid network assignment. First it sends a BOOTP request every 32 seconds for 12 minutes, then it sends one DHCP request with a time-out of 64 seconds, and so forth.



Note

If a DHCP server responds with an invalid offer (e.g., without the APC cookie), the Environmental Monitoring Unit accepts the lease from that server on the last request of the sequence and immediately releases that lease. This prevents the DHCP server from reserving the IP address associated with its invalid offer.



See also

For more information on what a valid response requires, see [DHCP response options](#).

DHCP Configuration Settings

Environmental Monitoring Unit settings

The **TCP/IP** option in the **Network** menu of the Web interface and control console accesses the network settings for the Environmental Monitoring Unit.

Three settings (**Port Speed**, **Host Name**, and **Domain Name**) are available regardless of the **TCP/IP** option's **Boot mode** selection, and three settings (**Vendor Class**, **Client ID**, and **User Class**) are available for any **Boot mode** selection except **Manual**.

When **Boot mode** is set to **DHCP & BOOTP**, two options are available:

- **After IP Assignment** in the control console (or **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** in the Web interface): By default, this option switches **Boot mode** to **DHCP Only** or **BOOTP Only**, depending on the configuration of the server that provided the TCP/IP settings.
- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.



For more information about the APC cookie, see [DHCP response options](#).

When **Boot mode** is set to **DHCP Only**, two options are available:

- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.



For more information about the APC cookie, see [DHCP response options](#).

- **Retry Then Stop** in the control console (or **Maximum # of Retries** in the Web interface): This option sets the number of times the Environmental Monitoring Unit will repeat the DHCP request if it does not receive a valid response. By default, the number of retries is 0, which sets the Environmental Monitoring Unit to continue repeating the DHCP request indefinitely.

DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings that the Environmental Monitoring Unit needs to operate on a network, and other information that affects the operation of the Environmental Monitoring Unit.

The Environmental Monitoring Unit uses the Vendor Specific Information option (option 43) in a DHCP response to determine whether the DHCP response is valid.

Vendor Specific Information (option 43). The Vendor Specific Information option contains up to two APC specific options encapsulated in a Tag/Len/Data format: the APC cookie and the Boot Mode Transition.

APC Cookie. Tag 1, Len 4, Data “1APC”

Option 43 notifies the Environmental Monitoring Unit that a DHCP server has been configured to service APC devices. By default, the APC cookie must be present in this DHCP response option before the Environmental Monitoring Unit can accept the lease.



Note

Use the **DHCP Cookie Is** setting described in [Environmental Monitoring Unit settings](#) to disable the APC cookie requirement.

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 **After IP Assignment** option which, by default, causes the **Boot mode** option to use the setting that reflects the server that provided the TCP/IP settings (**DHCP Only** or **BOOTP Only**).

- For a data value of 1, the **After IP Assignment** option is disabled, and the **Boot mode** option remains in its **DHCP & BOOTP** setting after successful network assignment. Whenever the Environmental Monitoring Unit restarts, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.



See [DHCP & BOOTP boot process](#).

- For a data value of 2, the **After IP Assignment** option is enabled and the **Boot mode** option switches to **DHCP Only** when the Environmental Monitoring Unit accepts the DHCP response. Whenever the Environmental Monitoring Unit restarts, it will request its network assignment (TCP/IP settings) from a DHCP server only.



For more information about the **After IP Assignment**, see [Environmental Monitoring Unit settings](#).

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

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

TCP/IP options. The Environmental Monitoring Unit uses the following options within a valid DHCP response to define its TCP/IP settings:

- **IP Address** (from the **yiaddr** field of the DHCP response): Provides the IP address that the DHCP server is leasing to the Environmental Monitoring Unit.
- **Subnet Mask** (option 1): Provides the subnet mask value needed by the Environmental Monitoring Unit to operate on the network.
- **Default Gateway** (option 3): Provides the default gateway address needed by the Environmental Monitoring Unit to operate on the network.
- **Address Lease Time** (option 51): Identifies the length of time for the lease associated with the identified **IP Address**.
- **Renewal Time, T1** (option 58): Identifies how long the Environmental Monitoring Unit must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): Identifies how long the Environmental Monitoring Unit must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other options. The Environmental Monitoring Unit uses the following options within a valid DHCP response to define NTP, DNS, host name, and domain name settings:

- **NTP Server, Primary and Secondary** (option 42): Identifies up to two NTP servers that can be used by the Environmental Monitoring Unit.
- **NTP Time Offset** (option 2): Specifies the offset, in seconds, of the subnet for the Environmental Monitoring Unit from Coordinated Universal Time (UTC).
- **DNS Server, Primary and Secondary** (option 6): Identifies one or two DNS servers that can be used by the Environmental Monitoring Unit.
- **Host Name** (option 12): Identifies the host name (maximum length of 32 characters) to be used by the Environmental Monitoring Unit.
- **Domain Name** (option 15): Identifies the domain name (maximum length of 64 characters) to be used by the Environmental Monitoring Unit.

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.

Summary of access methods

Serial control console.

Security Access	Description
Access is by user name and password.	Always enabled.

Remote control console.

Security Access	Description
Available methods: <ul style="list-style-type: none">• User name and password• Selectable server port• Server Enable/Disable• Secure SHell (SSH)	For high security, use SSH. <ul style="list-style-type: none">• With Telnet, the user name and password are transmitted as plain text.• SSH disables Telnet and provides encrypted access to the control console interface to provide additional protection from attempts to intercept, forge, or alter data during data transmission.

SNMP.

Security Access	Description
Available methods: <ul style="list-style-type: none">• Community Name• Domain Name• NMS IP filters• Agent Enable/Disable• Four access communities with read/write/disable capability	The domain name restricts access only to the NMS as that location, and the NMS IP filters allow access only from designated IP addresses. <ul style="list-style-type: none">• 162.245.12.1 allows only the NMS with that IP address to have access.• 162.245.12.255 allows access for any NMS on the 162.245.12 segment.• 162.245.255.255 allows access for any NMS on the 162.245 segment.• 162.255.255.255 allows access for any NMS on the 162 segment.• 0.0.0.0 or 255.255.255.255 allows access for any NMS.

File transfer protocols.

Security Access	Description
Available methods: <ul style="list-style-type: none">• User name and password• Selectable server port• Server Enable/Disable• Secure CoPy (SCP)	With FTP, the user name and password are transmitted as plain text, and files are transferred without the protection of encryption. Using SCP instead of FTP encrypts the user name and password and the files being transferred, such as firmware updates, configuration files, log files, Secure Sockets Layer (SSL) certificates, and Secure SHell (SSH) host keys. If you choose SCP as your file transfer protocol, enable SSH and disable FTP.

Web Server.

Security Access	Description
Available methods: <ul style="list-style-type: none">• User name and password• Selectable server port• Server Enable/Disable• Secure Sockets Layer (SSL) and Transport Layer Security (TLS)	<p>In basic HTTP authentication mode, the user name and password are transmitted base-64 encoded (with no encryption).</p> <p>SSL and TLS are available on Web browsers supported for the Environmental Monitoring Unit and on most Web servers. The Web protocol Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) encrypts and decrypts page requests to the Web server and pages returned by the Web server to the user.</p>

RADIUS.

Security Access	Description
Available methods: <ul style="list-style-type: none">• Centralized authentication of access rights• A server secret shared between the RADIUS server and the Environmental Monitoring Unit	<p>RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization, and accounting service used to centrally administer remote access for each Environmental Monitoring Unit.</p>

Changing default user names and passwords immediately

As soon as you complete the installation and initial configuration of the Environmental Monitoring Unit, immediately change the default user names and passwords. Configuring unique user names and passwords is essential for establishing basic security for your system.

Port assignments

If a Telnet, FTP, SSH/SCP, or Web/SSL 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 these 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 32768.

User names, passwords, and community names (SNMP)

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 on to the accounts of the control console or Web interface of the Environmental Monitoring Unit. If your network requires the higher security of the encryption-based options available for the control console and Web interface, be sure to disable SNMP access or set its access to read-only. (Read-only access allows you to receive status information and to use SNMP traps.)

