Contents

Introduction

Product Description

Features

The Embedded Network Module is a Web-based management product that uses multiple, open standards such as Telnet, HTTP, HTTPS, Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure CoPy (SCP), and Simple Network Management Protocol (SNMP) to provide full management of supported devices.

The following is a list of some of the Embedded Network Module features:

- Provides the ability to export a user configuration (.ini) file from a configured Embedded Network Module to one or more unconfigured Embedded Network Modules without converting the file to a binary file.
- Generates system log (Syslog) messages.
- Enables the use of a Dynamic Host Configuration Protocol (DHCP) server to provide the network (TCP/IP) values of the Embedded Network Module.
- Provides data and event logs.
- Provides uninterruptible power supply scheduling features.
- Provides support for the PowerChute® Network Shutdown utility.
- Limits SNMP traps and e-mail notifications based on the severity level of the uninterruptible power supply or system events.
- Provides a selection of security protocols for authentication and encryption.

Initial setup

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

- IP address of the Embedded Network Module.
- Subnet mask.
- IP address of the default gateway.

Attention! Do not use the loopback address (127.0.0.1) as the default gateway address for the Embedded Network Module. Doing so will disable the Embedded Network Module and will require you to reset TCP/IP settings to their defaults using a local serial login.

For instructions about how to configure the TCP/IP settings, see the *Uninterruptible Power Supply Quick Installation Guide*, provided in printed form and on the documentation CD as a PDF file.

To use a DHCP server to configure the TCP/IP settings of the Embedded Network Module, see **"Boot Mode" on page 129**.

Network management features

Following are some of the network management applications and utilities that can work with an IBM uninterruptible power supply that connects to the network through the Embedded Network Module:

- Network management applications:
  - PowerChute Network Shutdown provides unattended remote graceful shutdown of computers that are connected to uninterruptible power supplies.

- InfraStruXure® Manager provides enterprise-level power management and device management for uninterruptible power supplies.
- PowerChute Business Edition provides safe system shutdown and uninterruptible power supply management for workstations and servers operating in a small or medium business environment.

- Wizard utilities:
  - The Device IP Configuration Wizard discovers unconfigured Embedded Network Modules and enables you to configure their basic TCP/IP settings over the network.
  - The Security Wizard creates components needed for high security for the Embedded Network Module on the network when you are using Secure Sockets Layer (SSL) and related protocols and encryption routines.
- A Management Information Base (MIB) browser uses the Object Identifiers (OIDs) of a MIB to perform SNMP SETs and GETs on an uninterruptible power supply.

Internal Management Features

Overview

The Embedded Network Module has two internal interfaces (control console and Web interface), which provide menus with options that enable you to manage the uninterruptible power supply and the Embedded Network Module. The Embedded Network Module's SNMP interface also enables you to use an SNMP browser with the PowerNet® Management Information Base (MIB) to manage the uninterruptible power supply.

For more information about the internal user interfaces of the Embedded Network Module, see **"Control Console" on page 9** and **"Web Interface" on page 20**.

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

Access priority for logging on

Only one user at a time can log on to the Embedded Network Module 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 Embedded Network Module 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 has the lowest priority.

For information about how SNMP access to the Embedded Network Module is controlled, see **"SNMP" on page 47**.

Types of user accounts

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

- An Administrator can use all of the management menus available in the control console and the Web interface. The Administrator's default user name and password are both **apc**.
- A Device Manager can use only the uninterruptible power supply menu and the **Log** option in the **Events** menu. The Device Manager's default user name is **device**, and the default password is **apc**.
- A Read-Only User has the following restricted access:
  - Access through the Web interface only.
  - Access to the same 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.

  The Read-Only User's default user name is **readonly**, and the default password is **apc**.

To set the user name and password for the three account types, see **"User Manager" on page 61**.

Note

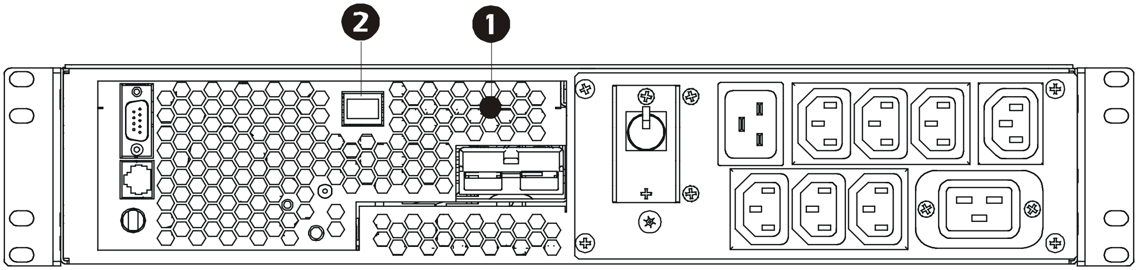
You must use the Web interface to configure values for the Read-Only User.

Rear Panel

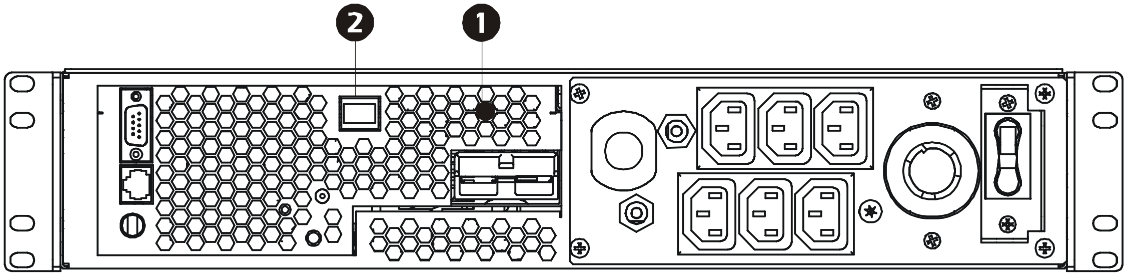
Introduction

The rear-panel features of the uninterruptible power supplies that support the Embedded Network Module are the Reset button, 10/100 Base-T Connector, and LEDs.

IBM UPS 3000XHV



IBM UPS 3000XLV



Features

❶ **Reset Button:** Resets the Embedded Network Module while power remains on.

❷ **10/100 Base-T Connector:** Connects the uninterruptible power supply to the Ethernet network.
Link RX/TX (10/100) LED: At the upper right on the connector. See **"Link-RX/TX (10/100) LED" on page 7**.
Status LED: At the upper left on the connector. See **"Status LED" on page 7**.

Link-RX/TX (10/100) LED

This LED indicates the network status.

Condition	Description
Off	Either the Embedded Network Module is receiving no network traffic, or the device that connects the Embedded Network Module to the network is turned off or not operating correctly.
Flashing **Green**	The Embedded Network Module is receiving data packets from the network at 10 Megabits per second (Mbps).
Flashing **Orange**	The Embedded Network Module is receiving data packets from the network at 100 Megabits per second (Mbps).

Status LED

This LED indicates the status of the Embedded Network Module.

Condition	Description
Off	The Embedded Network Module has no power.
Solid **Green**	The Embedded Network Module has valid TCP/IP settings.
Flashing **Green**	The Embedded Network Module does not have valid TCP/IP settings.[1]
Solid **Orange**	A hardware failure has been detected in the Embedded Network Module. Contact IBM Customer Support.
Flashing **Orange**	The Embedded Network Module is making BOOTP requests.
Flashing **Orange** and **Green**	The Embedded Network Module is making DHCP[2] requests.

[1] If you do not use a BOOTP server, see the uninterruptible power supply *Quick Installation Manual* provided in printed format and in PDF on the documentation CD to configure the TCP/IP settings of the Embedded Network Module.

[2] To use a DHCP server, see **"Boot Mode" on page 129**.

Watchdog Features

Overview

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

Network interface watchdog mechanism

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

Resetting the network timer

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

Control Console

How To Log On

Overview

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection with a computer on the same subnet as the Embedded Network Module to access the control console.

Use case-sensitive user name and password entries to log on (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device Manager). 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" on page 12**.

Remote access to the control console

You can access the control console through Telnet or Secure SHell (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 Embedded Network Module (when the Embedded Network Module uses the default Telnet port of 23), and press Enter. For example:

   ```
   telnet 139.225.6.133
   ```

   Note If the Embedded Network Module uses a non-default port number (between 5000 and 32767), 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 Secure SHell (SSH) for access to the control console. SSH encrypts user names, passwords and transmitted data.

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

Local access to the control console

You can use a local computer that connects to the Embedded Network Module through the serial port at the uninterruptible power supply containing the Embedded Network Module 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 smart-signaling cable that came with the uninterruptible power supply to the selected port and to the serial port of the uninterruptible power supply.
3. Run a terminal program (such as HyperTerminal), and configure the selected port for 2400 bps, 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.
4. Press Enter to display the **User Name** prompt.
5. Enter your user name and password.

How to Recover from a Lost Password

You can use a local computer that connects to the Embedded Network Module through the serial port at the uninterruptible power supply 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 smart-signaling cable that came with the uninterruptible power supply to the selected port and to the serial port of the uninterruptible power supply.
3. Run a terminal program (such as HyperTerminal) and configure the selected port as follows:
   – 2400 bps
   – 8 data bits
   – no parity
   – 1 stop bit
   – no flow control
4. Press Enter, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   – The serial port is not in use by another application.
   – The terminal settings are correct as specified in step 3.
   – The correct cable is being used as specified in step 2.
5. Immediately press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time while the LED is flashing to reset the user name and password to the 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.

Main Screen

Example main screen

The following is an example of the screen that appears when you log on to the control console at the Embedded Network Module.

```
American Power Conversion               Network Management Card AOS    v2.5.3
<c> Copyright 2004 All Rights Reserved  Smart-UPS & Matrix-UPS APP     v2.5.4
-------------------------------------------------------------------------------
Name      : Test Lab                                   Date : 02/15/2005
Contact   : Don Adams                                  Time : 05:58:30
Location  : Building 3                                 User : Administrator
Up Time   : 0 Days, 21 Hours, 21 Minutes               Stat : P+ N+ A+

IBM UPS 3000XLV named Tester 8  : On Line, No Alarms Present
Group 1: On   Group 2: On   Group 3: On

------- 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 operating system (AOS) and application (APP) firmware versions.

```
Embedded Network Module AOS   v2.5.3
APP                           v2.5.4
```

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

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

For information about how to set the **Name**, **Contact**, and **Location** values, see **"Identification" on page 62**.

- An **Up Time** field reports how long the Embedded Network Module has been running since it was last turned on or reset.

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

- Two fields identify when you logged in, by **Date** and **Time**.

```
Date : 02/15/2005
Time : 5:58:20
```

- A **User** field identifies whether you logged in 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 Embedded Network Module status.

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

`P+`	The operating system (AOS) is functioning properly.
`N+`	The network is functioning properly.
`N?`	A BOOTP request cycle is in progress.
`N–`	The Embedded Network Module failed to connect to the network.
`N!`	Another device is using the IP address of the Embedded Network Module.
`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

The AOS should always report that it is functioning properly (`P+`). If the AOS is not functioning properly, and you cannot access the Embedded Network Module, contact IBM® Customer Support.

- A **UPS model and name** field reports the status of the uninterruptible power supply.

```
IBM UPS 3000XHV named Tester 8 : On Line, No Alarms
Present
```

For more information about the status of the uninterruptible power supply, see **"Uninterruptible Power Supply Status" on page 69**.

Control Console Menus

Overview

The control console provides options to manage the Embedded Network Module and its uninterruptible power supply.

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 can access only the **Device Manager** menus and the **Logout** menu.

Menu structure

The menus in the control console list options by number and name. To use an option, type the number of the option and press Enter, then follow any on-screen instructions.

Options that enable you to change a setting have an **Accept Changes** option that you must use before you exit a menu 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" on page 106**.

Device Manager option

This option accesses the **Device Manager** menu. The options on this menu enable you to select the device that you want to manage.

