

Contents

Features of the System 1

Introduction	1
Battery Management Capabilities	2
System capacity 2	
Battery management features 3	
Network Management Features	4
Supported network management applications 4	
Supported Web browsers 5	

Getting Started 6

Initial Setup	6
Configuring TCP/IP settings 6	
Useful terms 7	

Accessing the User Interfaces 8

Access Procedures	8
Access priorities among the interfaces 8	
Access priority for logging on 8	
Web interface 9	
Control console interface 10	
SNMP interface 12	
Password-protected Accounts	13
Account types and access 13	
How to recover from a lost password 14	
Watchdog Features	16
Network interface watchdog mechanism 16	
Resetting the network timer 16	

Battery Management 17

Main Screen 17

General system information 17

Battery System and Device Manager Menus 19

Displaying data and alarms 19

Viewing details on alarms 22

Interpreting alarm details 23

Configuration menu 27

Calibration menu 29

Modbus 30

Reset Discharge Voltages 31

Reset Charge Current Deviation Benchmark 31

Network Menu 32

Access Restrictions and Menu Options 32

Access 32

Menu options 32

Option Settings 33

TCP/IP 33

DNS 37

Ping utility (control console) 38

FTP Server 39

Telnet/SSH 40

SNMP 47

Email 48

Syslog 49

Web/SSL 52

System Menu 61

Access Restrictions and Menu Options	61
Purpose and access	61
Menu options	62
Option Settings	63
User Manager	63
RADIUS	64
Identification	67
Date & Time	67
Tools	69
Preferences (Web interface)	71
Links (Web interface)	72
About System (control console)	73

Event-related Menus 74

Introduction	74
Overview	74
Menu options	75
Event Log	76
Overview	76
Logged events	76
Accessing the log	77
How to use FTP or SCP to retrieve log files	78
Actions Option (Web interface only)	81
Enabling and disabling event actions	81
Severity levels of events	81
Event Log action	81
SNMP Traps action	81
Email action	82
Related topics	82
Recipients Option	83
Trap Receivers	83
Email Recipients	84
Email Test	85

Email Option	86
Requirements for using SMTP	86
DNS servers	87
SMTP settings	87
How to Configure Individual Events	88
Options to configure individual events	88
Event list access	88
Event list format	89
Event mask settings	89
Event mask example	91
Management Card and Battery Manager Events	92
Event generation	92
Discharge cycle counter	92
Severity levels defined	93
Management Card events	94
Battery Management System events	97
Data Logging (Web interface)	99
Description	99
Configuration	100
Boot Mode	101
Introduction	101
Overview	101
DHCP & BOOTP boot process	102
DHCP Configuration Settings	104
Management Card settings	104
DHCP response options	106
Security	110
Security Features	110
Planning and implementing security features	110
Summary of access methods	110
Changing default user names and passwords	
immediately	112
Port assignments	112
User names, passwords, community names (SNMP)	113

Authentication 114
Authentication versus encryption 114

Encryption 115
Secure SHell (SSH) and Secure CoPy (SCP) 115
Secure Sockets Layer (SSL) 117

Creating and Installing Digital Certificates 119
Purpose 119
Choosing a method for your system 120

Firewalls 126

Using the APC Security Wizard 127

Overview 127
Authentication 127
Files you create for SSL and SSH security 129

Create a Root Certificate & Server Certificates 131
Summary 131
The procedure 132

Create a Server Certificate and Signing Request 137
Summary 137
The procedure 138

Create an SSH Host Key 142
Summary 142
The procedure 142

How to Export Configuration Settings 145

Retrieving and Exporting the .ini file 145
Summary of the procedure 145
Contents of the .ini file 146
Detailed procedures 147
The event and its error messages 150
Messages in config.ini 151
Errors generated by overridden values 151

Using the Device IP Configuration Wizard 152

APC Device IP Configuration Wizard 153

Purpose and Requirements	153
Purpose: configure basic TCP/IP settings	153
System requirements	153
Install the Wizard.	154
Download the wizard	154
Use the Wizard	155
Launch the Wizard	155
Configure the basic TCP/IP settings remotely	155
Configure or reconfigure the TCP/IP settings locally	157