Authentication versus encryption

You can select to use security features for the Environmental Monitoring Unit that control access by providing basic authentication through user names, passwords, and IP addresses, without using encryption. These basic security features are sufficient for most environments in which sensitive data are not being transferred.

To ensure that data and communication between the Environmental Monitoring Unit and the client interfaces, such as the control console and the Web interface, cannot be intercepted, you can provide a greater level of security by using one or more of the following encryption-based methods:

- For the Web interface, use the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.
- To encrypt user names and passwords for control console access, use the Secure SHell (SSH) protocol.
- To encrypt user names, passwords, and data for the secure transfer of files, use the SCP protocol.



For more information on these protocols for encryption-based security, see [Secure SHell \(SSH\) and Secure CoPy \(SCP\)](#) and [Secure Sockets Layer \(SSL\)](#).

Encryption

Secure SHell (SSH) and Secure CoPy (SCP)

The Secure SHell (SSH) protocol provides a secure mechanism to access computer consoles or *shells* remotely. The protocol authenticates the server (in this case, the Environmental Monitoring Unit) and encrypts all transmissions between the SSH client and the server.

- SSH is an alternative to Telnet, which does not provide encryption.
- SSH protects the username and password, the credentials for authentication, from being used by anyone intercepting network traffic.
- To authenticate the SSH server (the Environmental Monitoring Unit) to the SSH client, SSH uses a host key that is unique to the SSH server and that provides an identification that cannot be falsified. Therefore, an invalid server on the network cannot obtain a user name and password from a user by presenting itself as a valid server.



To create a host key, see [Create an SSH Host Key](#).

- The Environmental Monitoring Unit supports versions 1 and 2 of SSH. The encryption mechanisms of the versions differ, and each version has advantages. Version 1 provides faster login to the Environmental Monitoring Unit, and version 2 provides improved protection from attempts to intercept, forge, or change data that are transmitted.
- When you enable SSH, Telnet is automatically disabled.
- The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet.



For information on supported SSH client applications, see [Telnet/SSH](#).

Secure CoPy (SCP) is a secure file transfer application that you can use instead of FTP. SCP uses the SSH protocol as the underlying transport protocol for encryption of user names, passwords, and files.

- When you enable and configure SSH, you automatically enable and configure SCP. No further configuration of SCP is needed.
- You must explicitly disable FTP. It is **not** disabled by enabling SSH.

Secure Sockets Layer (SSL)

For secure Web communication, enable Secure Sockets Layer (SSL) and Transport Layer Security (TLS) by selecting HTTPS (SSL/TLS) as the protocol mode to use for access to the Web interface of the Environmental Monitoring Unit. Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) is a Web protocol that encrypts and decrypts page requests from the user and pages that are returned by the Web server to the user. Originally developed by Netscape, it has become an internet standard supported by most Web browsers.

The Environmental Monitoring Unit supports SSL version 3.0 and TLS version 1.0. Most browsers let you select the version of SSL to enable.



When SSL is enabled, your browser displays the lock icon, usually at the bottom of the screen.

SSL uses a digital certificate to enable the browser to authenticate the server (in this case, the Environmental Monitoring Unit). The browser verifies the following:

- The format of the server certificate is correct.
- The server certificate's expiration date and time has not passed.
- The DNS name or IP address specified when a user logs on matches the common name in the server certificate.
- The server certificate is signed by a trusted certifying authority.

Each major browser manufacturer distributes CA root certificates of the commercial Certificate Authorities in the certificate store (cache) of its browser so that it can compare the signature on the server certificate to the signature on a CA root certificate.

You can use the APC Security Wizard, provided on the APC Environmental Monitoring Unit *Utility* CD that came with your Environmental Monitoring Unit, to create a certificate signing request to an external Certificate Authority, or if you do not want to use an existing Certificate Authority, you can create an APC root certificate to upload to a browser's certificate store (cache). You can also use the Wizard to create a server certificate to upload to the Environmental Monitoring Unit.



See [Creating and Installing Digital Certificates](#) for a summary of how these certificates are used.



To create certificates and certificate requests, see [Create a Root Certificate & Server Certificates](#) and [Create a Server Certificate and Signing Request](#).

SSL also uses various algorithms and encryption ciphers to authenticate the server, encrypt data, and ensure the integrity of the data (i.e. that it has not been intercepted and sent by another server).



See [CipherSuite](#) to select which authentication and encryption algorithms to use.



Note

Web browsers cache (save) Web pages that you recently accessed and allow you to return to those pages without re-entering your user name and password. Always close your browser session before you leave your computer unattended.

Creating and Installing Digital Certificates

Purpose

For network communication that requires a higher level of security than password encryption, the Web interface of the Environmental Monitoring Unit supports the use of digital certificates with the Secure Sockets Layer (SSL) protocol. Digital certificates can authenticate the Environmental Monitoring Unit (the server) to the Web browser (the SSL client).

The sections that follow summarize the three methods of creating, implementing, and using digital certificates. Read these sections to determine the most appropriate method for your system.

- Method 1: Use the auto-generated default certificate.
- Method 2: Use the APC Security Wizard to create a CA certificate and a server certificate.
- Method 3: Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate.



Note

You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the APC Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

Choosing a method for your system

Using the Secure Sockets Layer (SSL) protocol, you can choose any of the following methods for using digital certificates.

Method 1: Use the auto-generated default certificate. When you enable SSL, you must reboot the Environmental Monitoring Unit. During rebooting, if no server certificate exists on the Environmental Monitoring Unit, the Environmental Monitoring Unit generates a default server certificate that is self-signed but that you cannot configure.

This method has the following advantages and disadvantages:

- **Advantages:**

- Before they are transmitted, the user name and password for Environmental Monitoring Unit access and all data to and from the Environmental Monitoring Unit are encrypted.
- You can use this default server certificate to provide encryption-based security while you are setting up either of the other two digital certificate options, or you can continue to use it for the benefits of encryption that SSL provides.

- **Disadvantages:**

- The Environmental Monitoring Unit takes up to 5 minutes to create this certificate, and the Web interface is not available during that time. (This delay occurs the first time you log on after you enable SSL.)
- This method does not include the browser-based authentication provided by a CA certificate (a certificate signed by a Certificate Authority) as Methods 2 and 3 provide. There is no CA Certificate cached in the browser. Therefore, whenever you log on to the Environmental Monitoring Unit, the browser generates a security alert, indicating that a certificate signed by a trusted authority is not available and asking if you want to proceed.

- The default server certificate on the Environmental Monitoring Unit has the Environmental Monitoring Unit's serial number in place of a valid *common name* (the DNS name or the IP address of the Environmental Monitoring Unit). Therefore, although the Environmental Monitoring Unit can control access to its Web interface by user name, password, and account type (e.g., **Administrator**, **Device Manager**, or **Read-Only User**), the browser cannot authenticate what Environmental Monitoring Unit is sending or receiving data.
- The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is only 768 bits. (The public key used in Methods 2 and 3 is 1024 bits, providing more complex encryption and consequently a higher level of security.)

Method 2: Use the APC Security Wizard to create a CA certificate and a server certificate. Use the APC Security Wizard to create two digital certificates:

- A *CA root certificate* (Certificate Authority root certificate) that the APC Security Wizard uses to sign all server certificates, and which you then install into the certificate store (cache) of the browser of each user who needs access to the Environmental Monitoring Unit.
- A *server certificate* that you upload to the Environmental Monitoring Unit. When the APC Security Wizard creates a server certificate, it uses the CA root certificate to sign the server certificate.

The Web browser authenticates the Environmental Monitoring Unit sending or requesting data:

- To identify the Environmental Monitoring Unit, the browser uses the *common name* (IP address or DNS name of the Environmental Monitoring Unit) that was specified in the server certificate's *distinguished name* when the certificate was created.
- To confirm that the server certificate is signed by a "trusted" signing authority, the browser compares the signature of the server certificate with the signature in the root certificate cached in the browser. An expiration date confirms whether the server certificate is current.

This method has the following advantages and disadvantages.

- **Advantages:**
 - Before they are transmitted, the user name and password for Environmental Monitoring Unit access and all data to and from the Environmental Monitoring Unit are encrypted.