```
1- IBM UPS 3000XHV
```

For information about the menu options that are available for managing an uninterruptible power supply, see **"Uninterruptible Power Supply Menu" on page 68**.

Network option

To do any of the following tasks, see **"Network Menu" on page 31**:

- Configure the TCP/IP settings of the Embedded Network Module, or, if the Embedded Network Module will obtain its TCP/IP settings from a server, configure the settings for the type of server (DHCP or BOOTP) to be used.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet, Web interface and SSL, SNMP, e-mail, DNS, Syslog, and WAP (Wireless Application Protocol) features of the Embedded Network Module.

System option

To do any of the following tasks, see **"System Menu" on page 59**:

- Control Administrator and Device Manager access. (You can control Read-Only User access by using the Web interface only.)
- Define system values for the **Name**, **Contact**, and **Location** fields.
- Set the date and time used by the Embedded Network Module.
- Through the **Tools** menu:
  - Restart the Embedded Network Module.
  - Reset parameters to their default values.
  - Delete SSH host keys and SSL certificates.
- Access system information about the Embedded Network Module.

Web Interface

Introduction

Overview

The Web interface provides options that you use to manage the Embedded Network Module and its uninterruptible power supply.

📖 See **"Web/SSL" on page 52** for information on the menu options you can use to select, enable, and disable the protocols that control access to the Web interface and to define the Web-server ports for the protocols.

Supported Web Browsers

You can use Microsoft® Internet Explorer (IE) 5.0 (or later) or Netscape 4.0.8 (or later, except Netscape 6.*x*) to access the Embedded Network Module through its Web interface. Other commonly available browsers also might work but have not been fully tested.

Data verification, the event log, the data log, and Message Digest 5 (MD5) authentication require that you enable the following for your Web browser:

- JavaScript
- Java
- Cookies

In addition, the Embedded Network Module 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 Embedded Network Module.
- Configure the proxy server so that it does not proxy the specific IP address of the Embedded Network Module.

How to Log On

Overview

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

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

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

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 Security Wizard:

- You must use an IP address to log on to the Embedded Network Module if an IP address was specified as the common name in the certificate.
- 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 is displayed when you log on to the Web interface, see **"Summary Page" on page 24**.

URL address formats

Type the DNS name or IP address of the Embedded Network Module in the URL address field of the Web browser, and press Enter. Except when you specify a non-default Web server port in Internet Explorer, http:// or https:// is automatically added by the browser.

Note

If the error message `You are not authorized to view this page` is displayed (Internet Explorer only), another user is logged onto the Web interface or control console. If the error message `No Response` (Netscape) or `This page cannot be displayed` (Internet Explorer) is displayed, Web access might be disabled, or the Embedded Network Module might 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 139.225.6.133, when the Embedded Network Module uses the default port (80) at the Web server, the entry would be one of the following:
  - `http://139.225.6.133` if HTTP is your access mode.
  - `https://139.225.6.133` if HTTPS (SSL/TLS) is your access mode.
- For a System IP address of 139.225.6.133, when the Embedded Network Module uses a non-default port (5000, in this example) at the Web server, the entry would be one of the following:
  - `http://139.225.6.133:5000` if HTTP is your access mode.
  - `https://139.225.6.133:5000` if HTTPS (SSL/TLS) is your access mode.

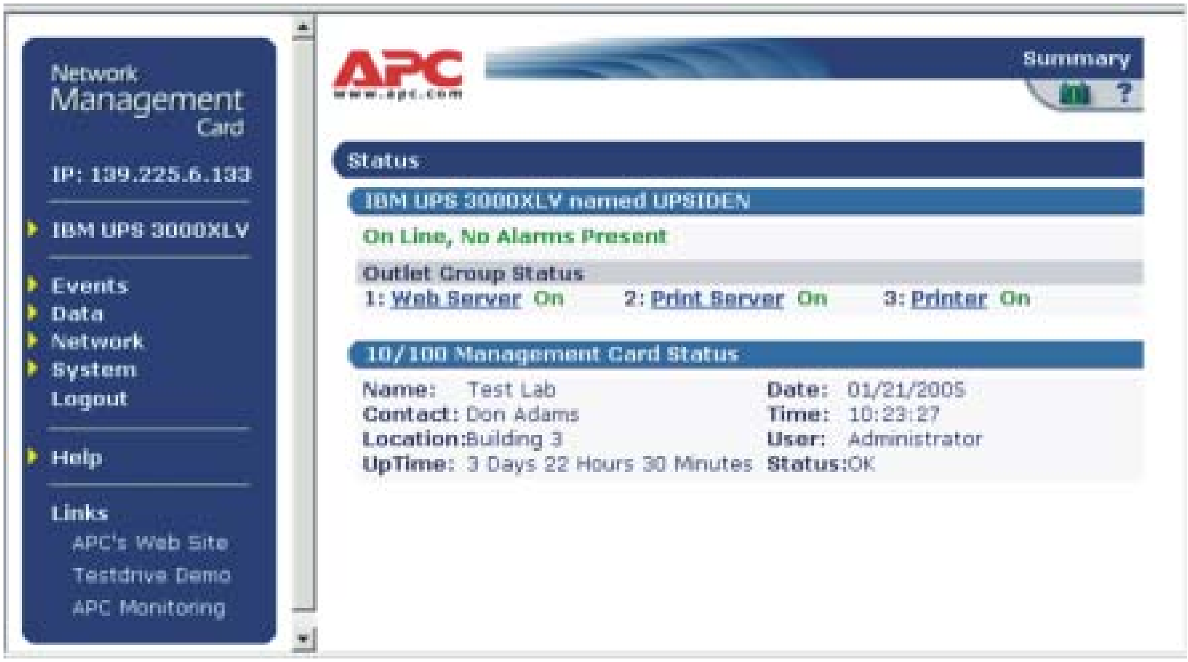
Summary Page

Example Web page

A navigation menu (see **"Navigation Menu" on page 27**) and summary page are displayed when you log on to the Web interface of the Embedded Network Module of an IBM UPS 3000XHV or IBM UPS 3000XLV model.

After the Embedded Network Module connects with an uninterruptible power supply, you can click the battery status icon on any Web interface page to access the summary page.

For more information about the help and status icons in the Web interface pages, see **"Quick status tab" on page 26**.



Status

IBM UPS 3000XLV named UPSIDEN

On Line, No Alarms Present

Outlet Group Status

1: Web Server On 2: Print Server On 3: Printer On

10/100 Management Card Status

Name:	Test Lab	**Date:**	01/21/2005
Contact:	Don Adams	**Time:**	10:23:27
Location:	Building 3	**User:**	Administrator
UpTime:	3 Days 22 Hours 30 Minutes	**Status:**	OK

Summary page fields

The summary page has two sections:

- The uninterruptible power supply section reports the status of a connected uninterruptible power supply and, under **Outlet Group Status**, the name and status of each outlet group.
- The Embedded Network Module section reports the following information:
  - The name, contact, and location information for the Embedded Network Module.
  - The login date and time.
  - Type of user (Administrator, Device Manager, or Read-Only User).
  - How long (**Up Time**) the Embedded Network Module has been continuously running since it was turned on or reset.
  - The status of the Embedded Network Module.

Quick status tab

The quick status tab in the upper-right corner of every Web interface page can display two icons:

- A question mark (?) provides access to the online help for that page:

  ?

- A battery icon identifies the current status of the uninterruptible power supply and accesses the summary page from any other page:

Not applicable to IBM UPS 3000XHV and IBM UPS 3000XLV.

The uninterruptible power supply is operating normally.

The uninterruptible power supply is turned off.

The uninterruptible power supply is overloaded.

The uninterruptible power supply has a bad battery.

The uninterruptible power supply is switched to battery operation.

A fault exists at the uninterruptible power supply.

Communication with the uninterruptible power supply has been lost, or the uninterruptible power supply is unsupported.

Navigation Menu

Overview

When you log on to the Web interface as an Administrator, the navigation menu (left frame) contains the following elements:

- The IP address of the Embedded Network Module.
- The uninterruptible power supply menu which uses the uninterruptible power supply model for its name (**IBM UPS 3000XHV** in the example on **"Example Web page" on page 24**).
- The **Events** menu.
- The **Data** menu.
- The **Network** menu.
- The **System** menu.

Note

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

- The **Logout** option.
- The **Help** menu.
- The **Links** menu.

Selecting a menu to perform a task

Use the menus to perform tasks as follows:

- To manage an uninterruptible power supply, and to set up and manage Synchronized Control Groups, see **"Uninterruptible Power Supply Menu" on page 68**.
- To do the following, see **"Event-Related Menus" on page 106**:
  - Access the event log.
  - Configure the actions to be taken based on the severity level of an event.
  - Configure SNMP Trap Receiver settings to send event-based traps.
  - Define who will receive e-mail notifications of events.
- To do the following, see **"Data Menu (Web Interface Only)" on page 127**:
  - Access the data log.
  - Define the log interval (how often data will be sampled and recorded) for the data log.
- To do the following, see **"Network Menu" on page 31**:
  - Configure new TCP/IP settings for the Embedded Network Module.
  - Identify the Domain Name System (DNS) Server, test its network connection, and enable or disable DNS Reverse Lookup Event Logging (which logs the domain name of the device associated with each event).
  - Define settings for FTP, Telnet, SSH, the Web interface, SNMP, e-mail, and SSL/TLS.
  - Configure the Syslog message feature of the Embedded Network Module.
  - Enable or disable access to the Embedded Network Module by users of the Wireless Application Protocol (WAP).

- To do the following, see **"System Menu" on page 59**.
  - – Control Administrator, Device Manager, and Read-Only User access.
  - – Define the system name, contact, and location.
  - – Set the date and time used by the Embedded Network Module.
  - – Through the **Tools** menu:
    - Restart the user interface of the Embedded Network Module.
    - Reset parameters to their default values.
    - Delete SSH host keys and SSL certificates.
    - Upload an initialization file (.ini file) that has been downloaded from another Embedded Network Module. The current Embedded Network Module then uses the values in that .ini file to configure its own settings.
  - – Select Fahrenheit or Celsius for temperature displays.
  - – Define the URL addresses used by the user links and logo link of the Web interface, as described in **"Links menu" on page 30**.

Help menu

When you click **Help**, the contents page for the online help is displayed to provide for easy navigation to a specific online help topic. However, from any of the Web interface pages, you can use the question mark (**?**) in the quick status bar to link to the section of the online help for the content of that page.

Use the **About System** option of the **Help** menu to view information about the Embedded Network Module model number, serial number, hardware revision, date of manufacture, MAC address, application module and AOS module, including the date and time these modules were created.

For help on the type of flash memory used, see Flash Type in the **About System** option of the **System** menu in the control console.

Links menu

This menu provides three user-definable URL link options. By default, these links access the following 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** option is not used with the IBM UPS 3000XHV and IBM UPS 3000XLV models.

You can use the following procedure to redefine these links so that they point to other URLs.

1. Click on **Links** in the **System** menu.
2. Define any new names for the user links.
3. Define any new valid URL addresses that you want the user links to access.
4. Click **Apply**.

Network Menu

Introduction

Overview

The **Network** menu has the options that you use to do the following tasks:

- Define TCP/IP settings, including DHCP or BOOTP server settings, when one of those types of servers is used to provide the required TCP/IP values.
- Use the Ping utility.
- Define and display settings that affect the Embedded Network Module settings for DNS, FTP, Telnet, SSH, SNMP, E-mail, Syslog, the Web interface (SSL/TLS), and WAP.

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" on page 33.
- "DNS" on page 36.
- "Send DNS Query (Web interface)" on page 37.
- "Ping utility (control console)" on page 38.
- "FTP Server" on page 39.
- "Telnet/SSH" on page 40.
- "SNMP" on page 47.
- "Email" on page 48.
- "Syslog" on page 49.
- "Web/SSL" on page 52.
- "WAP" on page 58.

Option Settings

TCP/IP

This option accesses the following settings:

- A Boot Mode setting selects the method used to define the TCP/IP values that the Embedded Network Module needs to operate on the network:
  - **System IP**: The IP address of the Embedded Network Module.
  - **Subnet Mask**: The subnet mask value.
  - **Default Gateway**: The IP address of the default gateway.

  For information about the watchdog role of the default gateway, see **"Resetting the network timer" on page 8**.

- Advanced Settings define the Embedded Network Module host and domain names, as well as Ethernet port speed, BOOTP, and DHCP settings used by the Embedded Network Module.

Current TCP/IP settings fields. The current values for **System IP**, **Subnet Mask**, and **Default Gateway**, and the Embedded Network Module **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 TCP/IP settings of the Embedded Network Module whenever the Embedded Network Module turns on, resets, or restarts:

- **Manual**: Three settings (**System IP**, **Subnet Mask**, and **Default Gateway**) which are available only 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 Embedded Network Module 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, by default, will 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 Embedded Network Module.

For information about the **After IP Assignment** setting, and other settings that affect how the Embedded Network Module uses BOOTP and DHCP, see **"Advanced settings" on page 35**. For more information about how to use DHCP, see **"Boot Mode" on page 129**.

Advanced settings. The boot mode affects which settings are available:

- Two settings are available for all **Boot mode** selections to define the Embedded Network Module **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 Embedded Network Module interface (except e-mail addresses) that accepts a domain name as input.
  - **Domain Name**: An Administrator needs to configure the domain name here only. In all other fields in the Embedded Network Module interface (except e-mail addresses) that accept domain names, the Embedded Network Module 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 Embedded Network Module 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 communication speed of the TCP/IP port (**Auto-negotiate**, by default).

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

    Attention: If the Client ID is changed from the Embedded Network Module MAC address, the new value must be unique on the LAN. Otherwise, the DHCP or BOOTP server might act incorrectly.

  - **User Class**: Uses the application firmware module type for the Embedded Network Module (**SUMX**, by default).
- Two settings are available if **BOOTP only** is the Boot mode selection:
  - **Retry Then Fail**: Defines how many times the Embedded Network Module 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 Embedded Network Module 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" on page 129**.

DNS

Use the **DNS** option to define the IP addresses of the primary and secondary Domain Name System (DNS) servers used by the e-mail feature of the Embedded Network Module. The primary DNS server will always be tried first.

For more information, see **"E-mail Feature" on page 119** and **"DNS servers" on page 120**.

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 following settings to define the parameters for the test DNS request; you 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** 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 have no 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 of the Embedded Network Module by testing whether a defined IP address or domain name responds to the Ping network utility. By default, the default gateway IP address (see **"TCP/IP" on page 33**) 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 Secure CoPy (SCP) for file transfers. When you select and configure Secure SHell (SSH), SCP is enabled automatically. If you decide to use SCP for file transfer, be sure to disable the FTP server.

To configure SSH, see **"Telnet/SSH" on page 40**.

Use the **Port** setting to identify the TCP/IP port that the FTP server uses for communications with the Embedded Network Module. 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 the Embedded Network Module IP address of 152.214.12.114, you would type this command:

```
ftp 152.214.12.114:5000
```

To access a text version of the Embedded Network Module event or data log, see **"How to use FTP or SCP to retrieve log files" on page 111**.

To use FTP to download configuration files:

- See **"File Transfer (control console only)" on page 65** if the files are on an FTP server of your company or agency.
- See **"Firmware file transfer methods" on page 189** if you are downloading files from the IBM Web site.

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, SSH version 2, or both.
- In the Web interface, specify a host key file previously created with the Security Wizard and load it to the Embedded Network Module.

Note From a command line interface, such as the command prompt on Windows operating systems, you can use FTP or Secure CoPy (SCP) to transfer the host key file. You must transfer the file to the /sec folder on the Embedded Network Module.

If you do not specify a host key file, the Embedded Network Module generates an RSA host key of 768 bits, instead of the 1024-bit RSA host key that the Wizard creates. *The Embedded Network Module 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 Embedded Network Module.

Note If you are using SSH version 2, expect a noticeable delay when logging on to the control console of the Embedded Network Module. 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	Enables or disables the access method selected in **Protocol Mode**. **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.
Protocol Mode	Choose one of the following: • **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 Embedded Network Module. • **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	Identifies the TCP/IP port used for communications by Telnet with the Embedded Network Module. The default is **23**.
	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 Embedded Network Module IP address of 152.214.12.114, your Telnet client would require one or the other of the following commands:
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`

SSH Port	Identifies the TCP/IP port used for communications by the Secure SHell (SSH) protocol with the Embedded Network Module. The default is **22**. 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.

Option	Description
SSH Server Configuration	
SSHv1 Encryption Algorithms	Enables or disables DES, and displays the status (always enabled) of Blowfish, two encryption algorithms (block ciphers) compatible with SSH version 1 clients. • **DES**: The key length is 56 bits. • **Blowfish**: The key length is 128 bits. You cannot disable this algorithm. **NOTE:** Not all SSH clients can use every algorithm. If your SSH client cannot use Blowfish, you must also enable DES.
SSHv2 Encryption Algorithms	Enables or disables the following encryption algorithms (Block Ciphers) that are compatible with SSH version 2 clients. • **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. **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.)

Option	Description
SSH User Host Key File	
Status:	The **Status** field Indicates the status of the host key (private key). In the control console, you display host key status by selecting **Advanced SSH Configuration**. • **SSH Disabled: No host key in use**: SSH currently is disabled and is not using a host key. A host key may or may not be loaded. **NOTE:** A host key must be installed to the /sec directory of the Embedded Network Module. • **Generating**: The Embedded Network Module is generating a host key because no valid host key was installed in its /sec directory. • **Loading**: A host key is being activated on the Embedded Network Module. • **Valid**: The host key is valid. (If you install an invalid host key, the Embedded Network Module discards it and generates a valid one. However, a host key that the Embedded Network Module generates is only 768 bits in length. A valid host key created by the Security Wizard is 1024 bits.)
Filename:	You can create a host key file with the Security Wizard and then upload it to the Embedded Network Module by using the Web interface. Use the **Browse** button for the **Filename** field to locate the file, then click **Apply**. Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the host key file to the Embedded Network Module. **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 Embedded Network Module creates one when it restarts. *The Embedded Network Module takes up to 5 minutes to create this key, and the SSH server is not accessible during that time.*

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

To define up to four Network Management Stations as trap receivers, see **"Trap Receivers" on page 118**.

Setting	Definition	
Community Name	This setting defines the password (maximum of 15 characters) which a Network Management Station (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: • 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/Domain Name** setting can use the channel, when that NMS uses the correct value for **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

You use this option to define two SMTP settings (**SMTP Server** and **From Address**) used by the e-mail feature of the Embedded Network Module.

For more information, see **"SMTP settings" on page 121** and **"E-mail Feature" on page 119**.

Syslog

By default, the Embedded Network Module can send messages to up to four Syslog servers whenever Embedded Network Module or uninterruptible power supply 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.

This user's guide does not describe Syslog or its configuration values in detail. For more information about Syslog, see RFC3164, 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.

Setting	Definition
General Settings	
Syslog	Enables (by default) or disables the Syslog feature.
Facility	Selects the facility code (**User**, by default) assigned to the Syslog messages of the Embedded Network Module. **NOTE:** Although several daemon-specific and process-specific selections are available, along with eight generic selections, **User** is the selection that best defines the Syslog messages sent by a Embedded Network Module.

Setting	Definition
Syslog Server Settings	
Server IP/ Domain Name	Uses specific IP addresses or domain names to Identify which of up to four servers will receive Syslog messages sent by the Embedded Network Module. **NOTE:** To use the Syslog feature, at least **Server IP/Domain Name** must be defined for at least one server.
Port	Identifies the user datagram protocol (UDP) port that the Embedded Network Module will use to send Syslog messages. The default is **514**, the number of the UDP port assigned to Syslog.
Local Priority (Severity Mapping)	
Map to Syslog's Priorities	Maps each of the severity levels (**Local Priority** settings) that can be assigned to uninterruptible power supply and Embedded Network Module events to the available Syslog priorities. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the four **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** • **None** (for events that have no severity level assigned) is mapped to **Info** **NOTE:** To disable sending Syslog messages for **Severe**, **Warning**, or **Informational** events, see **"Event Actions (Web Interface Only)" on page 114**.

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

1. Select the priority you want to assign to the test message.
2. Define the test message, using any text that is formatted as described in **"Syslog message format" on this page**. For example, `APC: Test message`, meets the required message format.
3. Click **Apply** to have the Embedded Network Module 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 event associated with the message and identifies the facility code assigned to messages sent by the Embedded Network Module.
- The Header includes a time stamp and the IP address of the Embedded Network Module.
- The message (MSG) part has two fields:
  - A TAG field, which is followed by a colon and a space, identifies the event type.
  - 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 Embedded Network Module:
  - 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 Embedded Network Module by means of digital certificates.

    See **"Creating and Installing Digital Certificates" on page 149** 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 Embedded Network Module. If a certificate has been created with the Security Wizard but is not installed:
  - In the Web interface, browse to the certificate file and upload it to the Embedded Network Module.
  - Alternatively, use the Secure CoPy (SCP) protocol or FTP to upload it to the /sec directory on the Embedded Network Module.

Note Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL/TLS). If no server certificate is loaded when you enable HTTPS (SSL/TLS), the Embedded Network Module creates one when it restarts. *The Embedded Network Module 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	Choose one of the following: • **HTTP:** User names, passwords, and data are transmitted without encryption. • **HTTPS (SSL/TLS):** User names, passwords and data are transmitted in encrypted form, and digital certificates are used for authentication. **NOTE:** To enable HTTPS (SSL/TLS), 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.

Option	Description
HTTP/HTTPS Port Configuration	
HTTP Port	Identifies the TCP/IP port used for communications by HTTP with the Embedded Network Module. The default is **80**. 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. 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 Embedded Network Module IP address of 152.214.12.114, you would use this command: `http://152.214.12.114:5000`
HTTPS Port	Identifies the TCP/IP port used for communications by HTTPS with the Embedded Network Module. The default is **443**. 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. 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 Embedded Network Module IP address of 152.214.12.114, you would use this command: `https://152.214.12.114:6502`

Option	Description
SSL Server Configuration	
CipherSuite	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/TLS Configuration**.) **NOTE:** All of these encryption ciphers and hash algorithms use the RSA public key algorithm. • **DES (SSL_RSA_WITH_DES_CBC_SHA)**: a block cipher with a key length of 56 bits. The 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_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. • **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.

Option	Description
SSL/TLS Server Certificate	
Status:	The **Status** field indicates whether a server certificate is installed. (To display the status in the control console, choose **Web/SSL/TLS**, then **Advanced SSL/TLS Configuration**.) • **Not installed**: No certificate is installed on the Embedded Network Module. **NOTE:** If you install a certificate by using FTP or SCP, you must specify the correct directory (/sec) on the Embedded Network Module. • **Generating**: The Embedded Network Module is generating a certificate because no valid certificate was installed. • **Loading**: A certificate is being loaded (activated on the Embedded Network Module). • **Valid**: A valid certificate was installed to or generated by the Embedded Network Module. (If you install an invalid certificate, the Embedded Network Module discards it and generates a valid one. However, a certificate that the Embedded Network Module generates has some limitations. See **"Method 1: Use the auto-generated default certificate of the Embedded Network Module" on page 150**.)
Filename:	You can create a server certificate with the Security Wizard and then upload it to the Embedded Network Module 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. Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Embedded Network Module. However, you must specify the correct location (**/sec**) on the Embedded Network Module. **NOTE:** Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL/TLS). If no server certificate is loaded when you enable HTTPS (SSL/TLS), the Embedded Network Module creates one when it restarts. *The Embedded Network Module can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time*.

Parameter	Description
Current Certificate Details	
Issued to:	**Common Name (CN)**: The IP Address or DNS name of the Embedded Network Module, except if the server certificate was generated by default by the Embedded Network Module. For a default server certificate, the **Common Name (CN)** field displays the Embedded Network Module serial number. **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 Embedded Network Module; 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. **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 Embedded Network Module, the **Organizational Unit (OU)** field displays “Internally Generated Certificate.” **Serial Number**: The serial number of the server certificate.
Issued By:	**Common Name (CN)**: The Common Name as specified in the CA root certificate, except if the server certificate was generated by default by the Embedded Network Module. For a default server certificate, the **Common Name (CN)** field displays the Embedded Network Module serial number. **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 Embedded Network Module, the **Organizational Unit (OU)** field displays “Internally Generated Certificate.”
Validity	**Issued on**: The date and time at which the certificate was issued. **Expires on**: The date and time at which the certificate expires.

Parameter	Description
Fingerprints	Each of the two fingerprints 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. **SHA1 Fingerprint**: This fingerprint is created by a Secure Hash Algorithm (SHA). **MD5 Fingerprint**: This fingerprint is created by a Message Digest 5 (MD5) algorithm.

WAP

Use this option to enable (the default) or disable the Wireless Application Protocol (WAP). WAP is a standard for providing cellular phones, pagers and other handheld devices with secure access to e-mail and text-based Web pages. WAP runs on all major wireless networks and is device-independent, so that it can be used with many phones and handheld devices.

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 Embedded Network Module real-time clock with a Network Time Protocol (NTP) server.
- Reset or restart the Embedded Network Module.
- Define the URL links available in the Web interface.
- Access hardware and firmware information about the Embedded Network Module.
- Set the units (Fahrenheit or Celsius) used for temperature displays.

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" on page 61**.
- **"Identification" on page 62**.
- **"Date & Time" on page 62**.
- **"Tools" on page 64**.
- **"Preferences (Web interface)" on page 66**.
- **"Links (Web interface)" on page 66**.
- **"About System" on page 67**.

Note **About System** is an option of the **Help** menu 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
Values affecting all users	
Auto Logout	The number of minutes (3 by default) before a user is automatically logged off because of inactivity.
Authentication	The **Basic** setting (default) causes the Web interface to use standard HTTP 1.1 login (base64-encoded passwords); **MD5** causes the Web interface to use an MD5-based authentication login. **NOTE:** Cookies must be enabled at a browser before it can be used with MD5 authentication.
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 password for the three account types). **NOTE:** A Read-Only User cannot log on through the control console.
Authentication Phrase	The case-sensitive, 15-to-32 character phrase used to log on to the Web interface when MD5 is the **Authentication** setting. Default settings are: • **admin user phrase** for Administrator • **device user phrase** for Device Manager • **readonly user phrase** for Read-Only User

Identification

Use this option to define the System **Name**, **Location**, and **Contact** values used by the SNMP agent of the Embedded Network Module. The settings for this option provide the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** OIDs.

For more information about the MIB-II OIDs, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide* provided on the Embedded Network Module CD.

Date & Time

Use this option to set the time and date used by the Embedded Network Module. The option displays the current settings, and enables 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 Embedded Network Module.

Note

An **Apply Local Computer Time to Embedded Network Module** 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 Embedded Network Module 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 time zone of the Embedded Network Module.
Update Interval	Defines how often, in hours, the Embedded Network Module 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 Embedded Network Module, 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 Embedded Network Module.
Reset to Defaults	Resets all configuration settings. **NOTE:** For information about how this affects the **Boot mode** setting, see the description of **Reset Only TCP/IP to Defaults** in this table.
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 TCP/IP settings of the Embedded Network Module must be defined by a DHCP or BOOTP server. See **"TCP/IP" on page 33**.
Delete SSH Host Keys and SSL Certificates	Removes any SSH host key and server certificate on the Embedded Network Module 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 Embedded Network Module to the current Embedded Network Module, export the .ini file from the configured Embedded Network Module, select the **Tools** menu on the current Embedded Network Module, browse to the file, and click **Upload**. The current Embedded Network Module 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" on page 174** 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 Embedded Network Modules.

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 Embedded Network Module.

Option	Description
XMODEM	Enables you to transfer either an .ini file or a firmware upgrade file to a Embedded Network Module 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" on page 11**.
FTP Client	Use one of these two option 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 Embedded Network Module. These options assume that your organization has a centralized system for configuring or upgrading Embedded Network Modules. 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 Embedded Network Module 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 **APC Monitoring**).
URL	Defines the URL addresses used by the links. By default, the following URL addresses are used: • **http://www.apc.com** (**APC's Web Site**) • **http://testdrive.apc.com** (**Testdrive Demo**) • **http://rms.apc.com** (not used with the IBM UPS 3000XHV and IBM UPS 3000XLV models) **NOTE:** For information about these pages see **"Links menu" on page 30**.
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

This option identifies hardware information for the Embedded Network Module, including model number, serial number, date of manufacture, hardware revision, MAC address, and flash type.

This information is set at the factory and cannot be changed.

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

Uninterruptible Power Supply Menu

Introduction

Overview

In the Web interface, the uninterruptible power supply menu is in the navigation menu; in the control console, you access the uninterruptible power supply menu through the **Device Manager** option in the **Control Console** menu. The menu is named with the model name of the uninterruptible power supply you are using, such as **IBM UPS 3000XHV**.

Uninterruptible power supply menu options

The uninterruptible power supply menu options and the information they provide vary by uninterruptible power supply model.

For information about the uninterruptible power supply menu options available in both the control console and the Web interface, see the following:

- **"Uninterruptible Power Supply Status" on page 69**.
- **"Diagnostics" on page 74**.
- **"Control" on page 77**.
- **"Configuration" on page 87**.
- **"Outlet Groups" on page 90**.
- **"PowerChute (PowerChute Network Shutdown)" on page 94**.
- **"Scheduling Uninterruptible Power Supply Shutdown" on page 98**.
- **"Sync Control" on page 103**.

Uninterruptible Power Supply Status

Overview

The **Status** options provide access to the information described in the following sections:

- **"Detailed uninterruptible power supply status" on page 70.**
- **"Utility Power Status" on page 71**.
- **"Output Power Status" on page 72**.
- **"Battery Status" on page 73**.
- **"About UPS" on page 73**

Detailed uninterruptible power supply status

The uninterruptible power supply menu provides an option to display uninterruptible power supply status.

- In the Web interface, use the **Status** option.
- In the control console, use the **Detailed Status** option

Note In the control console, the **Detailed Status** option accesses expanded descriptions of the uninterruptible power supply status.

The following information is displayed:

- The current status of the uninterruptible power supply:
  - Whether the uninterruptible power supply is online, and whether any alarms are present.

    For a list of the uninterruptible power supply events that can be reported as part of the uninterruptible power supply status, see **"Event List page" on page 125**.
  - When uninterruptible power supply output is on, the status of each outlet group (**On** or **Off**).
    - In the Web interface, outlet status is displayed wherever uninterruptible power supply status is displayed. If a command is pending for the outlet group, the status of the outlet group is displayed in orange.
    - In the control console, outlet status is displayed when you choose any **Control** option of the uninterruptible power supply menu as well as above the uninterruptible power supply menu itself. If a command is pending for the outlet group, the status of the outlet group is displayed with an asterisk (**On*** or **Off***).
- The reason for the last transfer to battery power at the uninterruptible power supply.
- The internal temperature of the uninterruptible power supply.

- The runtime that is available currently to the uninterruptible power supply.
- The values described in **"Utility Power Status" on this page**, **"Output Power Status" on page 72**, and **"Battery Status" on page 73**.

Utility Power Status

Status Field	**Definition**
Input Voltage	The AC voltage (VAC) being input to the uninterruptible power supply.
Input Frequency	The frequency of the input voltage in Hertz (Hz). **NOTE:** In the control console, the **Operating Frequency** field reports the frequency value shared by the input and output voltages.
Maximum Line Voltage	The highest AC voltage input to the uninterruptible power supply during the previous minute of operation.
Minimum Line Voltage	The lowest AC voltage input to the uninterruptible power supply during the previous minute of operation.

Output Power Status

Status Field	**Definition**
Output Voltage	The AC voltage the uninterruptible power supply is providing to its load.
Output Frequency	The frequency, in Hz, used by the output voltage. **NOTE:** In the control console, the **Operating Frequency** field reports the frequency value shared by the input and output voltages.
Load Power	The uninterruptible power supply load as a percentage of available Watts.
Apparent Load Power	The power that the load of the uninterruptible power supply is using, as a percentage of available output Volt-Amps.
Load Current	The current, in Amps, supplied to the load.

Battery Status

Status Field	**Definition**
Battery Capacity	The percentage of the battery capacity of the uninterruptible power supply available to support the attached equipment.
Battery Voltage	The available DC power.
Number of External Batteries	How many external batteries the uninterruptible power supply has.
Runtime Remaining	How long the uninterruptible power supply can use battery power to support its attached equipment.
Self-Test Result	The result of the last self-test.
Self-Test Date	The date when the last self-test was performed.
Calibration Result	The result of the last runtime calibration.
Calibration Date	When the last runtime calibration was performed.

About UPS

This option displays information in the following fields: **Model Number**, **Firmware Revision**, **Manufacture Date**, and **Serial Number**.

Diagnostics

Overview

There are two types of diagnostics options you can use with the uninterruptible power supply:

- Options that cause a specified test to occur immediately.
- A scheduling option that controls when an uninterruptible power supply self-test occurs.

Diagnostic tests

To perform diagnostic tests on the uninterruptible power supply or to display the results of the last self-test and runtime calibration:

- In the Web interface, use the **Diagnostics** option of the uninterruptible power supply menu.
- In the control console, use the diagnostics options of the **Control** menu to perform the test. For the results of the last self-test and runtime calibration, use the option **Detailed Status**.

You can use diagnostics options to perform the following tests.

Test	**Definition**
Self-Test	Performs a self-test of the uninterruptible power supply.
Simulate Power Failure	Causes the uninterruptible power supply to test its ability to switch to battery operation.
Start/Stop Runtime Calibration	Initiates (or cancels) a runtime calibration, a process which calculates how much runtime the uninterruptible power supply has available. **NOTE:** You can perform a runtime calibration only when the battery is at 100% capacity.
Test UPS Alarm	Causes the uninterruptible power supply to generate an alarm tone and flash its front panel lights. If the uninterruptible power supply is a member of a Synchronized Control Group: • In the Web interface, this option always tests the alarms of all enabled members of the group. • In the control console, you are prompted to choose whether to apply the action to the initiating uninterruptible power supply or to all members of the group. • In SNMP, you can set the OID **upsAdvControlFlashAndBeep** to either **flashAndBeep (2)** to test the alarm of an individual uninterruptible power supply or **flashAndBeepSyncGroup (3)** to test the alarms of all enabled group members.

Scheduled self-tests of the uninterruptible power supply

To schedule a self-test:

- In the Web interface, select **Diagnostics** on the uninterruptible power supply menu, then use the **Auto Self-Test** option.
- In the control console, from the uninterruptible power supply menu, select in order **Configuration**, **General**, and **Self-Test Schedule**.

The scheduling option enables you to control when an uninterruptible power supply self-test occurs. The available selections are **Never**, **UPS Startup**, **Every 7 Days**, or **Every 14 Days**.

Control

Initiating an uninterruptible power supply control option

You can initiate an uninterruptible power supply control option in either of these ways:

- For the uninterruptible power supply of the initiating Embedded Network Module only.
  - In the Web interface, select **No** for "Apply to Sync Group?"
  - In the control console, type `NO` (in uppercase) in response to the question "Apply command to all SCG members?"
- For all members of the Synchronized Control Group to which this Embedded Network Module belongs (if the option is supported for Synchronized Control Groups).
  - In the Web interface, select **Yes** for "Apply to Sync Group?"
  - In the control console, press Enter in response to the question "Apply command to all SCG members?"

Guidelines for Synchronized Control Groups

The option to apply an action to a Synchronized Control Group is displayed only if this Embedded Network Module is an active (enabled) member of a Synchronized Control Group.

All Embedded Network Modules in a Synchronized Control Group must belong to uninterruptible power supplies of the same model.

To configure an Embedded Network Module to be a member of a Synchronized Control Group, see **"Sync Control" on page 103**.

The synchronization process. If you apply an action to the Synchronization Control Group, the uninterruptible power supplies with Embedded Network Modules that are enabled group members behave as follows:

- Each uninterruptible power supply receives the command regardless of its output status, even if it is in a low-battery state.
- The action uses the delay periods (such as **Shutdown Delay**, **Sleep Time**, and **Return Delay)** that are configured for the initiating uninterruptible power supply.
- When the action begins, any uninterruptible power supply that is unable to participate retains its present output status while the other uninterruptible power supplies in the group perform the action. If an uninterruptible power supply is already in the output state that the action requires (for example, an uninterruptible power supply is already off when the **Reboot UPS** action starts), that uninterruptible power supply logs an event, but performs the rest of the action, if any.
- All uninterruptible power supplies participating in the action synchronize their performance of the action (within a one-second time period under ideal conditions).
- In restart and sleep actions:
  - Immediately before the initiating uninterruptible power supply begins its **Return Delay**, by default it waits up to 120 seconds (its configurable **Power Synchronized Delay**) for any uninterruptible power supply that does not have input power to regain that power. Any uninterruptible power supply that fails to regain input power within the **Power Synchronized Delay** does not participate in the synchronized restart, but instead waits until its own input power returns before restarting.

  - The LEDs on the front of the uninterruptible power supply do not sequence their lights as they do for a normal (not synchronized) restart or sleep action.

- Uninterruptible power supply status and events are reported in the same way for synchronized actions as for actions on individual uninterruptible power supplies.

For more information about the delays and required battery capacity settings in the following table, see **"Configuration" on page 87** and **"Sync Control" on page 103**.

Actions (for a single uninterruptible power supply and Synchronized Control Groups). Use the actions described in the table on the next several pages for individual uninterruptible power supplies and for Synchronized Control Groups.

For descriptions of the uninterruptible power supply control options **Self-Test**, **Simulate Power Failure**, **Start/Stop Runtime Calibration**, and **Test UPS Alarm**, see **"Diagnostic tests" on page 74**.

Action	Definition
Turn UPS On (control console)	This action turns on power at the uninterruptible power supply. • For an uninterruptible power supply that has outlet groups, this action then turns on the outlet groups according to the value configured **Power On Delay** for each group. See **"Delay Settings" on page 91**. • For a Synchronized Control Group, after a delay of a few seconds, this action turns on all enabled group members that have input power.
Turn UPS Off	This action turns off the output power of the uninterruptible power supply and all its outlet groups immediately, without a shutdown delay. The uninterruptible power supply and all its outlet groups remain off until you turn on its power again. If the uninterruptible power supply is a member of a Synchronized Control Group, this action turns off power at all uninterruptible power supplies that are enabled members of the group. No **Shutdown Delay** value is used. The uninterruptible power supplies turn off after a few seconds, and they remain off until you turn on their power again. See **"Shutdown Parameters" on page 88**. **NOTE:** For a synchronized turn-off action that uses the **Shutdown Delay** of the initiating uninterruptible power supply, use SNMP. Set the value to **turnUpsSyncGroupOffAfterDelay (5)** for the **upsAdvControlUpsOff** OID.
Turn UPS Off Gracefully[1] (control console)	This action turns off outlet power of the uninterruptible power supply and all its outlet groups after the uninterruptible power supply **Maximum Shutdown Time** plus two minutes, and its **Shutdown Delay**. See **"Maximum Shutdown Time negotiation" on page 96** and **"Shutdown Parameters" on page 88**. For a Synchronized Control Group, the action is performed using the delays configured for the group member that initiated the action.

[1] When you select **Yes** for the **Signal servers** option of the Web interface, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, or **Put UPS To Sleep Gracefully** in the control console.

Action	Definition
Reboot UPS	This action restarts the attached equipment by doing the following: • Turns off power at the uninterruptible power supply after the **Shutdown Delay.** • Turns on power at the uninterruptible power supply after the battery capacity of the uninterruptible power supply returns to at least the percentage configured for **Return Battery Capacity** and the uninterruptible power supply waits the time specified as **Return Delay**. See **"Shutdown Parameters" on page 88**. • For an uninterruptible power supply with outlet groups configured, a **Power On Delay** occurs after the uninterruptible power supply turns on and before an outlet group turns on. You configure **Power On Delay** for each outlet group through the **Outlet Control** option of the uninterruptible power supply menu. See **"Delay Settings" on page 91**. For a Synchronized Control Group action: • This action turns off power at the uninterruptible power supplies that are enabled group members after waiting the time configured as **Shutdown Delay** of the initiating uninterruptible power supply. See **"Shutdown Parameters" on page 88**. • The initiating uninterruptible power supply then waits up to the number of seconds specified as **Power Synchronized Delay** to allow time for group members to regain input power. If all group members have already regained input power, this delay is omitted. If all group members regain input power during the delay, the remainder of the delay is cancelled. To configure the **Power Synchronized Delay**, see **"Configure Synchronized Control" on page 104**. • The **Return Delay** then starts when the initiating uninterruptible power supply is at its configured **Return Battery Capacity**. See **"Shutdown Parameters" on page 88**. • The **Return Battery Capacity** of the initiating uninterruptible power supply is also required of group members, but you can reduce the capacity required of a group member by configuring **Return Battery Capacity Offset** (set at 10% by default) for that member. For example, if **Return Battery Capacity** of the initiator is set at 50%, and **Return Battery Capacity Offset** of a member is set to 5%, that battery capacity of that member will need to be at only 45% for that member to restart. See **"Configure Synchronized Control" on page 104**.

[1] When you select **Yes** for the **Signal servers** option of the Web interface, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, or **Put UPS To Sleep Gracefully** in the control console.

Action	Definition
Reboot UPS Gracefully[1] (control console)	• This action is performed similarly to the **Reboot UPS** action, but with an additional delay before the shutdown portion of the action. The attached equipment shuts down only after the uninterruptible power supply (or the initiating uninterruptible power supply for a Synchronized Control Group action) waits the **Maximum Shutdown Time** plus two minutes. For information about how the **Maximum Shutdown Time** is determined, see **"Maximum Shutdown Time negotiation" on page 96**. • For an uninterruptible power supply with outlet groups configured, a **Power On Delay** occurs after the uninterruptible power supply turns on and before an outlet group turns on. You configure **Power On Delay** for each outlet group through the **Outlet Control** option of the uninterruptible power supply menu. See **"Delay Settings" on page 91**.
Put UPS To Sleep	This action puts the uninterruptible power supply into sleep mode by turning off its output power for a defined period of time, as follows: • The uninterruptible power supply turns off output power after waiting the time configured as its **Shutdown Delay**. See **"Shutdown Parameters" on page 88**. • When input power returns, the uninterruptible power supply turns on output power after two configured periods of time, its **Sleep Time** and **Return Delay**. See **"Shutdown Parameters" on page 88**. • For a synchronized control group action, the Embedded Network Module of the uninterruptible power supply initiating the action waits up to the number of seconds configured as its **Power Synchronized Delay** for enabled group members to regain input power before it starts the **Return Delay**. If all group members have already regained input power, the **Power Synchronized Delay** is omitted. If all group members regain input power during the delay, the remainder of the delay is cancelled. See **"Configure Synchronized Control" on page 104**.

[1] When you select **Yes** for the **Signal servers** option of the Web interface, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, or **Put UPS To Sleep Gracefully** in the control console.

Action	Definition
Put UPS To Sleep Gracefully[1] (control console)	This action puts the uninterruptible power supply into sleep mode (turns off power for a defined period of time), as follows: • The uninterruptible power supply turns off output power after waiting the delay time configured as its **Maximum Shutdown Time** plus 2 minutes (to allow time for PowerChute Network Shutdown to shut down its server safely) and its **Shutdown Delay**. See **"Maximum Shutdown Time negotiation" on page 96** and **"Shutdown Parameters" on page 88**. • When input power returns, the uninterruptible power supply turns on output power after two configured periods of time, its **Sleep Time** and **Return Delay**. See **"Shutdown Parameters" on page 88**. • For a Synchronized Control Group action, the Embedded Network Module of the uninterruptible power supply initiating the action waits up to the number of seconds configured as its **Power Synchronized Delay** for enabled group members to regain input power before it starts the **Return Delay**. If all group members have already regained input power, the **Power Synchronized Delay** is omitted. If all group members regain input power during the delay, the remainder of the delay is cancelled. See **"Configure Synchronized Control" on page 104**.

[1] When you select **Yes** for the **Signal servers** option of the Web interface, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, or **Put UPS To Sleep Gracefully** in the control console.

Outlet group behavior when you turn on the uninterruptible power supply. How the outlet groups of an uninterruptible power supply turn on depends on how they are configured and how the uninterruptible power supply is turned on or off.

- Until you configure the following actions and their related delays, when you turn on the uninterruptible power supply output, any outlet group that is off turns on by default and applies power to all devices attached to the outlets in that group.
- After you configure the actions and delays:
  - The actions and delays control how outlet groups turn on and off when you turn the uninterruptible power supply on or off from the user interfaces of the Embedded Network Module (the Web interface or control console).
  - When you turn on the uninterruptible power supply from its front panel, each group turns on after the number of seconds configured for **Power On Delay**.

Outlet group behavior when you turn off the uninterruptible power supply. When you turn an uninterruptible power supply off at its front panel, all outlets turn off immediately.

How to control outlet group actions

Initiating an action. While the output of the uninterruptible power supply is on, select the **Control** option of the uninterruptible power supply menu to turn on, turn off, or restart any outlet group, with or without a delay.

- In the Web interface, these actions are under the heading **Initiate an Outlet Group control action**.
- In the control console, choose the sub-menu option **Outlet Groups**.

To configure any of the three delay values that the following actions use, see **"Delay Settings" on page 91**.

To override the turning on of outlet groups during the **Delayed On**, **Reboot**, or **Delayed Reboot** action, check-mark the **Never** box when configuring the **Power On Delay**, as described in **"Delay Settings" on page 91**. When that box is check-marked, the only action that turns on outlet groups is the **Immediate on** action.

Action	**Definition**
Immediate on	Turns on the outlet group immediately.
Delayed on	Turns on the outlet group after the number of seconds configured for **Power On Delay**.
Immediate off	Turns off the outlet group immediately.
Delayed off	Turns off the outlet group after the number of seconds configured for **Power Off Delay**.
Reboot	Turns the outlet group off immediately, then turns it on after the number of seconds configured for **Reboot Duration** and **Power On Delay**.
Delayed reboot	Turns the outlet group off after the number of seconds configured for **Power Off Delay**, then turns it on after the number of seconds configured for **Reboot Duration** and **Power On Delay**.

Outlet Group Events and Traps. A change in the state of any outlet group generates the event **UPS: Outlet Group turned on** with a default severity level of Informational, or **UPS: Outlet Group turned off** with a default severity level of Warning.The event messages are `UPS: Outlet Group` *`group_number`*`,` *`group_name`*`,` *`action`* `due to` *`reason`* and `UPS: Outlet Group` *`group_number`*`,` *`group_name`*`,` *`action`* `due to` *`reason`*. For example:

```
UPS: Outlet Group 1, Web Server, turned on due to user control.
UPS: Outlet Group 3, Printer, turned off due to line fail.
```

By default, each of these events generates an event log entry, an e-mail notification, and a Syslog message.

If you configure trap receivers for these events, SNMP trap 298 is generated when an outlet group turns on and SNMP trap 299 is generated when an outlet group turns off, with the event messages as trap arguments and with the default severity levels the same as for the events.

Configuration

Overview

The **Configuration** option of the uninterruptible power supply menu provides access to the configurable parameters described in the following sections:

- **"Utility Line Settings" on this page**.
- **"Shutdown Parameters" on page 88**.
- **"General Settings (Configuration)" on page 89**.
- **"Reset UPS Defaults" on page 89**.

Utility Line Settings

Setting	Definition
Output Voltage	The nominal AC voltage level for the uninterruptible power supply output.
High Transfer Voltage	The upper limit of acceptable input voltage. When the input reaches this value, the uninterruptible power supply starts to use its AVR Trim feature.
Low Transfer Voltage	The lower limit of acceptable input voltage. When the input reaches this value, the uninterruptible power supply starts to use its AVR Boost feature.
Sensitivity	How sensitive the uninterruptible power supply will be to distortions in the input voltage.

Shutdown Parameters

Note In the control console, use the **Battery** option in the **Configuration** menu to access the **Return Battery Capacity** setting.

Setting	Definition
Return Battery Capacity	Defines the minimum battery capacity required before the uninterruptible power supply turns on after a shutdown that was caused by a power failure. **NOTE:** The uninterruptible power supply must also wait the time defined by the **Return Delay** setting before it can turn on.
Low-Battery Duration	Defines how long the uninterruptible power supply can continue to run on battery power after a low-battery condition occurs. **NOTE:** This setting also defines the time available for PowerChute to shut down its server safely in response to the **Control** options **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, and **Put UPS To Sleep Gracefully**.
Maximum Shutdown Time (Web interface only)	Reports the delay that is defined by the **Maximum Shutdown Time** setting for the PowerChute Network Shutdown feature. **NOTE:** For information about the PowerChute Network Shutdown feature, see **"PowerChute (PowerChute Network Shutdown)" on page 94**; for information about how the **Maximum Shutdown Time** is determined, see **"Maximum Shutdown Time negotiation" on page 96**.
Shutdown Delay	Defines how long the uninterruptible power supply waits before it shuts down in response to a turn-off command.
Return Delay	Defines how long the uninterruptible power supply waits before it turns on after a shutdown that was caused by a power failure. **NOTE:** The uninterruptible power supply must also have the capacity specified by the **Return Battery Capacity** setting before it can turn on.
Sleep Time	Defines how long the uninterruptible power supply sleeps (keeps its output power turned off) when you use either of the sleep options in the **Control** menu (**Put UPS To Sleep** or **Put UPS To Sleep Gracefully**). **NOTE:** This setting also is in the Control page of the Web interface.

General Settings (Configuration)

Note

In the control console, use the **Battery** option in the **Configuration** menu to access the **Last Battery Replacement** and **External Batteries** settings.

Setting	Definition
UPS Name	Defines the name of the uninterruptible power supply.
Last Battery Replacement	Defines the date of the most recent uninterruptible power supply battery replacement. **NOTE:** Use *mm/dd/yy* format.
Self-Test Schedule (control console only)	Schedules when and how frequently an uninterruptible power supply self-test occurs. See **"Scheduled self-tests of the uninterruptible power supply" on page 76**.
Audible Alarm	Defines when an uninterruptible power supply generates an alarm in response to switching to battery operation.
External Batteries	Defines how many external battery packs are connected to the uninterruptible power supply. The uninterruptible power supply cannot automatically sense and report the number of connected battery packs.
Simple Signal Shutdowns	When enabled, allows simple-signalling shutdown through PowerChute Network Shutdown.

Reset UPS Defaults

This option resets the uninterruptible power supply to use the default EEPROM values.

Attention!

Before you use this option, make sure that resetting the EEPROM values will not adversely affect the load equipment or any shutdown sequence.

Outlet Groups

Overview

The uninterruptible power supply provides AC output to three outlet groups (groups of one or more AC outlets). By using the network interface to control each outlet group remotely, you can start or stop devices sequentially and restart locked devices.

The **Outlet Groups** option of the uninterruptible power supply menu provides access to the configurable parameters described in the following sections:

- **"Delay Settings" on page 91**.
- **"General Settings (Outlet Groups)" on page 92**.
- **"Automatic Load Shedding for Outlet Groups (Web interface only)" on page 93**.

Delay Settings

In the Web interface or control console, you can set the following delays for each outlet group. The minimum value for each delay is 0 seconds, and the maximum value is 600 seconds. For information on the actions that use these delays, see **"How to control outlet group actions" on page 84**.

Delay	Definition
Power On Delay	If the box **Never** is cleared (the default), the actions **Delayed On**, **Reboot**, and **Delayed Reboot** use this delay. In response to the action **Delayed On**, the outlet group waits the number of seconds configured for **Power On Delay** before it turns on. In response to the action **Reboot**, the outlet group turns off immediately, then waits the number of seconds configured for **Reboot Duration** and for **Power On Delay** before it turns on. In response to the action **Delayed Reboot**, the outlet group turns off after the number of seconds configured for **Power Off Delay**. The outlet group then waits the number of seconds configured for **Reboot Duration** and for **Power On Delay** before it turns on. If the box **Never** is check-marked, all outlets remain off when the uninterruptible power supply turns on, except when you use the **Immediate On** action.
Power Off Delay	The actions **Delayed Off** and **Delayed Reboot** use this delay. In response to the action **Delayed Off**, the outlet group waits the number of seconds configured for **Power Off Delay** before it turns off. In response to the action **Delayed Reboot**, the outlet group turns off after the number of seconds configured for **Power Off Delay**. The outlet group then waits the number of seconds configured for **Reboot Duration** and for **Power On Delay** before it turns on.

Delay	Definition
Reboot Duration	The actions **Reboot** and **Delayed Reboot** use this delay. • In response to the action **Reboot**, the outlet group turns off immediately, then waits the number of seconds configured for **Reboot Duration** and for **Power On Delay** before it turns on. • In response to the action **Delayed Reboot**, the outlet group turns off after the number of seconds configured for **Power Off Delay**. The outlet group then waits the number of seconds configured for **Reboot Duration** and for **Power On Delay** before it turns on.

General Settings (Outlet Groups)

Setting	Definition
Name	Defines a name for the outlet group. Use a name that describes the device or devices powered by the outlet group. The name is displayed with the outlet group number wherever the Web or control console interfaces display that number.
Link (URL) (Web interface only)	For each outlet group, defines a hyperlink that can be used from anywhere in the Web interface where the outlet group name is displayed. The default for each link is **http://www.apc.com**. You must use http:// or https:// when redefining any of the links. For example: • **https://www.*mysite*.com** • **http://www.ibm.com**

Automatic Load Shedding for Outlet Groups (Web interface only)

Use the check-boxes provided to enable or disable the following settings for each outlet group, and configure a value for each setting that you enable. Use these settings to provide automatic, sequenced, load-shedding when a problem occurs with input voltage or battery capacity and to provide automatic sequenced start-up of outlet groups when the problem is resolved.

Note These settings are disabled by default.

Type	Setting	Definition
Group Off Settings	Turn off when a power failure is longer than *n* seconds	Turns off the outlet group after input power fails for longer than the number of seconds you specify.
	Turn off when a power failure and battery capacity is less than *n*%	Turns off the outlet group when input power fails and battery capacity drops below the percentage you specify.
	Turn off when the UPS percent load is greater than *n*%	Turns off the outlet group when the output drawn from the uninterruptible power supply exceeds the percentage of uninterruptible power supply output overload that you specify.
Group On Settings	Turn on when the UPS returns from a power failure after the duration of *n* seconds	After the uninterruptible power supply switches from battery power to input power, waits the number of seconds you specify before the outlet group turns on.
	Turn on when the UPS returns from a power failure after battery capacity is greater than *n*%	Turns on the outlet group after input power to the uninterruptible power supply is restored and battery capacity of the uninterruptible power supply reaches the percentage of full capacity that you specify.

PowerChute (PowerChute Network Shutdown)

Overview

The **PowerChute** option of the uninterruptible power supply menu in the Web interface enables you to use the PowerChute Network Shutdown utility to shut down as many as 50 servers on your network that are using any client version of PowerChute Network Shutdown.

For more information about PowerChute Network Shutdown, see the *PowerChute Network Shutdown Installation Guide* and the *PowerChute Network Shutdown Release Notes*, provided on the Embedded Network Module CD.

PowerChute Network Shutdown Parameters

Parameter	Definition
Maximum Shutdown Time	Defines the maximum time that the uninterruptible power supply at a PowerChute Network Shutdown client waits before it shuts down in response to a graceful turn-off command. **NOTE:** For information about how this shutdown delay is determined, see **"Maximum Shutdown Time negotiation" on page 96**.
Shutdown Behavior	Defines how the uninterruptible power supply turns off after the PowerChute Network Shutdown clients finish shutting down their computer systems.
Add Client IP Address	Enables you to add as many as 50 PowerChute Network Shutdown clients to the Configured Client IP Addresses list. **NOTE:** When you install a PowerChute Network Shutdown client on your network, it is added to the list automatically.
Configured Client IP Addresses	Enables you to view the list of PowerChute Network Shutdown clients, and remove PowerChute Network Shutdown clients from the list. **NOTE:** When you uninstall a PowerChute Network Shutdown client, it is removed from the list automatically.

Maximum Shutdown Time negotiation

The **Maximum Shutdown Time** setting provides the delay needed to make sure that a server has enough time to shut down safely when the Embedded Network Module or PowerChute Network Shutdown client initiates a graceful shutdown at that server.

For information about the **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, and **Put UPS To Sleep Gracefully** options that use this delay for uninterruptible power supplies and Synchronized Control Groups, see **"Control" on page 77**.

The time reported in the **Maximum Shutdown Time** field represents the maximum delay needed by at least one of the servers listed in the Configured Client IP Addresses list. This time is determined by a negotiation process that is initiated when any of the following occurs:

- The Embedded Network Module turns on (a **System: Coldstart** event).
- The Embedded Network Module is reset (a **System: Warmstart** event).
- You select **Force negotiation** from the drop-down list for the **Maximum Shutdown Time** field, and click **Apply**.

During the negotiation process, which can take up to 10 minutes, each server listed in the Configured Client IP Addresses is contacted to determine the shutdown delay needed by that server. The delay time defined by the **Maximum Shutdown Time** setting will be changed, if necessary, to the highest delay time reported by the servers.

For example:

- If **3 minutes** was the result of the last negotiation process, and a new server that requires a 4-minute shutdown delay has been added to the Configured Client IP Addresses list, **4 minutes** will be the new **Maximum Shutdown Time**.

- If none of the servers needs more than a 2-minute delay, **2 minutes** will be the **Maximum Shutdown Time** setting.

Note

At the end of the negotiation process, the two-minute time period is added to the calculated total for **Maximum Shutdown Time** to allow for any unusual delays that might occur in notifying servers to shut down.

Scheduling Uninterruptible Power Supply Shutdown

Overview

This option is available in the Web interface only.

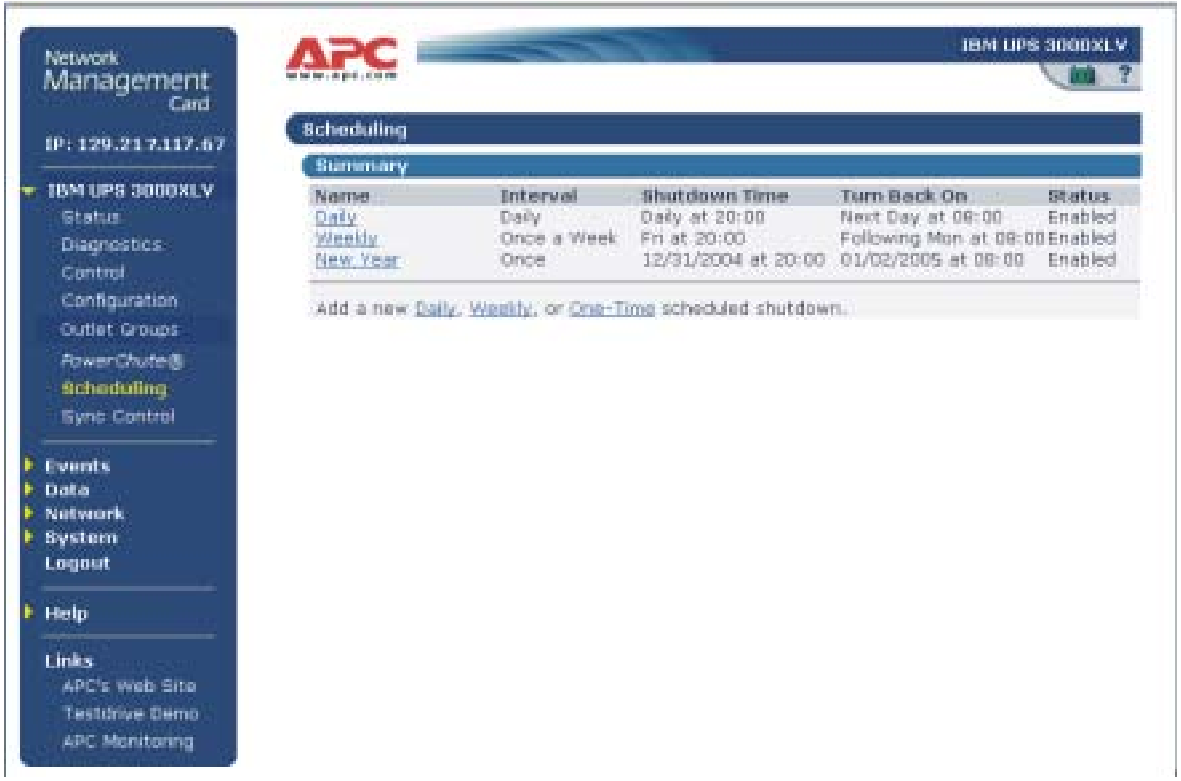
You can schedule shutdowns on a daily, weekly or one-time basis, and you can schedule them for a single uninterruptible power supply or for all uninterruptible power supplies in a Synchronized Control Group.

For more information about how to use this option, see the following sections:

- **"Examples" on page 99**.
- **"How to schedule a shutdown" on page 100**.
- **"How to schedule a synchronized shutdown" on page 101**.
- **"How to edit, disable, or delete a shutdown" on page 102**.

Examples

The following Web page provides examples of **Daily**, **Weekly**, and **One-Time** shutdowns that were scheduled using the **Scheduling** option, which is available in the Web interface only.



Scheduling

Summary

Name	Interval	Shutdown Time	Turn Back On	Status
Daily	Daily	Daily at 20:00	Next Day at 08:00	Enabled
Weekly	Once a Week	Fri at 20:00	Following Mon at 08:00	Enabled
New Year	Once	12/31/2004 at 20:00	01/02/2005 at 08:00	Enabled

Add a new Daily, Weekly, or One-Time scheduled shutdown.

How to schedule a shutdown

Click the **Daily**, **Weekly**, or **One-Time** option to choose the type of shutdown, and then use the following fields:

1. Use **Name of Scheduled Shutdown** to define a name for the shutdown.
2. Use **Shutdown** to define when the shutdown will begin.
3. Use **Turn back on** to define whether the uninterruptible power supply will turn on at a specific day and time, **Never** (the uninterruptible power supply will be turned on manually), or **Immediately** (the uninterruptible power supply will turn on after a six-minute delay).
4. Select whether PowerChute servers will be warned before the shutdown begins.
5. Click **Apply**.

How to schedule a synchronized shutdown

To use the Web interface of the Embedded Network Module to schedule shutdowns within a Synchronized Control Group, always schedule all shutdowns through the same member of the group.

The following guidelines apply to Synchronized Control Groups:

- All Embedded Network Modules in a Synchronized Control Group must be of the same uninterruptible power supply model.
- For a scheduled uninterruptible power supply shutdown to occur, a network connection to the uninterruptible power supply must exist at the time at which the action is scheduled to occur.

⚠ Attention! Scheduled shutdowns through more than one group member is not a supported configuration and may cause unpredictable results.

All scheduled shutdowns will be synchronized when the Embedded Network Module that initiates the shutdown is a member of a Synchronized Control Group and its status as a group member is enabled.

How to edit, disable, or delete a shutdown

Click a listed shutdown to display the Daily Shutdown Detail page. Use this page to do the following:

- View a summary of the shutdown, including information about the values for settings that can affect how the uninterruptible power supply shuts down and turns on again:
  - For information about **Maximum Shutdown Time**, a **PowerChute** option, see **"Maximum Shutdown Time negotiation" on page 96**.
  - For information about **Shutdown Delay** and **Return Delay**, see **"Shutdown Parameters" on page 88**.
- Change any shutdown parameter.
- Use **Status of Scheduled Shutdown** to enable, disable or delete the shutdown.

Sync Control

Overview

The **Sync Control** option of the uninterruptible power supply menu displays the status of each member of the Synchronized Control Group, if any, in which the Embedded Network Module is a member and the parameters necessary for the Embedded Network Module to be identified and operate as a member of the group.

Note All Embedded Network Modules in a Synchronized Control Group must be of the same uninterruptible power supply model.

Sync Control Group Status

Item	Description
IP Address	The IP address of the group member
Input Status	The state of the input power of the group member: **good** (acceptable) or **bad** (not acceptable)
Output Status	The status of the output power of the group member: **On** or **Off**

Configure Synchronized Control

Parameter	Description
Synchronized Group Membership	Determines whether this Synchronized Control Group member is an active member of its group. If you set this value to **Disabled** (the default value), the Embedded Network Module ignores all Synchronized Control Group commands, and its uninterruptible power supply functions as if it were not a member of any Synchronized Control Group.
Synchronized Control Group Number	The unique identifier of the Synchronized Control Group of which this Embedded Network Module is a member. This value must be a number from 1 through 65534. The Embedded Network Module of an uninterruptible power supply can be a member of only one Synchronized Control Group. All members of a Synchronized Control Group must have the same **Synchronized Control Group Number** and **Multicast IP Address**.
Power Synchronized Delay	The maximum time (120 seconds by default) that the initiating uninterruptible power supply of a synchronized sleep or restart action will wait for other group members to regain input power when the initiating uninterruptible power supply is ready to turn on. • For a synchronized restart, the initiating uninterruptible power supply waits up to this delay period for other group members to regain input power, then waits until its return battery capacity is reached, and then begins the **Return Delay**. The **Power Synchronized Delay** does not occur if all group members have input power immediately after they turn off for the restart. • For a synchronized sleep command, after the configured sleep time expires, the initiating uninterruptible power supply waits up to this delay period for other group members to regain input power, and then begins the **Return Delay**. The **Power Synchronized Delay** does not occur if all group members have input power after the sleep time expires.