- The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is 1024 bits, providing more complex encryption and consequently a higher level of security than the public key used in Method 1. (This longer encryption key is also used in Method 3.)
- The server certificate that you upload to the Environmental Monitoring Unit enables SSL to authenticate that data are being received from and sent to the correct Environmental Monitoring Unit. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
- The root certificate that you install to the browser enables the browser to authenticate the Environmental Monitoring Unit's server certificate to provide additional protection from unauthorized access.
- **Disadvantage:**

Because the certificates do not have the digital signature of a commercial Certificate Authority, you must load a root certificate individually into the certificate store (cache) of each user's browser. (Browser manufacturers already provide root certificates for commercial Certificate Authorities in the certificate store within the browser. See Method 3.)

Method 3: Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate. Use the APC Security Wizard to create a request (a **.csr** file) to send to a Certificate Authority. The Certificate Authority returns a signed certificate (a **.crt** file) based on information you submitted in your request. You then use the APC Security Wizard to create a server certificate (a **.p15** file) that includes the signature from the root certificate returned by the Certificate Authority. You upload the server certificate to the Environmental Monitoring Unit.



Note

You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the APC Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

This method has the following advantages and disadvantages.

- **Advantages:**

- Before they are transmitted, the user name and password for Environmental Monitoring Unit access and all data to and from the Environmental Monitoring Unit are encrypted.
- You have the benefit of authentication by a Certificate Authority that already has a signed root certificate in the certificate cache of the browser. (The CA certificates of commercial Certificate Authorities are distributed as part of the browser software, and a Certificate Authority of your own company or agency has probably already loaded its CA certificate to the browser store of each user's browser.) Therefore, you do not have to upload a root certificate to the browser of each user who needs access to the Environmental Monitoring Unit.

- The length of the *public key* (RSA key) that is used for setting up an SSL session is 1024 bits, providing more complex encryption and consequently a higher level of security than the public key used in Method 1. (This longer encryption key is also used in Method 2.)
- The server certificate that you upload to the Environmental Monitoring Unit enables SSL to authenticate that data are being received from and sent to the correct Environmental Monitoring Unit. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
- The browser matches the digital signature on the server certificate that you uploaded to the Environmental Monitoring Unit with the signature on the CA root certificate that is already in the browser's certificate cache to provide additional protection from unauthorized access.
- **Disadvantages:**
 - Setup requires the extra step of requesting a signed root certificate from a Certificate Authority.
 - An external Certificate Authority may charge a fee for providing signed certificates.

Firewalls

Although some methods of authentication provide a higher level of security than others, complete protection from security breaches is almost impossible to achieve. Well-configured firewalls are an essential element in an overall security scheme.

Using the APC Security Wizard

Overview

Authentication

Authentication verifies the identity of a user or a network device (such as an APC Environmental Monitoring Unit). Passwords typically identify computer users. However, for transactions or communications requiring more stringent security methods on the Internet, the Environmental Monitoring Unit supports more secure methods of authentication.

- Secure Sockets Layer (SSL), used for secure Web access, uses digital certificates for authentication. A digital *CA root* certificate is issued by a Certificate Authority (CA) as part of a public key infrastructure, and its digital signature must match the digital signature on a server certificate on the Environmental Monitoring Unit.
- Secure SHell (SSH), used for remote terminal access to the Environmental Monitoring Unit's control console, uses a public *host key* for authentication rather than a digital certificate.

How certificates are used. Most Web browsers, including all browsers supported by the Environmental Monitoring Unit, contain a set of CA root certificates from all of the commercial Certificate Authorities.

Authentication of the server (in this case, the Environmental Monitoring Unit) occurs each time a connection is made from the browser to the server. The browser checks to be sure that the server's certificate is signed by a Certificate Authority known to the browser. For this authentication to occur:

- Each Environmental Monitoring Unit with SSL enabled must have its own server certificate on the Environmental Monitoring Unit itself.
- Any browser that is used to access the Environmental Monitoring Unit's Web interface must contain the CA root certificate that signed the server certificate.

If authentication fails, the browser prompts you whether to continue despite the fact that it cannot authenticate the server.

If your network does not require the authentication provided by digital certificates, you can use the default certificate that the Environmental Monitoring Unit generates automatically. The default certificate's digital signature will not be recognized by browsers, but a default certificate enables you to use SSL for the encryption of transmitted user names, passwords, and data. (If you use the default certificate, the browser prompts you to agree to unauthenticated access before it logs you on to the Web interface of the Environmental Monitoring Unit.)

How SSH host keys are used. An SSH *host key* authenticates the identity of the server (the Environmental Monitoring Unit) each time an SSH client contacts the Environmental Monitoring Unit. Each Environmental Monitoring Unit with SSH enabled must have an SSH host key on the Environmental Monitoring Unit itself.

Files you create for SSL and SSH security

Use the APC Security Wizard to create the following components of an SSL and SSH security system:

- The server certificate for the Environmental Monitoring Unit, if you want the benefits of authentication that such a certificate provides. You can create either of the following types of server certificate:
 - A server certificate signed by a custom CA root certificate also created with the APC Security Wizard. Use this method if your company or agency does not have its own Certificate Authority and you do not want to use an external Certificate Authority to sign the server certificate.
 - A server certificate signed by an external Certificate Authority. This Certificate Authority can be one that is managed by your own company or agency or can be one of the commercial Certificate Authorities whose CA root certificates are distributed as part of a browser's software.
- A certificate signing request containing all the information required for a server certificate except the digital signature. You need this request if you are using an external Certificate Authority.
- A CA root certificate.
- An SSH host key that your SSH client program uses to authenticate the Environmental Monitoring Unit when you log on to the control console interface.



All public keys for SSL certificates and all host keys for SSH that are created with the APC Security Wizard are 1024-bit RSA keys. If you do not create and use SSL server certificates and SSH host keys with the APC Security Wizard, the Environmental Monitoring Unit generates 768-bit RSA keys.

Only APC server management and key management products can use server certificates, host keys, and CA root certificates created by the APC Security Wizard. These files will not work with products such as OpenSSL® and Microsoft IIS.

Create a Root Certificate & Server Certificates

Summary

Use this procedure if your company or agency does not have its own Certificate Authority and you do not want to use a commercial Certificate Authority to sign your server certificates.



Note

The public RSA key that is part of a certificate generated by the APC Security Wizard is 1024 bits. (The default key generated by the Environmental Monitoring Unit, if you do not use the Wizard, is 768 bits.)

- Create a CA root certificate that will be used to sign all server certificates to be used with Environmental Monitoring Units. During this task, two files are created.
 - The file with the **.p15** extension is an encrypted file which contains the Certificate Authority's private key and public root certificate. This file signs the server certificates.
 - The file with the **.crt** extension, which contains only the Certificate Authority's public root certificate. Load this file into each Web browser that will be used to access the Environmental Monitoring Unit so that the browser can validate the server certificate of the Environmental Monitoring Unit.
- Create a server certificate, which is stored in a file with a **.p15** extension. During this task, you are prompted for the CA root certificate that signs the server certificate.
- Load the server certificate onto the Environmental Monitoring Unit.
- For each Environmental Monitoring Unit that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the CA root certificate. Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC *Utility* CD that came with your Environmental Monitoring Unit.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled “Step 1,” select **CA Root Certificate** as the type of file to create.
4. Enter a name for the file that will contain the Certificate Authority’s public root certificate and private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. On the screen labeled “Step 2,” provide the information to configure the CA root certificate. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter an identifying name of your company or agency; use only alphanumeric characters, with no spaces.



Note

By default, a CA root certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate’s unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.



Note

The certificate's subject information and the certificate's issuer information should be identical.

7. The last screen verifies that the certificate has been created and instructs you on the next tasks.
 - This screen displays the location and name of the **.p15** file that you will use to sign the server certificates.
 - This screen also displays the location and name of the **.crt** file, which is the CA root certificate that you will load into the browser of each user who needs to access the Environmental Monitoring Unit.

Load the CA root certificate to your browser. Load the **.crt** file to the browser of each user who needs to access the Environmental Monitoring Unit.



See also See the help system of the browser for information on how to load the **.crt** file into the browser's certificate store (cache). Following is a summary of the procedure for Microsoft Internet Explorer.