Parameter	Description
Return Battery Capacity Offset	An amount of battery capacity, as a percentage, that is configured individually for each member of the Synchronized Control Group. This offset percentage enables you to set a different and lower **Return Battery Capacity** for each group member for use during synchronized actions only. To determine the **Return Battery Capacity** that will be required of each participating group member during a synchronized **Turn UPS On**, **Reboot UPS**, **Reboot UPS Gracefully**, **Sleep**, or **Sleep Gracefully** action, this offset percentage is subtracted from the **Return Battery Capacity** of the uninterruptible power supply that initiates the action.
Multicast IP Address	The IP address used by members of a Synchronized Control Group to communicate with each other. This address must be within the range of 224.0.0.3 to 224.0.0.254. All members of the Synchronized Control Group must have the same group number and multicast IP address.

Event-Related Menus

Introduction

Overview

Use the options of the **Events** menu 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. (You must use the Web interface to define which events will use which actions.)
  - Event logging.
  - Syslog messages.
  - SNMP trap notification.
  - E-mail notification.

To define which events will use which actions, see **"Event Log" on page 108** and **"How to Configure Individual Events" on page 125**.

- Define up to four SNMP trap receivers, by NMS-specific IP address or domain name, for event notifications by SNMP traps.
- Define up to four recipients for event notifications by e-mail.

Menu options

To access the event-related options:

- In the Web interface, use the **Events** menu.
- In the control console:
  - 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.
  - Press Ctrl+L to access the event log from any menu.

For information about event-related settings and about the e-mail feature, see the following descriptions:

- **"Event Log" on page 108**.
- **"Event Actions (Web Interface Only)" on page 114**.
- **"Event Recipients" on page 117**.
- **"E-mail Feature" on page 119**.
- **"How to Configure Individual Events" on page 125**.

Event Log

Overview

The Embedded Network Module supports event logging for all uninterruptible power supply application firmware modules. You can record and view uninterruptible power supply and Embedded Network Module events.

Use any of the following to view the event log:

- Web interface.
- Control console.
- FTP.
- SCP.

Logged events

By default, the following events are logged:

- Any event that causes an SNMP trap, except for SNMP authentication failures.
- The abnormal internal system events of the Embedded Network Module.

To disable the logging of events based on their assigned severity level, use the **Actions** option in the **Events** menu of the Web interface.

See **"Event Actions (Web Interface Only)" on page 114**.

Even if you disable the event log for all severity levels, some System (Embedded Network Module) events will still be logged because some of those events have no severity level.

See **"Event List page" on page 125** to access a list of all configurable events (uninterruptible power supply and Embedded Network Module) that indicates which events and how many events have been configured individually.

Note

The event log will log a graceful shutdown of the uninterruptible power supply, even when that shutdown was not initiated by the Embedded Network Module; a graceful shutdown from Serial Port 1 typically indicates that PowerChute performed the shutdown.

Web interface

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

Control console

In the 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 Deleted events cannot be retrieved.

How to use FTP or SCP to retrieve log files

If you are an Administrator or Device Manager, you can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) or data log file (*data.txt*) that you can import into a spreadsheet application.

- The file reports all of the events or data recorded since the log was last deleted.
- The file includes information that the event log or data log does not display.
  - The version of the file format (first field).
  - The date and time the file was retrieved.
  - The **Name**, **Contact**, and **Location** values and IP address of the Embedded Network Module.
  - The unique **Event Code** for each recorded event (*event.txt* file only).

Note The Embedded Network Module uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits of the year.

If you are using the encryption-based security protocols for your system, use Secure CoPy (SCP) to retrieve the log file. (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" on page 138** for information on the available protocols and methods for setting up the type of security appropriate for your needs.

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

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

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

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

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

1. At a command prompt, type `ftp` and the IP address of the Embedded Network Module, and press Enter.

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

   ```
   ftp>open ip_address port_number
   ```

   To use non-default port values to enhance security, see **"Port assignments" on page 140**.

2. Use the case-sensitive user name and password for either an Administrator or a Device Manager user to log on.
   - 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 log or data log to your local drive.

   ```
   ftp>get event.txt
   ```

   or

   ```
   ftp>get data.txt
   ```

4. You can use the **del** command to clear the contents of the event log or data log.

   ```
   ftp>del event.txt
   ```

   or

   ```
   ftp>del data.txt
   ```

   You will not be asked to confirm the deletion.
   - If you clear the data log, the event log records a deleted-log event.
   - If you clear the event log, a new *event.txt* file is created to record the deleted-log event.
5. Type `quit` at the **ftp>** prompt to exit from FTP.

Event Actions (Web Interface Only)

Overview

Use the **Actions** option in the **Events** menu to do the following:

- Select which actions will occur for events that have a severity level:
  - **Event Log** selects which severity levels cause an event to be logged.

    See **"Event Log action" on page 115**.
  - **Syslog** selects which severity levels cause messages to be sent to Syslog servers to log events.

    See **"Syslog action" on page 116**.
  - **SNMP Traps** selects which severity levels generate SNMP traps, and which trap receivers are notified for events of each severity level.

    See **"SNMP Traps action" on page 116**.
  - **Email** selects which severity levels cause e-mail notifications and which e-mail recipients receive e-mail for events of each severity level.

    See **"Email action" on page 116**.
- Click **Details** for a complete list of Embedded Network Module (System) and uninterruptible power supply events that can occur, and then edit the actions that will occur for an individual event. Click **Hide Details** to return to the **Actions** option.

  See **"How to Configure Individual Events" on page 125**.

Severity levels

Except for some System (Embedded Network Module) events that do not have a severity level, events are assigned a default severity level.

- **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 which does not require immediate attention.
- **Severe**: Indicates an event that requires immediate attention. Unless resolved, severe uninterruptible power supply and Embedded Network Module events can cause incorrect operation of the uninterruptible power supply or its supported equipment, or can result in the loss of uninterruptible power supply protection during a power failure.

Event Log action

To stop logging events that have a severity level, disable the **Event Log** action. System (Embedded Network Module) events that have no severity level will still be logged. By default, all events are logged, even events that have no severity level.

For more information about the log, see **"Event Log" on page 108**.

Syslog action

By default, the **Syslog** action is enabled for all events that have a severity level. However, before you can use this feature to send Syslog messages when events occur, you must configure it.

See **"Syslog" on page 49**.

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" on page 117**.

Email action

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

See **"E-mail Feature" on page 119**.

Event Recipients

Overview

Use the Web interface or control console to define up to four trap receivers, four e-mail addresses, and four paging recipients to be used when an event occurs that has SNMP, e-mail, or paging enabled, as described in **"Event Actions (Web Interface Only)" on page 114**.

To identify the servers that will receive Syslog messages, see **"Syslog" on page 49**.

Trap Receivers

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.

Email options

See **"E-mail Feature" on page 119**.

E-mail Feature

Overview

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

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

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

  See **"DNS servers" on page 120**.

- The DNS name of the **SMTP Server** and the **From Address** settings for SMTP.

  See **"SMTP settings" on page 121**.

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

  See **"Email Recipients" on page 122**.

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

DNS servers

The Embedded Network Module cannot send any e-mail messages unless at least the IP address of the primary DNS server is defined.

See **"DNS" on page 36**.

The Embedded Network Module will wait a maximum of 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the Embedded Network Module 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 Embedded Network Module, or on a nearby segment (but not across a wide-area network (WAN).

After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for computer.

SMTP settings

Use the **Email** option in the **Network** menu to define the following settings:

Setting	Description
SMTP Server	The IP address (or if DNS is configured, The DNS name) of the SMTP server. **NOTE:** This definition is required only when the **SMTP Server** option is set to **Local**. See **"Email Recipients" on page 122**.
From Address	The contents of the **From** field in the format *user@domain*.com (if an IP address is specified as **SMTP Server**) or *user@* [*IP_address*] (if DNS is configured and the DNS name is specified as **SMTP Server**) in the e-mail messages sent by the Embedded Network Module. **NOTE:** To configure the SMTP server, you may be required to use a valid user account on the server for this setting. See the server 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	Defines the user and domain names of the recipient. You can bypass the DNS lookup of the IP address of the mail server by using the IP address in brackets instead of the e-mail domain name. For example, use jsmith@[xxx,xxx.x.xxx] instead of jsmith@company.com. 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, myacct100@skytel.com). The pager gateway will generate the page. **NOTE:** The recipient's pager must be able to use text-based messaging.
Use SMTP Server	Selects one of the following methods for routing e-mail: • Through the SMTP server of the Embedded Network Module (the recommended option is **Local**). This option ensures that the e-mail is sent before the 20-second time-out of the Embedded Network Module, and, if necessary, is retried several times. Also do one of the following: • Enable forwarding at the SMTP server of the Embedded Network Module 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 enable forwarding. • Set up a special e-mail account for the Embedded Network Module 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 Embedded Network Module tries to send the e-mail only once. When the recipient uses the SMTP server of the Embedded Network Module, this setting has no affect.
Generation	Enables (by default) or disables sending e-mail to the recipient.

Setting	Description

Format	Selects the format used for e-mail messages:
	Short: Identifies only the event that occurred. For example:
	UPS: `Communications Established`
	Long: Includes information about the Embedded Network Module and the uninterruptible power supply, as well as the event. For example:
	`Name     : Test Lab`
	`Location : Building 3`
	`Contact  : Don Adams`
	`http://139.225.6.133`
	`Serial # : Wa12`
	`UPS Ser #: XS9849007541`
	`Date     : 10/12/2004`
	`Time     : 16:09:48`
	`Code      : 0x0002`
	`Severe - UPS: Communications Established`

How to Configure Individual Events

Event List page

The **Actions** option in the **Events** menu opens the Event Actions Configuration page. Use the **Details** button on that page for a complete list of the Embedded Network Module (System) and uninterruptible power supply events that can be reported by your Embedded Network Module.

On the Event List page, an asterisk at the beginning of an event description indicates that the event has been configured individually and is no longer set to its default configuration. A message at the bottom of the page indicates how many events have been configured.

Each event is identified by its unique code, its description, and its assigned severity level, as shown in the following examples.

For information about severity levels and how they define the actions associated with events, see **"Event Actions (Web Interface Only)" on page 114**.

Code	Description	Severity
0x0008	System: Password changed.	Informational
0x0109	UPS: Switched to battery backup power.	Warning

Detailed Event Action Configuration page

Each event code on the Event List page is a link to a page that enables you to do the following:

- Change the severity level of the selected event.
- Enable or disable whether the event uses the event log, Syslog messages, SNMP traps, paging, or e-mail notifications.
- Reset the event to its default configuration.

Log Option

Use this option to access a log that stores information about the uninterruptible power supply and the power input to that uninterruptible power supply.

Use the **Configuration** option of the **Data** menu to define how frequently data is sampled and stored in the data log. Each entry is listed by the date and time the data was recorded, and provides the data in a column format.

The data recorded depends on the uninterruptible power supply model.

See **"Configuration Option" on page 128**.

For descriptions of the recorded data that is specific to your uninterruptible power supply, see the online help in the Web interface of your Embedded Network Module.

To retrieve the data log as a text file, see **"How to use FTP or SCP to retrieve log files" on page 111**.

Configuration Option

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

The minimum interval is 60 seconds; the maximum interval is 8 hours, 10 minutes, 15 seconds.

Boot Mode

Introduction

Overview

In addition to using a BOOTP server or manual settings, the Embedded Network Module can use a dynamic host configuration protocol (DHCP) server to provide the settings the Embedded Network Module needs to operate on a TCP/IP network.

To use a DHCP server to provide the network settings of the Embedded Network Module, use **Boot mode**, a **TCP/IP** option in the **Network** menu. **Boot mode** must be set to either **DHCP & BOOTP**, its default setting, or **DHCP only**.

For information on DHCP and DHCP options, see RFC 2131 at **www.ietf.org/rfc/rfc2131** and RFC 2132 at **www.ietf.org/rfc/rfc2132**.

DHCP & BOOTP boot process

When **Boot mode** is set to its default **DHCP & BOOTP** setting, the following occurs when the Embedded Network Module is turned on or reset:

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

Note

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

See **"Embedded Network Module settings" on page 132**.

3. If the Embedded Network Module fails to receive a valid DHCP response after five DHCP requests, it repeats sending 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 (for example, the offer does not contain the APC cookie), the Embedded Network Module accepts the lease from that server on the last request of the sequence and then immediately releases that lease. This prevents the DHCP server from reserving the IP Address associated with its invalid offer.

For more information on what a valid response requires, including information on the APC cookie, see **"DHCP response options" on page 134**.

DHCP Configuration Settings

Embedded Network Module settings

Use the **TCP/IP** option in the **Network** menu of either the Web interface or the control console to configure the network settings of the Embedded Network Module.

- The **Port Speed**, **Host Name**, and **Domain Name** settings are available for any **Boot mode** selection.
- The **Vendor Class**, **Client ID**, and **User Class** settings are available for any **Boot mode** selection, except **Manual**.

See **"Advanced settings" on page 35**.

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 the selection based on the server that provided the TCP/IP settings (**DHCP Only** or **BOOTP Only**).
- **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" on page 134**.

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.
- **Retry Then Stop** in the control console (**Maximum # of Retries** in the Web interface): This option sets the number of times the Embedded Network Module will repeat the DHCP request if it does not receive a valid response. The default setting (**0** in the Web interface, **None** in the control console) requires that the Embedded Network Module continuously send out DHCP requests until a valid DHCP response is received.

DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings a Embedded Network Module needs to operate on a network and other information that affects the operation of the Embedded Network Module.

The Embedded Network Module 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 has this format.

  Tag 1, Len 4, Data "1APC"

  Option 43 communicates to the Embedded Network Module that a DHCP server has been configured to service devices that use Network Management Cards. By default, the APC cookie must be present in this DHCP response option before the Embedded Network Module can accept the lease.

  To disable the requirement of an APC cookie, see **"Embedded Network Module settings" on page 132**.

  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
  ```