1. Select **Tools**, then **Internet Options** from the menu bar.
2. On the **Content** tab in the **Internet Options** dialog box, click **Certificates** and then **Import**.
3. The Certificate Import Wizard will guide you through the rest of the procedure. The file type to select is X.509, and the CA Public Root Certificate is the **.crt** file created in the procedure [Create a Root Certificate & Server Certificates](#).

Create an SSL Server User Certificate. Perform these steps. (Click **Next** to move from screen to screen.)

1. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
2. On the screen labeled Step 1, select **SSL Server Certificate** as the type of file to create.
3. Enter a name for the file that will contain the server certificate and the private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
4. Click the **Browse** button, and select the CA root certificate created in the procedure **Create a Root Certificate & Server Certificates**. The CA Root Certificate is used to sign the Server User Certificate being generated.
5. On the screen labeled Step 2, provide the information to configure the server certificate. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter the IP address or DNS name of the server (Environmental Monitoring Unit). Because the configuration information is part of the signature, it cannot be exactly the same as the information you provided when creating the CA root certificate; the information you provide in some of the fields must be different.



Note

By default, a server certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.



Note

The information for every certificate must be unique. The configuration of a server certificate cannot be the same as the configuration of the CA root certificate. (The expiration date is not considered part of the unique configuration; some other configuration information must also differ.)

7. The last screen verifies that the certificate has been created and instructs you on the next task, to load the server certificate to the Environmental Monitoring Unit. It displays the location and name of the Server Certificate, which has a **.p15** file extension and contains the Environmental Monitoring Unit private key and public root certificate.

Load the server certificate to the Environmental Monitoring Unit.

Perform these steps:

1. On the **Network** menu of the Web interface of the Environmental Monitoring Unit, select the **Web/SSL** option.
2. In the **SSL/TLS Server Certificate** section of the page, browse to the server certificate, the **.p15** file you created in the procedure [Create a Root Certificate & Server Certificates](#). (The default is **C:\Program Files\American Power Conversion\APC Security Wizard.**)



Note

Alternatively, you can use FTP or SCP to transfer the server certificate to the Environmental Monitoring Unit. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Environmental Monitoring Unit. For SCP, the command to transfer a certificate named **cert.p15** to a Environmental Monitoring Unit with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\cert.p15
```

Create a Server Certificate and Signing Request

Summary

Use this procedure if your company or agency has its own Certificate Authority or if you plan to use a commercial Certificate Authority to sign your server certificates.

- Create a Certificate Signing Request (CSR). The CSR contains all the information for a server certificate except the digital signature. This process creates two output files:
 - The file with the **.p15** extension contains the Environmental Monitoring Unit's private key.
 - The file with the **.csr** extension contains the certificate signing request, which you send to an external Certificate Authority.
- When you receive the signed certificate from the Certificate Authority, import that certificate. Importing the certificate combines the **.p15** file containing the private key and the file containing the signed certificate from the external Certificate Authority. The output file is a new encrypted server certificate file with a **.p15** extension.
- Load the server certificate onto the Environmental Monitoring Unit.
- For each Environmental Monitoring Unit that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the Certificate Signing Request (CSR). Perform these steps.

(Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC *Utility* CD.

2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled “Step 1,” select **Certificate Request** as the type of file to create.
4. Enter a name for the file that will contain the Environmental Monitoring Unit’s private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. On the screen labeled Step 2, provide the information to configure the certificate signing request (CSR) with the information that you want the signed server certificate to contain. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter the IP Address or DNS name of the Environmental Monitoring Unit.



Note

By default, a server certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate’s unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.



Note

The certificate’s subject information and the certificate’s issuer information should be identical.

7. The last screen verifies that the certificate signing request has been created and displays the location and name of the file, which has a **.csr** extension.

8. Send the certificate signing request to an external Certificate Authority, either a commercial Certificate Authority or, if applicable, a Certificate Authority managed by your own company or agency.



See also

See the instructions provided by the Certificate Authority regarding the signing and issuing of server certificates.

Import the signed certificate. When the external Certificate Authority returns the signed certificate, perform these steps to import the certificate. This procedure combines the signed certificate and the private key into an SSL server certificate that you then upload to the Environmental Monitoring Unit. (Click **Next** to move from screen to screen.)

1. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
2. On the screen labeled Step 1, select **Import Signed Certificate**.
3. Browse to and select the signed server certificate that you received from the external Certificate Authority. The file has a **.cer** or **.crt** extension.
4. Browse to and select the file you created in step 4 of the task, **Create the CA root certificate**. This file has a **.p15** extension, contains the Environmental Monitoring Unit's private key, and, by default, is located in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. Specify a name for the output file that will be the signed server certificate that you upload to the Environmental Monitoring Unit. The file must have a **.p15** extension.
6. Click **Next** to generate the server certificate. The certificate's **Issuer Information** on the summary screen confirms that the external Certificate Authority signed the certificate.

7. The last screen verifies that the certificate has been created and instructs you on the next task, to load the server certificate to the Environmental Monitoring Unit. It displays the location and name of the server certificate, which has a **.p15** file extension and contains the Environmental Monitoring Unit's private key and the public key obtained from the **.cer** or **.crt** file.

Load the server certificate to the Environmental Monitoring Unit.

Perform these steps:

1. On the **Network** menu of the Web interface of the Environmental Monitoring Unit, select the **Web/SSL** option.
2. In the **SSL/TLS Server Certificate** section of the page, browse to the server certificate, the **.p15** file you created in the procedure **Import the signed certificate**. (The default location is **C:\Program Files\American Power Conversion\APC Security Wizard.**)



Note

Alternatively, you can use FTP or SCP to transfer the server certificate to the Environmental Monitoring Unit. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Environmental Monitoring Unit. For SCP, the command to transfer a certificate named **cert.p15** to a Environmental Monitoring Unit with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\cert.p15
```

Create an SSH Host Key

Summary

This procedure is optional. If you select SSH encryption, but do not create a host key, the Environmental Monitoring Unit generates a 768-bit RSA key when it reboots. Host keys for SSH that are created with the APC Security Wizard are 1024-bit RSA keys.

- Use the APC Security Wizard to create a host key, which is encrypted and stored in a file with **.p15** extension.
- Load the host key onto the Environmental Monitoring Unit.

The procedure

Create the host key. Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC *Utility* CD.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled Step 1, select **SSH Server Host Key** as the type of file to create.
4. Enter a name for the file that will contain the host key. The name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. Click **Next** to generate the Host Key.
6. The summary screen displays the SSH version 1 and version 2 fingerprints, which are unique for each host key and identify the host key. After you load the host key onto the Environmental Monitoring Unit, you can verify that the correct host key was uploaded by verifying

that the fingerprints displayed here match the SSH fingerprints on the Environmental Monitoring Unit, as displayed by your SSH client program.

7. The last screen verifies that the host key has been created and instructs you on the next task, to load the host key to the Environmental Monitoring Unit. It displays the location and name of the host key, which has a **.p15** file extension.

Load the host key to the Environmental Monitoring Unit. Perform these steps:

1. On the **Network** menu of the Web interface of the Environmental Monitoring Unit, select the **Telnet/SSH** option.
2. In the **SSH User Host Key File** section of the page, browse to the host key, the **.p15** file you created in the procedure **Create the host key**. (The default location is **C:\Program Files\American Power Conversion\APC Security Wizard.**)
3. On the **SSH Host Key Fingerprint** section of the page, note the fingerprint for the version (or versions) of SSH you are using. Then log on to the Environmental Monitoring Unit through your SSH client program, and verify that the correct host key was uploaded by verifying that these fingerprints match the fingerprints that the client program displays.



Note

Alternatively, you can use FTP or SCP to transfer the host key file to the Environmental Monitoring Unit. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Environmental Monitoring Unit. For SCP, the command to transfer a host key named **hostkey.p15** to a Environmental Monitoring Unit with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\hostkey.p15
```

APC Device IP Configuration Wizard

Purpose and Requirements

Purpose: configure basic TCP/IP settings

You can use the APC Device IP Configuration Wizard to configure the basic TCP/IP settings (IP address, subnet mask, and default gateway) of the following:

- Network Management Cards
- Devices that contain embedded Network Management Cards

Using the Wizard, you can configure the basic TCP/IP settings of installed or embedded Network Management Cards in either of the following ways:

- Automatically discover and configure unconfigured Network Management Cards remotely over your TCP/IP network.
- Configure or reconfigure a Network Management Card through a direct connection from the serial port of your computer to the device that contains the card.



Note

The Wizard can discover and configure Network Management Cards only if they are on the same network segment as the computer that is running the Wizard.

System requirements

The Wizard runs on Windows NT[®], Windows 2000, Windows 2003, and Windows XP Intel-based workstations.

Install the Wizard

Automated installation

If autorun is enabled on your CD-ROM drive, the installation program starts automatically when you insert the CD.

Manual installation

If autorun is not enabled on your CD-ROM drive, run **setup.exe** in the Wizard directory on the CD, and follow the on-screen instructions.

You can download the latest version of the APC Device IP Configuration Wizard from the APC Web site, www.apc.com and run **setup.exe** from the folder to which you downloaded it.

Use the Wizard

Launch the Wizard

The installation creates a shortcut link in the **Start** menu that you can use to launch the Wizard.

Configure the basic TCP/IP settings remotely

Prepare to configure the settings. Before you run the Wizard, be sure that you have the information you will need during the configuration procedure:

1. Contact your network administrator to obtain valid TCP/IP settings to use.
2. If you are configuring multiple unconfigured Network Management Cards, obtain the MAC address of each one so that you can identify each Network Management Card that the Wizard discovers. (The Wizard displays the MAC address for a discovered card on the same screen on which you then enter the TCP/IP settings.)
 - For Network Management Cards that you install, the MAC address is on a label on the bottom of the card.
 - For embedded Network Management Cards, the MAC address is on a label on the device containing the card — for example, usually on the side of a device that you mount in a rack.

You can also obtain the MAC address from the Quality Assurance slip that came with the Network Management Card or with the device containing an embedded Network Management Card.

Run the Wizard to perform the configuration. To discover and configure, over the network, installed or embedded Network Management Cards that are not configured:

1. From the **Start** menu, launch the Wizard. The Wizard automatically detects the first Network Management Card that is not configured.
2. Select **Remotely (over the network)**, and click **Next >**.
3. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the unconfigured Network Management Card identified by the MAC address at the top of the screen. Then click **Next >**.
4. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the device that contains the Network Management Card after you transmit the card's settings.
5. 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**.
6. The Wizard searches for another installed or embedded but unconfigured Network Management Card. If it finds one, it displays the screen with data entry boxes for the TCP/IP settings of that card.
 - To skip configuring the card whose MAC address is currently displayed, click **Cancel**.
 - To configure the TCP/IP settings of the next card, repeat this procedure beginning at step 4.

Configure or reconfigure the TCP/IP settings locally

To configure a single Network Management Card through a serial connection:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the serial configuration cable that came with the Network Management Card or with the device that contains an embedded Network Management Card.
 - a. Connect one end to an available communications port on your computer. Make sure no other application is using the port.
 - b. Connect the other end to the serial port of the card or device.
3. From the **Start** menu, launch the Wizard application.
 - If the Network Management Card is not configured, wait for the Wizard to detect it.
 - If you are assigning basic TCP/IP settings serially to a Network Management Card, click **Next>** to move to the next screen.
4. Select **Locally (through the serial port)**, and click **Next >**.
5. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the Network Management Card. Then click **Next >**.
6. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the device that contains the Network Management Card after you transmit the card's settings.
7. 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**.
8. 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.

How to Export Configuration Settings

Retrieving and Exporting the .ini file

Summary of the procedure

As an Administrator, you can retrieve a dynamically generated .ini file of an Environmental Monitoring Unit's current configuration and export that file to another Environmental Monitoring Unit or to multiple Environmental Monitoring Units.

1. Configure an Environmental Monitoring Unit to have the settings you want to export.
2. Retrieve the .ini file from that Environmental Monitoring Unit.
3. Customize the .ini file (to change at least the TCP/IP settings) and make a copy to export.
4. Use any of the file transfer protocols supported by the Environmental Monitoring Unit to transfer the copied file to one or more additional Environmental Monitoring Units. (To transfer the file to multiple Environmental Monitoring Units simultaneously, write an FTP script that repeats the steps for transferring the file to a single Environmental Monitoring Unit.)
5. Each receiving Environmental Monitoring Unit stores the file temporarily in its flash memory, uses it to reconfigure its own Environmental Monitoring Unit settings, and then deletes the file.

Contents of the .ini file

The config.ini file that you retrieve from an Environmental Monitoring Unit contains the following:

- *section headings*, which are category names enclosed in brackets ([]), and under each section heading, *keywords*, which are labels describing specific Environmental Monitoring Unit settings.



Note

Only section headings and keywords supported for the specific device (in this case, the Environmental Monitoring Unit) from which you retrieve the file are included.

- Each keyword is followed by an equals sign and the current *value* for that parameter's setting, either the default value (if the value has not been specifically configured) or the configured value.
- The `Override` keyword, with its default value, prevents one or more keywords and their device-specific values from being exported. In the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the Environmental Monitoring Unit) blocks the exporting of the values for the keywords `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.
- You must edit the section `[SystemDate/Time]` if you want to set the system date and time of a receiving Environmental Monitoring Unit or cause that Environmental Monitoring Unit to use an NTP Server to set its date and time.



See [Customizing](#) for configuration guidelines for date and time settings.

Detailed procedures

Use the following procedures to retrieve the settings of one Environmental Monitoring Unit and export them to one or more Environmental Monitoring Units.

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

1. Configure an Environmental Monitoring Unit with the settings you want to export.



Note

To avoid errors, configure the Environmental Monitoring Unit by using its Web interface or control console whenever possible. Directly editing the .ini file risks introducing errors.

2. Use FTP to retrieve the file config.ini from the Environmental Monitoring Unit you configured:
 - a. Open a connection to the Environmental Monitoring Unit, using its IP address. For example:

```
ftp> open 158.165.2.132
```

- b. Log on, using the Administrator user name and password configured for the Environmental Monitoring Unit.
- c. Retrieve the config.ini file containing the Environmental Monitoring Unit's current settings:

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

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



See also

To create batch files and use an APC utility to retrieve configuration settings from multiple Environmental Monitoring Units and export them to other Environmental Monitoring Units, see *Release Notes: ini File Utility, version 1.0* ([.\doc\en\ininotes.pdf](#)) on the APC *Utility* CD that came with your Environmental Monitoring Unit.

Customizing. You must customize the file to change at least the TCP/IP settings 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.
 - To define values, opening and closing quotation marks are optional, except to enclose values that contain leading or trailing spaces or values which are already enclosed in quotation marks. (Leading or trailing spaces not within the opening and closing quotation marks are ignored.)
 - To export a specific system date and time or any scheduled events, you must configure the values directly in the .ini file.
 - To export a specific system time, export only the configured `[SystemDate/Time]` section as a separate .ini file. (The time necessary to export a large file would cause the configured time to be significantly inaccurate.)
 - For greater accuracy, if the Environmental Monitoring Units receiving the file can access a Network Time Protocol (NTP) Server, set the value for the `NTPEnable` keyword as follows:

```
NTPEnable=enabled
```
 - Add comments about changes that you made. The first printable character of a comment line must be a semicolon (;).
2. Copy the customized file to another file name in the same folder:
 - The copy, which you will export to other Environmental Monitoring Units, can have any file name 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.** They are removed automatically from the file that you export.

Exporting the file to a single Environmental Monitoring Unit. To export the .ini file to another Environmental Monitoring Unit, use any of the file transfer protocols supported by Environmental Monitoring Units (including FTP, FTP Client, SCP, and TFTP). The following example uses FTP:

1. From the folder containing the customized .ini file and its copy, use FTP to log in to the Environmental Monitoring Unit to which you are exporting the .ini file. For example:

```
ftp> open 158.165.4.135
```

2. Export the copy of the customized .ini file. The receiving Environmental Monitoring Unit accepts any file name that has the .ini suffix, is no more than 64 characters in length, and is exported to its root directory.

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

Exporting the file to multiple Environmental Monitoring Units. To export the .ini file to multiple Environmental Monitoring Units:

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



See also

To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* ([.\doc\en\ininotes.pdf](#)) on the APC Utility CD.

The Upload Event and its Error Messages

The event and its error messages

The following system event occurs when the receiving Environmental Monitoring Unit completes using the .ini file to update its settings.

Configuration file upload complete, with *number* valid values

This event has no default severity level.

If a keyword, section name, or value is invalid, the event text is extended to include notification of the following errors.



Note

The export to and the subsequent upload by the receiving Environmental Monitoring Unit succeeds even if there are errors.

Event text	Description
Configuration file warning: Invalid keyword on line <i>number</i> . Configuration file warning: Invalid value on line <i>number</i> .	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line <i>number</i> .	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line <i>number</i> .	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, the Environmental Monitoring Unit stores and processes what it can, but ignores what it cannot. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in config.ini

A feature might not be supported for the device from which you retrieve the configuration settings or might not be supported for the device to which you export the configuration settings. In this case, the user configuration file contains, under the section name for that feature, a message stating that the feature is not supported. No keywords and values are listed, and that feature will not be configured on any device to which you export the user configuration file.

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.

The overridden values are device-specific and not appropriate to export to other Environmental Monitoring Units. Therefore, you can ignore these error messages. To prevent these error messages from occurring, 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.

Using the Device IP Configuration Wizard

On Windows operating systems, instead of using the preceding procedure for exporting .ini files, you can choose to update Environmental Monitoring Unit settings by using the Device IP Configuration Wizard.



For a detailed description of how to update the configuration settings of one or more Environmental Monitoring Units using the Device IP Configuration Wizard, see [APC Device IP Configuration Wizard](#).

File Transfers

Introduction

Overview

The Environmental Monitoring Unit automatically recognizes binary firmware files. Each of these files contains a header and one or more Cyclical Redundancy Checks (CRCs) to ensure that the data contained in the file is not corrupted before or during the transfer operation.

When new firmware is transmitted to the Environmental Monitoring Unit, the program code is updated and new features become available.

This chapter describes how to transfer firmware files to Environmental Monitoring Units.



To transfer a firmware file to a Environmental Monitoring Unit, see [Upgrading Firmware](#).



To verify a file transfer, see [Verifying Upgrades and Updates](#).

Upgrading Firmware

Benefits of upgrading firmware

Upgrading the firmware on the Environmental Monitoring Unit has the following benefits:

- New firmware has 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 Environmental Monitoring Units support the same features in the same manner.

Firmware files (Environmental Monitoring Unit)

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module.

The APC Operating System (AOS) and application module files used with the Environmental Monitoring Unit share the same basic format:

```
apc_hw0x_type_version.bin
```

- *apc*: Indicates that this is an APC file.
- *hw0x*: Identifies the version of the Environmental Monitoring Unit that will run this binary file.
- *type*: Identifies whether the file is for the APC Operating System (AOS) or the application module (APP) for the Environmental Monitoring Unit.
- *version*: The version number of the application file. For example, a code of 266 would indicate version 2.6.6.
- *bin*: Indicates that this is a binary file.

Obtain the latest firmware version

Automated upgrade tool for Microsoft Windows systems. An automated self-extracting executable tool combines the firmware modules that you need to automate your upgrades on any supported Windows operating system.

- The version of the tool on the APC *Utility* CD that came with your Environmental Monitoring Unit will upgrade your device to the latest AOS and application modules available when the CD was released.
- If a later firmware upgrade is available, you can obtain an updated version of the tool at no cost from the support section of the APC Web site www.apc.com/tools/download. At this Web page, find the latest firmware release for your APC product (in this case, your Environmental Monitoring Unit) and download the automated tool, not the individual firmware modules.

If the AOS firmware module you already have is a 1.x.x version, the executable tool must perform two consecutive upgrades:

- The first upgrade is from version 1.x.x to the latest available 2.0.x version of the AOS firmware module.
- The second upgrade is from the 2.0.x version to the most recently released version of the AOS module.

The tool therefore contains firmware modules for both upgrades.

Each upgrade tool is specific to an APC product type. Do not use the tool from one product CD to upgrade firmware of a different APC product. If you use a version of the tool from the APC Web site, make sure that you use the upgrade tool that corresponds with your APC product type.

Manual upgrades, primarily for Linux systems. If all computers on your network are running Linux, you must upgrade the firmware of your Environmental Monitoring Units manually, i.e., by using the separate APC firmware modules (AOS module and application module).



If you have a networked computer running a supported Microsoft Windows operating system on your network, you can use the tool described in [Automated upgrade tool for Microsoft Windows systems](#) to upgrade the firmware of a Environmental Monitoring Unit automatically over the network. This tool automates the entire upgrade process, even if your current firmware is a 1.x.x version.



Note

When performing a manual upgrade, not using the automated tool, you cannot upgrade the AOS firmware module of any APC device directly from firmware version 1.x.x to firmware version 2.1.0 or later. The upgrade attempt will fail. You must first upgrade to the latest available 2.0.x version of the AOS module and then to the later version.

You can obtain the individual firmware modules you need for a manual firmware upgrade from the support section of the APC Web site www.apc.com/tools/download.

Firmware file transfer methods

To upgrade the firmware of an Environmental Monitoring Unit:

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



Note

When you transfer individual firmware modules and do not use the automated firmware upgrade tool to upgrade the firmware for a Environmental Monitoring Unit, you must transfer the APC Operating System (AOS) module to the Environmental Monitoring Unit before you transfer the application module.



For more information about the firmware modules, see [Firmware files \(Environmental Monitoring Unit\)](#).

Use FTP or SCP to upgrade one Environmental Monitoring Unit

Instructions for using FTP. For you to be able to use FTP to upgrade a single Environmental Monitoring Unit over the network.

- The Environmental Monitoring Unit must be connected to the network.
- The FTP server must be enabled at the Environmental Monitoring Unit.
- The Environmental Monitoring Unit must have its TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway** addresses) configured.

To use FTP to upgrade the Environmental Monitoring Unit:

1. Open an MS-DOS command prompt window on a computer that is connected to the network. Go to the directory that contains the firmware upgrade files, and list the files. For the directory `C:\apc`, the commands would be those shown in **bold**:

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

Files listed for an Environmental Monitoring Unit, for example, might be the following:

- `apc_hw02_aos_264.bin`
- `apc_hw02_app_266.bin`

2. Open an FTP client session:

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

3. Type `open` and the Environmental Monitoring Unit's IP address, and press ENTER. If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default of **21**, you must use the non-default value in the FTP command.
 - a. For some FTP clients, use a colon to add the port number to the end of the IP address.

- b. For Windows FTP clients, separate the port number from the IP address by a space. For example, if the Environmental Monitoring Unit's **FTP Server Port** setting has been changed from its default of **21**, such as to **21000**, you would use the following command for a Windows FTP client transferring a file to an Environmental Monitoring Unit with an IP address of 150.250.6.10.

```
ftp> open 150.250.6.10 21000
```

4. Log on using the Administrator user name and password (**apc** is the default for both).
5. Upgrade the AOS. For example:

```
ftp> bin  
ftp> put apc_hw02_aos_264.bin
```
6. When FTP confirms the transfer, type `quit` to close the session.
7. Wait 20 seconds, and then repeat **step 2** through **step 5**, but in **step 5**, use the application module file name instead of the AOS module.

Instructions for using SCP. To use SCP to upgrade the firmware for one Environmental Monitoring Unit:

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 Environmental Monitoring Unit. The following example assumes a Environmental Monitoring Unit IP address of 158.205.6.185, and an AOS module of **apc_hw02_aos_264.bin**.)