- The Boot Mode Transition has this format.

  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 base its setting on the server that provided the network assignment values (**DHCP Only** or **BOOTP Only**):

  – A data value of 1 disables the **After IP Assignment** option. The **Boot mode** option remains as **DHCP & BOOTP** after network values are assigned successfully. Whenever the Embedded Network Module 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" on page 130**.

- A data value of 2 enables the **After IP Assignment** option. The **Boot mode** option switches to **DHCP Only** when the Embedded Network Module accepts the DHCP response. Whenever the Embedded Network Module restarts, it will request its network assignment from a DHCP server, only.

For more information about the **After IP Assignment** option, see **"Embedded Network Module settings" on page 132**.

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 Embedded Network Module 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): The IP address that the DHCP server is leasing to the Embedded Network Module**.**
- Subnet Mask (option 1): The Subnet Mask value which the Embedded Network Module needs to operate on the network.
- Default Gateway (option 3): The default gateway address, which the Embedded Network Module needs to operate on the network.
- Address Lease Time (option 51): The time duration for the lease associated with the identified IP Address.
- Renewal Time, T1 (option 58): The time that the Embedded Network Module must wait after an IP address lease is assigned before it can request a renewal of that lease.
- Rebinding Time, T2 (option 59): The time that the Embedded Network Module must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other options. The Embedded Network Module uses the following options within a valid DHCP response to define NTP, DNS, hostname and domain name settings:

- NTP Server, Primary and Secondary (option 42): Up to two NTP servers that can be used by the Embedded Network Module.
- NTP Time Offset (option 2): The offset of the Embedded Network Module's subnet, in seconds, from Coordinated Universal Time (UTC), formerly Greenwich Mean Time (GMT).
- DNS Server, Primary and Secondary (option 6): Up to two DNS servers that can be used by the Embedded Network Module.
- Host Name (option 12): The host name to be used by the Embedded Network Module (32-character maximum length).
- Domain Name (option 15): The domain name to be used by the Embedded Network Module (64-character maximum length).

Security Features

Planning and implementing security features

As a network device that passes information across the network, the Embedded Network Module 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: • User name and password • Selectable server port • Server Enable/Disable • Secure SHell (SSH)	For high security, use SSH. • 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: • Community Name • Domain Name • NMS IP filters • Agent Enable/Disable • 4 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. • 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: • 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: • User name and password • Selectable server port • Server Enable/Disable • MD5 authentication • Secure Sockets Layer (SSL) and Transport Layer Security (TLS)	In basic HTTP authentication mode, the user name and password are transmitted base-64 encoded (with no encryption). MD5 authentication mode uses a user name and password phrase. SSL and TLS are available on Web browsers supported for the Embedded Network Module 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.

Changing default user names and passwords immediately

As soon as you complete the installation and initial configuration of the Embedded Network Module, immediately change the default user names and passwords. Configuring unique user names and passwords is essential to establish basic security for your system.

Port assignments

If a Telnet, FTP, SSH/SCP, or Web/SSL/TLS 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 ports for the protocols. To hide the interfaces, use any port numbers from 5000 to 32768.

User names, passwords, 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 Embedded Network Module. 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

Authentication vs. Encryption

You can select to use security features for the Embedded Network Module 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.

For a security method that provides additional authentication for the Web interface, but does not provide the higher security of encryption, use Message Digest 5 (MD5) Authentication.

See **"MD5 authentication (for the Web interface)" on page 143**.

To ensure that data and communication between the Embedded Network Module 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. You can also use these protocols in combination with MD5 authentication.
- 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 Secure CoPy (SCP) protocol.

For more information on these protocols for encryption-based security, see **"Secure SHell (SSH) and Secure CoPy (SCP)" on page 145** and **"Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)" on page 146**.

MD5 authentication (for the Web interface)

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

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

If you use MD5 authentication for the Web interface, be sure to increase the security for other interfaces to the Embedded Network Module.

- **Control console:** Use SSH (which disables Telnet) for encrypted access.
- **File transfer:** Disable FTP, and instead use SCP, which encrypts user names, passwords, and files.
- **SNMP:** Disable SNMP or disable its write access. With read-only access, trap facilities remain available.

For additional information on MD5 authentication, see RFC document #1321 at **http://www.ietf.org**, the Web site of the Internet Engineering Task Force. For CHAP, see RFC document #1994.

You can use MD5 and the encryption-based SSL/TSL security protocols together. See **"Secure Sockets Layer (SSL)/Transport Layer Security (TLS)" on page 146** for an example of the extra security benefits of using both.

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 Embedded Network Module) 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 Embedded Network Module) 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" on page 169**.

- The Embedded Network Module 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 Embedded Network Module, 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" on page 40**.

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)/Transport Layer Security (TLS)

For secure Web communication, you 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 Embedded Network Module. 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 Embedded Network Module 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 Embedded Network Module). The browser verifies the following:

- The format of the server certificate is correct.
- The expiration date and time for the server certificate 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 Security Wizard, provided on the Embedded Network Module CD, 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 a root certificate to upload to the certificate store (cache) of a browser. You can also use the Wizard to create a server certificate to upload to the Embedded Network Module.

See **"Creating and Installing Digital Certificates" on page 149** for a summary of how these certificates are used.

To create certificates and certificate requests, see **"Create a Root Certificate & Server Certificates" on page 160** and **"Create a Server Certificate and Signing Request" on page 165**.

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

See **"CipherSuite" on page 55** to select which authentication and encryption algorithms to use.

You can use SSL/TLS and MD5 authentication together to provide the security benefits of both. MD5 authentication does not provide encryption, but its authentication methods can be a useful enhancement to the security provided by SSL/TLS.

Note

Web browsers cache (save) Web pages that you recently accessed and enable you to return to those pages without re-entering your user name and password. MD5 authentication, however, requires you to enter your user name and password even to access a cached Web page, for example, when you use the **Back** button of Microsoft Internet Explorer. Therefore, if you are using the SSL and TLS protocols without also using MD5 authentication, 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 Embedded Network Module supports the use of digital certificates with the Secure Sockets Layer (SSL) protocol. Digital certificates can authenticate the Embedded Network Module (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 of the Embedded Network Module" on page 150**.
- **"Method 2: Use the Security Wizard to create a CA certificate and a server certificate" on page 152**.
- **"Method 3: Use the 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" on page 154**.

Note

You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the Security Wizard 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 of the Embedded Network Module. When you enable SSL, you must restart the Embedded Network Module. While restarting, if no server certificate exists on the Embedded Network Module, the Embedded Network Module 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 Embedded Network Module access and all data to and from the Embedded Network Module 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 Embedded Network Module 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 Embedded Network Module, 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 Embedded Network Module has the serial number of the Embedded Network Module in place of a valid common name (the DNS name or the IP address of the Embedded Network Module). Therefore, although the Embedded Network Module can control access to its Web interface by user name, password, and account type (for example, Administrator, Device Manager, or Read-Only User), the browser cannot verify what Embedded Network Module 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 Security Wizard to create a CA certificate and a server certificate. You use the Security Wizard to create two digital certificates:

- A CA root certificate (Certificate Authority root certificate) that the 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 Embedded Network Module.
- A server certificate that you upload to the Embedded Network Module. When the Security Wizard creates a server certificate, it uses the CA root certificate to sign the server certificate.

The Web browser authenticates the Embedded Network Module sending or requesting data:

- To identify the Embedded Network Module, the browser uses the common name (IP address or DNS name of the Embedded Network Module) that was specified in the distinguished name of the server certificate 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 Embedded Network Module access and all data to and from the Embedded Network Module 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 Embedded Network Module enables SSL to verify that data are being received from and sent to the correct Embedded Network Module. 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 server certificate of the Embedded Network Module 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 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. You use the 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 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 Embedded Network Module.

Note

You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the Security Wizard 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 Embedded Network Module access and all data to and from the Embedded Network Module 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 Embedded Network Module.
  - 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 Embedded Network Module enables SSL to verify that data are being received from and sent to the correct Embedded Network Module. 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 Embedded Network Module with the signature on the CA root certificate that is already in the certificate cache of the browser 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 Security Wizard

Overview

Authentication

Authentication verifies the identity of a user or a network device (such as an Embedded Network Module). Passwords typically identify computer users. However, for transactions or communications requiring more stringent security methods on the Internet, the Embedded Network Module 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 Embedded Network Module.
- Secure SHell (SSH), used for remote terminal access to the control console of the Embedded Network Module, 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 Embedded Network Module, contain a set of CA root certificates from all of the commercial Certificate Authorities.

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

- Each Embedded Network Module with SSL enabled must have a server certificate on the Embedded Network Module itself.
- Any browser that is used to access the Web interface of the Embedded Network Module must contain the CA root certificate that signed the server certificate.

If authentication fails, the browser prompts you on 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 Embedded Network Module generates automatically. The digital signature of the default certificate 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 Embedded Network Module.)

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

Files you create for SSL and SSH security

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

- The server certificate for the Embedded Network Module, 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 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 the software of a browser.
- 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 Embedded Network Module when you log on to the control console interface.

Note

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

Server certificates, host keys, and CA root certificates created by the Security Wizard will not work with products such as OpenSSL and Microsoft Internet Information Server (ISS).

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 Security Wizard is 1024 bits. (The default key generated by the Embedded Network Module, 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 Embedded Network Modules. During this task, two files are created.
  - The file with the .p15 extension is an encrypted file that contains the private key and public root certificate of the Certificate Authority. This file signs the server certificates.
  - The file with the .crt extension, which contains only the public root certificate of the Certificate Authority. You load this file into each Web browser that will be used to access the Embedded Network Module so that the browser can validate the server certificate of the Embedded Network Module.
- 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 Embedded Network Module.
- For each Embedded Network Module 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 Security Wizard is not already installed on your computer, install it by running the installation program APC Security Wizard.exe from the Embedded Network Module 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 **CA Root Certificate** as the type of file to create.
4. Enter a name for the file that will contain the public root certificate and private key of the Certificate Authority. 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 down to view the unique serial number and fingerprints of the certificate. To make any changes to the information you provided, click **Back**, and revise the information.

   Note: The subject information and the issuer information of the certificate 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 Embedded Network Module.

Load the CA root certificate to your browser. Load the .crt file to the browser of each user who needs to access the Embedded Network Module.

See the help system of the browser for information on how to load the .crt file into the certificate store (cache) of the browser.

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" on page 160**.

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" on page 160**. 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 (Embedded Network Module). 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 down to view the unique serial number and fingerprints of the certificate 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 Embedded Network Module. It displays the location and name of the Server Certificate, which has a .p15 file extension and contains the Embedded Network Module private key and public root certificate.

Load the server certificate to the Embedded Network Module

Perform these steps:

1. On the **Network** menu of the Web interface of the Embedded Network Module, 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" on page 160**. The default is C:\Program Files\American Power Conversion\APC Security Wizard.

Note

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Embedded Network Module. If you use FTP or SCP for the transfer, you must specify the \sec directory on the Embedded Network Module. For SCP, the command to transfer a certificate named cert.p15 to a Embedded Network Module 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 private key of the Embedded Network Module.
  - 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 Embedded Network Module.
- For each Embedded Network Module 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 Security Wizard is not already installed on your computer, install it by running the installation program APC Security Wizard.exe from the Embedded Network Module 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 private key of the Embedded Network Module. 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 Embedded Network Module.

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 down to view the unique serial number and fingerprints of the certificate. To make any changes to the information you provided, click **Back**, and revise the information.

Note The subject information and the issuer information of the certificate 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 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 Embedded Network Module. (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 Certificate Signing Request (CSR)" on page 165**. This file has a .p15 extension, contains the private key of the Embedded Network Module, 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 Embedded Network Module. The file must have a .p15 extension.
6. Click **Next** to generate the server certificate. The Issuer Information of the certificate, 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 Embedded Network Module. It displays the location and name of the server certificate, which has a .p15 file extension and contains the private key of the Embedded Network Module and the public key obtained from the .cer or .crt file.