```
scp apc_hw02_aos_264.bin apc@158.205.6.185:apc_hw02_aos_264.bin
```

3. Use a similar SCP command line, with the name of the application module instead of the AOS module, to transfer the application module to the Environmental Monitoring Unit.

How to upgrade multiple Environmental Monitoring Units

Export configuration settings. You can create batch files and use an APC utility to retrieve configuration settings from multiple Environmental Monitoring Units and export them to other Environmental Monitoring Units.



See *Release Notes: ini File Utility, version 1.0* ([.\doc\en\ininotes.pdf](#)) on the APC *Utility* CD that came with your Environmental Monitoring Unit.

Use FTP or SCP to upgrade multiple Environmental Monitoring Units.

To upgrade multiple Environmental Monitoring Units using an FTP client or using SCP, write a script which automatically performs the procedure. For FTP, use the steps in [Use FTP or SCP to upgrade one Environmental Monitoring Unit](#).

Use XMODEM to upgrade one Environmental Monitoring Unit



Note

You cannot upgrade the AOS firmware module of any APC device directly from firmware version 1.x.x to 2.1.0 or later. The upgrade attempt will fail.

To upgrade the AOS firmware module of an APC device from version 1.x.x to 2.1.0 or later, first upgrade the module to the latest available version 2.0.x AOS firmware module. Then upgrade it again, this time from version 2.0.x to the 2.x.x version you want.

If your APC device is running a 2.0.x of the AOS firmware module already, you can upgrade directly to version 2.1.0 or a later version.

To use XMODEM to upgrade the firmware for a single Environmental Monitoring Unit that is not on the network:

1. Obtain the individual firmware modules (the AOS module and the application module) from the support section of the APC Web site www.apc.com/tools/download.
2. Select a serial port at the local computer, disable any service which uses that port, and connect the smart-signaling cable that came with the Environmental Monitoring Unit to the selected port and to the serial port at the Environmental Monitoring Unit.
3. Run a terminal program (such as HyperTerminal), and configure the selected port for 9600 bps (or 19200 bps, if you are using Modbus configured at that rate), 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.



Note

Modbus runs at 9600 or 19200 bps. To use the Control Console when Modbus is enabled, your computer's serial port must communicate at the same serial protocol rate as Modbus.

4. Press ENTER to display the **User Name** prompt.
5. Enter your Administrator user name and password. The default for both is **apc**.
6. Start an XMODEM transfer:
 - a. Select option 3—**System**
 - b. Select option 4—**File Transfer**
 - c. Select option 2—**XMODEM**
 - d. Type `Yes` at the prompt to continue with the transfer.
7. Select the appropriate baud rate. A higher baud rate causes faster firmware upgrades. Also, change the terminal program's baud rate to match the one you selected, and press ENTER.
8. From the terminal program's menu, select the binary AOS file to transfer via XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600. The Environmental Monitoring Unit will automatically restart.
9. Repeat step 3 through step 8 to install the application module. In step 8, substitute the application module file name for the AOS module file name.



For information about the format used for application modules, see [Firmware files \(Environmental Monitoring Unit\)](#).

Verifying Upgrades and Updates

Overview

To verify that the firmware upgrade was successful, see the **Last Transfer Result** message, available through the **FTP Server** option of the **Network** menu (in the control console only), or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last transfer result codes

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

You can also verify the versions of the upgraded APC Operating System (AOS) and application modules by using the **About System** option in the **System** menu of the control console or in the **Help** menu of the Web interface, or by using an SNMP GET to the MIB II **sysDescr** OID.

Product Information

Warranty and Service

Limited warranty

APC warrants the Environmental Monitoring Unit to be free from defects in materials and workmanship for a period of two years from the date of purchase. Its obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. 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. This warranty applies only to the original purchaser.

Obtaining service

To obtain support for problems with your Environmental Monitoring Unit:

1. Note the serial number and date of purchase. The serial number is printed on a label on the bottom of the Environmental Monitoring Unit
2. Contact Customer Support at a phone number located at the end of this manual. A technician will try to help you solve the problem by phone.
3. If you must return the product, the technician will give you a return material authorization (RMA) number. If the warranty expired, you will be charged for repair or replacement.
4. Pack the unit carefully. The warranty does not cover damage sustained in transit. Enclose a letter with your name, address, RMA number and daytime phone number; a copy of the sales receipt; and a check as payment, if applicable.
5. Mark the RMA number clearly on the outside of the shipping carton.
6. Ship by insured, prepaid carrier to the address provided by the Customer Support technician.

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 American Power Conversion 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 System 27
- Access
 - Access Type setting for SNMP 89
 - FTP Server 80
 - limiting NMS SNMP access by IP address 89
- Access setting for RADIUS 104
- Actions 61
- Advanced settings (DHCP) 115
- Alarm maps 41
- A-Link devices
 - ARUs 42
 - remote environmental probes 38
- APC cookie 117
- APC OS 27
- Apply local computer time 106
- Authentication
 - SNMP traps 64
 - with SSL 128
- Authentication traps setting 64
- Auto logout 102

B

- Boot mode 112
- BOOTP
 - After IP Assignment setting 115
 - DHCP & BOOTP boot process 113
 - Remain in DHCP & BOOTP Mode setting 115
 - Status LED indicating BOOTP requests 12

Browsers

- CA certificates in browser's store (cache) 128
- supported versions 18

C

Certificates

- choosing which method to use 130
- creating and installing for SSL 130
- deleting 108
- methods
 - use the APC default certificate 131

CipherSuite

- choosing SSL encryption ciphers and hash algorithms 96
- purpose of the algorithms and ciphers 129

Client ID setting (DHCP) 115

Community name

- for SNMP access control 89
- for trap receivers 64

config.ini file, contents 159

Configuring proxy server before using Web interface 18

Control console

- device manager menu 36
- navigating menus 35
- refreshing menus 35

Cookie

- APC 117

Current Settings fields (TCP/IP) 75

Customizing user configuration files 161

D

- Data log
 - configuration 72
 - log interval 72
- Data Menu (Web Interface Only) 71
- Delete SSH Host Keys and SSL Certificates 108
- Device IP configuration wizard 153
 - installing 154
 - using 155
 - using to update configuration settings 165
- Device manager menu
 - control console 36
- DHCP
 - After IP Assignment setting 115
 - APC cookie 117
 - Cookie Is setting 115, 116
 - DHCP & BOOTP boot process 113
 - embedded management card settings 114
 - Remain in DHCP & BOOTP Mode setting 115
 - require vendor specific cookie to accept DHCP address setting 115
 - response options 117
 - Retry Then Stop setting 116
- Disabling
 - e-mail to a recipient 68
 - event logging 62
 - reverse DNS lookup 80
 - sending any traps to an NMS 64
 - sending authentication traps to an NMS 64
 - use of a proxy server 18
- Domain Name setting (DHCP) 115
- Domain names
 - configuring 77
 - of trap receivers 64

- overriding expansion of host name to domain name 77

E

- E-mail
 - configuring 65
 - enabled by default for severe events 63
 - enabling and disabling 68
 - message format (long or short) 69
 - setting up an account 68
 - using for paging 67
- Email
 - Events menu option 63
- Email recipients 67
 - format 69
- Enabling
 - e-mail forwarding to external SMTP servers 68
 - e-mail to a recipient 68
 - reverse DNS lookup 80
 - sending any traps to an NMS 64
 - sending authentication traps to an NMS 64
- Encryption
 - with SSH and SCP 126
 - with SSL 93
- Environmental probes
 - local 38
 - remote 38
- Error messages 19
 - for firmware file transfer 176
 - from overridden values during .ini file transfer 164
- Event log
 - accessing 35
 - disabling 62
 - errors from overridden values during .ini file transfer 164
 - using FTP del command 60
- Event maps 41

- event.txt file
 - contents 58
 - importing into spreadsheet 58
- Events menu
 - Actions 61
 - e-mail (Web interface) 63
 - Event log 62
 - SNMP Traps 63

F

- Facility setting 90
- Firewall, as essential to security 137
- Firmware
 - benefits of upgrading 167
 - file transfer methods 170
 - FTP or SCP 171
 - XMODEM 174
 - files for Environmental Monitoring Unit 167
 - obtaining the latest version 168
 - upgrading 167
 - verifying upgrades and updates 176
 - versions displayed on main screen 33
- Firmware files (Environmental Monitoring Unit) 167
- From address 66
- FTP
 - disabling when SCP is used 80
 - to retrieve text version of event log 58

G

- Generation (e-mail recipients) 68
- GMT offset (time zone) 107

H

- Help
 - About System option (Web

- interface) 27
- in control console 35
- Host keys
 - creating 151
 - deleting 108
 - file name 87
 - file status 87
 - fingerprints
 - displaying for versions 1 and 2 88
 - generated by the Environmental Monitoring Unit 83
 - transferring to the Environmental Monitoring Unit 83
 - transferring to the management card 87

Host Name

- configuring 77
- setting (DHCP) 115
- HTTP port 95
- HTTP protocol mode 94
- HTTPS port 95
- HTTPS protocol mode 94
- Humidity sensors, optional 13
- Hyperlinks, defining 110

I

- Identification fields on main screen 33
- ini files, See User configuration files
- Input contacts 43
- IP addresses
 - of DNS server for e-mail 65
 - of trap receivers 64
 - to limit access to specified NMSs 89

K

- keywords, user configuration file 159

L

- Life support policy 178
- Links
 - redirecting user-definable links 28, 110
- Local SMTP server 68
- Lock icon indicating SSL is enabled 94
- Logging on
 - DNS Name or IP address matched to common name 17
 - error messages for Web interface 19
 - Web interface 17
- Login date and time
 - control console 33
 - Web interface 22

M

- Main screen
 - displaying identification 33
 - firmware values displayed 33
 - login date and time 33
 - status 34
 - Up Time 33
 - User access identification 33
- Manual option to set date and time 106
- Mapping events to alarms 41
- Menus
 - control console 36
 - Data 71
 - Events 25
 - Help 26
 - Links 110
 - Network 26
 - System 26
- Modbus 51
 - serial port 6, 31

N

- Network menu
 - FTP 80
 - FTP server 80
 - Telnet/SSH 82
- Network time protocol (NTP) 106
- NMS IP/Domain Name setting 89
- NTP 106

O

- OS, APC 27
- Output relays 44
- Override keyword, in user configuration file 159

P

- Paging by using e-mail 67
- Passwords
 - default for Administrator account 17
 - default for Device Manager account 17
 - for NMS that is a trap receiver 64
 - user manager access 102
 - using non-standards ports as extra passwords 124
- Port Speed setting (DHCP) 115
- Ports
 - assigning 124
 - default
 - for FTP server 80
 - for HTTP 95
 - for HTTPS 95
 - for SSH 85
 - for Telnet 85
 - using a non-default port
 - for FTP 80
 - for HTTP 95
 - for HTTPS 95
 - for SSH 85
 - for Telnet 85

- Primary NTP server 107
- Primary Server Secret setting for RADIUS 104
- Primary Server setting for RADIUS 104
- Protocol mode
 - selecting for control console access 84
 - selecting for Web access 94
- Proxy servers
 - configuring not to proxy the Environmental Management System 18
 - disabling use of 18

R

- Rack air removal units (ARUs) 42
- RADIUS settings 103, 104
- Read access by an NMS 89
- Reboot 108
 - preventing reboot for inactivity 15
 - Reboot Management Interface 108
- Receiver NMS IP/Domain Name, for trap receivers 64
- Recipient's SMTP server 68
- Reset Only TCP/IP to Defaults 108
- Reset to Defaults 108
- Reset to Defaults Except TCP/IP 108
- Retry Then Stop setting (DHCP) 116
- Reverse DNS lookup 80
- Root certificates, creating 142

S

- SCP
 - enabled and configured with SSH 82, 127
- Secondary NTP server 107
- Secondary Server Secret setting for RADIUS 104

- Secondary Server setting for RADIUS 104
- Section headings, user configuration file 159
- Secure CoPy. See SCP.
- Secure hash algorithm (SHA) 96
- Secure SHell. See SSH.
- Security
 - authentication
 - authentication vs. encryption through digital certificates with SSL 125
 - certificate-signing requests 129
 - disabling less secure interfaces 127
 - encryption with SSH and SCP 126
 - how certificates are used 138
 - how SSH host keys are used 139
 - planning and implementing 125
 - SCP as alternative to FTP 127
 - SSL
 - choosing a method to use certificates 130
 - CipherSuite algorithms and ciphers 129
 - supported SSH clients 82
 - using non-standards ports as extra passwords 124
- Security wizard 138
 - creating certificates without a certificate authority 142
 - creating SSH host keys 151
- Send DNS query 79
- Sensors
 - environmental probes 38
 - humidity, optional 13
 - temperature, optional 13
- Server certificates
 - creating without a certificate authority 142

- Set manually (date and time) 106
 - Severity levels of events 62
 - events with no severity level 62
 - SMTP
 - from address 66
 - server 66, 68
 - SNMP
 - Access Type setting 89
 - authentication traps 64
 - Community Name setting 89
 - NMS IP/Domain Name setting 89
 - SNMP Traps option 63
 - SSH
 - enabling 82, 84
 - encryption 126
 - host key
 - as identifier that cannot be falsified 126
 - creating 151
 - file name 87
 - file status 87
 - transferring to the Environmental Monitoring Unit 83
 - modifying the port setting 85, 95
 - obtaining an SSH client 82
 - server configuration 86
 - v1 encryption algorithms 86
 - v2 encryption algorithms 86
 - SSL
 - authentication through digital certificates 128
 - certificate signing requests 129
 - encryption ciphers and hash algorithms 96
 - Status
 - on control console main screen 34
 - Synchronize with NTP server, (date & time) 106
 - Syslog
 - facility setting 90
 - System
 - information, obtaining 27
 - System menu
 - About System option (control console) 27
 - RADIUS
 - settings 104
 - Tools 108
 - User Manager 102
- ## T
- TCP/IP 115
 - restoring default settings 108
 - setting port assignments for extra security 124
 - Telnet
 - enabling 84
 - Telnet/SSH
 - access option 84
 - host key fingerprints, displaying 88
 - modifying the port settings 85
 - option in Network menu 82
 - selecting the protocol mode 84
 - SSH host key file name 87
 - SSH host key file status 87
 - SSH Port option 85
 - SSHv1 encryption algorithms 86
 - SSHv2 encryption algorithms 86
 - Telnet Port option 85
 - Temperature sensors, optional 13
 - Testing the network connection to the DNS server 79
 - Timeout setting for RADIUS 104
 - To address 67
 - Tools menu 108
 - File Transfer 109
 - Transport layer security (TLS) 128
 - Trap generation 64
 - Troubleshooting
 - problems logging on to
 - Web interface 17
 - proxy server problems 18

U

- Up time
 - control console main screen 33
 - Web interface 22
- Update Interval, Date & Time setting 107
- Upgrading firmware
 - without using a utility 167
- URL address formats 19
- User access identification, control console rinterface 33
- User Class setting (DHCP) 115
- User configuration files
 - contents 159
 - customizing 161
 - exporting system time separately 161
 - messages for undiscovered devices 164
 - overriding device-specific values 159
 - system event and error messages 163
 - using the APC utility to retrieve and transfer the files 160, 173
- User manager 102
 - auto logout 102
 - password 102
 - user name 102
- User name
 - default for Administrator account 17
 - default for Device Manager account 17
 - user manager access 102

V

- Vendor Class setting (DHCP) 115
- Vendor specific information
 - cookies 117

W

- Web interface
 - enable or disable protocols 94
 - logging on 17
 - logon error messages 19
 - Modifying the port setting
 - for FTP 81
 - for HTTP 95
 - for HTTPS 95
 - for SSH 85
 - for Telnet 85
 - up time 22
 - URL address formats 19
- Web/SSL 93
- Web/SSL/TLS 93

X

- XMODEM 109

APC Worldwide Customer Support

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

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

Direct InfraStruXure Customer Support Line	(1)(877)537-0607 (toll free)
APC headquarters U.S., Canada	(1)(800)800-4272 (toll free)
Latin America	(1)(401)789-5735 (USA)
Europe, Middle East, Africa	(353)(91)702000 (Ireland)
Japan	(0) 35434-2021
Australia, New Zealand, South Pacific area	(61) (2) 9955 9366 (Australia)

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

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

Copyright

Entire contents © 2005 American Power Conversion. All rights reserved. Reproduction in whole or in part without permission is prohibited. APC, the APC logo, PowerNet, and InfraStruXure are trademarks of American Power Conversion Corporation and may be registered in some jurisdictions. All other trademarks, product names, and corporate names are the property of their respective owners and are used for informational purposes only.

990-0815D

1/2005