Load the server certificate to the Embedded Network Module

Perform these steps:

1. On the **Network** menu of the Web interface of the Embedded Network Module, 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" on page 167**. The default location is C:\Program Files\American Power Conversion\APC Security Wizard.

Note

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Embedded Network Module. If you use FTP or SCP for the transfer, you must specify the \sec directory on the Embedded Network Module. For SCP, the command to transfer a certificate named cert.p15 to a Embedded Network Module 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 Embedded Network Module generates a 768-bit RSA key when it restarts. Host keys for SSH that are created with the Security Wizard are 1024-bit RSA keys.

- Use the Security Wizard to create a host key, which is encrypted and stored in a file with .p15 extension.
- Load the host key onto the Embedded Network Module.

The procedure

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

1. If the Security Wizard is not already installed on your computer, install it by running the installation program APC Security Wizard.exe from the Embedded Network Module 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 Embedded Network Module, you can verify that the correct host key was uploaded by verifying that

the fingerprints displayed here match the SSH fingerprints on the Embedded Network Module, 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 Embedded Network Module. It displays the location and name of the host key, which has a .p15 file extension.

Load the host key to the Embedded Network Module. Perform these steps:

1. On the **Network** menu of the Web interface of the Embedded Network Module, 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" on page 169**. (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 Embedded Network Module 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 Secure CoPy (SCP) to transfer the host key file to the Embedded Network Module. If you use FTP or SCP for the transfer, you must specify the \sec directory, on the Embedded Network Module. For SCP, the command to transfer a host key named hostkey.p15 to a Embedded Network Module with an IP address of 156.205.6.185 would be:

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

Embedded Network Module

Embedded Network Module access problems

Problem	Solution
Unable to ping the Embedded Network Module	If the Status LED of the Embedded Network Module is green, try to ping another node on the same network segment as the Embedded Network Module. If that fails, it is not a problem with the Embedded Network Module. If the Status LED is not green, or if the ping test succeeds, perform the following checks: • Verify all network connections. • Verify the IP addresses of the Embedded Network Module and the NMS. • If the NMS is on a different physical network (or subnetwork) from the Embedded Network Module, verify the IP address of the default gateway (or router). • Verify the number of subnet bits for the subnet mask of the Embedded Network Module.
The terminal program cannot allocate the communications port when you try to configure the Embedded Network Module	Before you can use a terminal to configure the Embedded Network Module, you must shut down any application, service, or program using the communications port.
Cannot access the control console through a serial connection	Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.

Problem	Solution
Cannot access the control console remotely	• Make sure you are using the correct access method (Telnet or SSH). 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. • For Secure SHell (SSH), the Embedded Network Module may be creating a host key. The Embedded Network Module can take up to 5 minutes to create this host key, and SSH is not accessible during that time.
Cannot access the Web interface	• Verify that HTTP or HTTPS access is enabled. • Make sure you are specifying the correct URL, one that is consistent with the security system used by the Embedded Network Module. SSL requires https, not http, at the beginning of the URL. • Verify that you can ping the adapter. • Verify that you are using a Web browser that is supported for the Embedded Network Module. See **"Supported Web Browsers" on page 21**. • If the Embedded Network Module has just restarted and SSL security is being set up, the Embedded Network Module may be generating a server certificate. The Embedded Network Module can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.

SNMP issues

The following table describes known SNMP problems:

Problem	Solution
Unable to perform a GET	• Verify the read (GET) community name. • Use the control console or Web interface to ensure that the NMS has access. See **"SNMP" on page 47**.
Unable to perform a SET	• Verify the read/write (SET) community name. • Use the control console or Web interface to ensure that the NMS has write (SET) access. See **"SNMP" on page 47**.
Unable to receive traps at the NMS	Query the **mconfigTrapReceiverTable** MIB OID to verify that the NMS IP address is listed correctly, and the community name defined for the NMS matches the community name in the table. If either is not correct, use SETs to the **mconfigTrapReceiverTable** OIDs, or use the control console or Web interface to correct the trap receiver definition. See **"SNMP" on page 47**.
Traps received at an NMS are not identified	See your NMS documentation to verify that the traps are properly integrated in the alarm/trap database.

Synchronization problems

Problem	Solution
A Synchronized Control Group member does not participate in a synchronized action.	Make sure the status of the group member is set to **Enabled**. Also check the battery capacity of the group member, if the synchronized action required uninterruptible power supplies to turn on.
An attempt to add a member to a Synchronized control group fails.	The **Multicast IP Address**, **Synchronized Control Group Number**, and firmware version must match those of other members of the group.

How to Export Configuration Settings

Retrieving and Exporting the .ini file

Summary of the procedure

An Administrator can retrieve a dynamically generated .ini file of the current configuration of one Embedded Network Module and export that file to another Embedded Network Module or to multiple Embedded Network Modules.

1. Configure an Embedded Network Module to have the settings you want to export.
2. Retrieve the .ini file from that Embedded Network Module.
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 Embedded Network Module to transfer the copied file to one or more additional Embedded Network Modules. (To transfer the file to multiple Embedded Network Modules simultaneously, write an FTP or SCP script that repeats the steps for transferring the file to a single Embedded Network Module.)
5. Each receiving Embedded Network Module stores the file temporarily in its flash memory, uses it to reconfigure its own Embedded Network Module settings, and then deletes the file.

Contents of the .ini file

The config.ini file that you retrieve from an Embedded Network Module contains the following:

- Section headings, which are category names enclosed in brackets ([ ]), and under each section heading, keywords, which are labels describing specific Embedded Network Module settings.

  Note Only section headings and keywords supported for the specific device associated with the Embedded Network Module from which you retrieve the file are included.

- Each keyword is followed by an equals sign and the current value that is set for that parameter, 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 Embedded Network Module) blocks the exporting of the values for the keywords SystemIP, SubnetMask, DefaultGateway, and BootMode.
    - In the UPS section, the default value for Override (the serial number of the uninterruptible power supply) blocks the exporting of the value for the RatedOutputVoltage keyword. (RatedOutputVoltage and its value are included in the .ini file only if the output voltage of the uninterruptible power supply is configurable.)
  - You must edit the section [SystemDate/Time] if you want to set the system date and time of a receiving Embedded Network Module or cause that Embedded Network Module to use an NTP Server to set its date and time.

    See **"Customizing" on page 177** for configuration guidelines for date and time settings.

Detailed procedures

Use the following procedures to retrieve the settings of one Embedded Network Module and export them to one or more other Embedded Network Modules.

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

1. Configure an Embedded Network Module with the settings you want to export.

   Note: To avoid errors, configure the Embedded Network Module 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 Embedded Network Module you configured:

   a. Open a connection to the Embedded Network Module, 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 Embedded Network Module.

   c. Retrieve the config.ini file containing the current settings of the Embedded Network Module:

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

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

To create batch files and use a utility to retrieve configuration settings from multiple Embedded Network Modules and export them to other Embedded Network Modules, see *Release Notes: ini File Utility, version 1.0* on the Embedded Network Module CD.

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 Embedded Network Modules 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 Embedded Network Modules, can have any name up to 64 characters and must have the .ini file 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 Embedded Network Module. To export the .ini file to another Embedded Network Module, use any of the file transfer protocols supported by Embedded Network Modules (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 Embedded Network Module 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 Embedded Network Module 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 Embedded Network Modules. To export the .ini file to multiple Embedded Network Modules:

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single Embedded Network Module.
- Use a batch processing file and the .ini file utility.

To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* on the Embedded Network Module CD.

The Upload Event and its Error Messages

The event and its error messages

The following system event occurs when the receiving Embedded Network Module 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 Embedded Network Module succeeds even if there are errors.

Event text	**Description**
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number.*	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number*.	A keyword entered at the beginning of the file (before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, the Embedded Network Module 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 device associated with the Embedded Network Module from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the device (such as an uninterruptible power supply) is not present or, for some other reason, is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values. For example:

```
UPS not discovered
```

If you did not intend to export the configuration of the device as part of the .ini file import, ignore these messages.

Errors generated by overridden values

The Override keyword and its value will generate error messages in the event log when it blocks the exporting of values.

See **"Contents of the .ini file" on page 175** for information about which values are overridden.

The overridden values are device-specific and not appropriate to export to other Embedded Network Modules. 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 Embedded Network Module settings by using the Device IP Configuration Wizard.

For a detailed description of how to update the configuration settings of one or more Embedded Network Module using the Device IP Configuration Wizard, see **"Device IP Configuration Wizard" on page 182**.

Device IP Configuration Wizard

Purpose and Requirements

Purpose: configure basic TCP/IP settings

You can use the Device IP Configuration Wizard to configure the basic TCP/IP settings (IP address, subnet mask, and default gateway) of Embedded Network Modules in either of the following ways:

- Automatically discover and configure unconfigured Embedded Network Modules remotely over your TCP/IP network.
- Configure or reconfigure an Embedded Network Module through a direct connection from the serial port of your computer to the uninterruptible power supply that contains the Embedded Network Module.

Note The Wizard can discover and configure Embedded Network Modules 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.

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 Embedded Network Modules, obtain the MAC address of each one so that you can identify each Embedded Network Module that the Wizard discovers. (The Wizard displays the MAC address for a discovered Embedded Network Module on the same screen on which you then enter the TCP/IP settings.)

   The MAC address is on a label on the uninterruptible power supply containing the Embedded Network Module and on the Quality Assurance slip that came with the uninterruptible power supply.

Run the Wizard to perform the configuration. To discover and configure, over the network, Embedded Network Modules that are not configured:

1. From the **Start** menu, launch the Wizard. The Wizard automatically detects the first Embedded Network Module 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 Embedded Network Module 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 Embedded Network Module after you transmit the settings of the Embedded Network Module.
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 unconfigured Embedded Network Module. If it finds one, it displays the screen with data entry boxes for the TCP/IP settings of that Embedded Network Module.
   - To skip configuring the Embedded Network Module whose MAC address is currently displayed, click **Cancel**.
   - To configure the TCP/IP settings of the next Embedded Network Module, repeat this procedure beginning at **step 3**.

Configure or reconfigure the TCP/IP settings locally

To configure a single Embedded Network Module 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 uninterruptible power supply that contains the Embedded Network Module.
   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 uninterruptible power supply.
3. From the **Start** menu, launch the Wizard application.
   – If the Embedded Network Module is not configured, wait for the Wizard to detect it.
   – If you are assigning basic TCP/IP settings serially to the Embedded Network Module, 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 Embedded Network Module. 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 Embedded Network Module after you transmit the Embedded Network Module 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 Embedded Network Module.

File Transfers

Introduction

Overview

The Embedded Network Module 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 Embedded Network Module, the program code is updated and new features become available.

This chapter describes how to transfer firmware files to Embedded Network Modules.

To transfer a firmware file to an Embedded Network Module, see **"Upgrading Firmware" on page 188**.

To verify a file transfer, see **"Verifying Upgrades and Updates" on page 195**.

Upgrading Firmware

Firmware defined

Broadly defined, firmware is highly specialized, reliable software that resides on a memory chip within a computer or computer-related device.

Firmware files (Embedded Network Module)

The operating system (AOS) and application module files used with the Embedded Network Module share the same basic format:

```
apc_hw0x_type_version.bin
```

- **hw0*x***: Identifies the version of the Embedded Network Module that will run this binary file.
- ***type***: Identifies whether the file is for the operating system (AOS) or the application module (APP) for the Embedded Network Module.
- ***version***: The version number of the application file. For example, a code of 254 would indicate version 2.5.4.
- **bin**: Indicates that this is a binary file.

Firmware file transfer methods

To upgrade the firmware of an Embedded Network Module on a Microsoft Windows operating system, use the firmware upgrade tool, a self-extracting executable file available at no cost from the IBM Web site (**http://www.ibm.com**).

On a Linux operating system, you must upgrade the two firmware modules (the AOS module and the APP module) separately. The separate firmware modules are also available on the IBM Web site. After you download them, use one of the following upgrade methods:

- Use FTP or SCP to upgrade the firmware of one or more Embedded Network Modules over the network.
- Use XMODEM to upgrade the firmware for an Embedded Network Module that is not on the network.

When you use FTP, SCP, or XMODEM to upgrade the firmware for an Embedded Network Module, the operating system (AOS) module must be transferred to the Embedded Network Module before you transfer the application (APP) module.

For more information about the firmware modules, see **"Firmware files (Embedded Network Module)" on page 188**.

Use FTP or SCP to upgrade one Embedded Network Module

For you to be able to use FTP to upgrade a single Embedded Network Module over the network:

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

To use FTP to upgrade the Embedded Network Module:

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, use the following commands:

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

   Files listed for the Embedded Network Module, for example, might be the following:

   – `apc_hw02_aos_253.bin`

   – `apc_hw02_app_254.bin`

2. Open an FTP client session:

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

3. Type `open` and the IP address of the Embedded Network Module, and press Enter. If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default value 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 **FTP Server Port** setting of the Embedded Network Module 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 a Embedded Network Module 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_253.bin
```

6. When FTP confirms the transfer, type `quit` to close the session.
7. Wait 20 seconds, and then repeat this procedure for the application module. In **step 5**, use the application module file instead of the AOS module.

To use Secure CoPy (SCP) to upgrade the firmware for one Embedded Network Module:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the Embedded Network Module. The following example assumes the Embedded Network Module IP address of 158.205.6.185 and an AOS module apc_hw02_aos_253.bin:

   ```
   scp apc_hw02_aos_253.bin apc@158.205.6.185:apc_hw02_aos_253.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 Embedded Network Module.

How to upgrade multiple Embedded Network Modules

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

See *Release Notes: ini File Utility, version 1.0* on the Embedded Network Module CD.

Use an FTP client or SCP. To upgrade multiple Embedded Network Modules using an FTP client or using SCP, write a script which automatically performs the appropriate procedure described in **"Use FTP or SCP to upgrade one Embedded Network Module" on page 190**.

Use XMODEM to upgrade one Embedded Network Module

To use XMODEM to upgrade the firmware for a single Embedded Network Module that is not on the network:

1. Select a serial port at the local computer and disable any service which uses that port.
2. Connect the smart-signaling cable that came with the Embedded Network Module to the selected port and to the serial port at the uninterruptible power supply that contains the Embedded Network Module.
3. Run a terminal program (such as HyperTerminal), configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.
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 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 Embedded Network Module 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 (Embedded Network Module)" on page 188**.

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 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.

Index

Edition notice

Trademarks

IBM is a trademark of International Business Machines Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

APC, the APC logo, InfraStruXure, Matrix-UPS, PowerChute, PowerNet, and Smart-UPS are trademarks of American Power Conversion Corporation.

Other company, product, or service names may be the trademarks or service marks of others.

Part Number: *02R2721*