File Transfers 158

Introduction	158
Overview	158
Upgrading Firmware	159
Firmware defined	159
Benefits of upgrading firmware	159
Obtain the latest firmware version	160
Firmware files (Battery Management System)	161
Firmware file transfer methods	162
Use FTP or SCP to upgrade one Battery Management System Management Card	163
Use FTP or SCP to upgrade multiple Battery Management System Management Cards	166
Use XMODEM to upgrade one Battery Management System Management Card	166
Verifying Upgrades and Updates	168
Overview	168
Last Transfer Result codes	168

Alarms 169

Fault Alarm Criteria	169
Alarm Relay and LED Operation	170

Troubleshooting 171

Management Card 171

Access problems (Battery Management System
Management Card) 171

SNMP issues (Battery Management System Management
Card) 173

Product Information 174

Limited warranty 174

Warranty limitations 174

Obtaining service (service contracts) 175

Life-Support Policy 176

General policy 176

Examples of life-support devices 176

Index 177

APC Worldwide Customer Support 186

Features of the System

Introduction

The APC Battery Management System provides automated monitoring of large battery systems that supply backup for 120-, 240-, and 480-volt power systems. The Battery Management System provides battery management for nominal 2 V, 4 V, 8 V, or 12 V lead-acid batteries; or 1.2 V or 2.4 V nickel-cadmium batteries.

The Battery Management System is controlled through a network interface provided by a Network Management Card built into the master controller (the first unit in a group of up to 6 total units). This card uses the open standards Telnet, SSH, HTTP, SSL, RS-485 Modbus, RS-232 serial connection, e-mail, and SNMP to manage the Battery Management System.



For more information see [Network Management Features](#) and [Network Menu](#).

Battery Management Capabilities

System capacity

Using the APC Battery Management System, you can monitor and maintain the batteries of one master unit and up to five expansion units, each unit handling up to 64 individual batteries.

Five battery management expansion units can be connected in a group to one master unit. The master unit provides the network connection through its built-in management card so that the entire group can be managed remotely through either one IP address or a serial connection.

The Battery Management System will support up to 244 lead-acid batteries or up to 375 nickel-cadmium batteries.



See also

To install and connect the system, see the *Installation and Quick Start* manual ([.\doc\en\insguide.pdf](#)), provided in Portable Document Format (PDF) on the APC Battery Management System *Utility* CD and in printed form.

Battery management features

The system enables you to do the following:

- Identify weak or defective batteries that need replacement.
- Optimize the charge state of batteries within a string by automated charging of individual batteries with a lower voltage. Charging these batteries causes the batteries with high voltage to normalize. All the batteries in the string become properly charged. This extends the useful life of overcharged batteries and achieves full capacity of undercharged batteries.
- Be alerted to alarm conditions that are displayed and logged to warn of battery system or Battery Management System conditions.

Network Management Features

Supported network management applications

An APC Network Management Card (AP9517SQD) is built into the master controller (AP9921X) that provides the network connection. It is the first battery management unit in a group of one master unit and up to 5 expansion units (AP9921XS).

The Battery Management System supports the following access methods:

Network Connection	Access	Description
Telnet & SSH	APC control console interface	A non-graphical interface through which you can configure network, system, and battery management parameters, and display and monitor battery management data.
HTTP & SSL	Web browser	A graphical user interface to the Battery Management System through a standard Web browser. With this Web interface, you can configure network, system, and battery management parameters, and display and monitor battery management data.
SNMP	MIB browser	Uses MIB II OIDs to configure the built-in management card, and use SNMP traps to report Battery Management System events.
FTP	Device IP Configuration Wizard	Consecutively discovers each unconfigured controller on the same network segment and enables you to configure its basic TCP/IP settings remotely.
Display interface (optional)	LCD display	Remote LCD interface through which you can configure network, system, and battery management data.

Supported Web browsers

As your browser, you can use Microsoft® Internet Explorer (IE) 5.x or Netscape® 7.x to access the Battery Management System through its Web interface. Other commonly available browsers also may work but have not been fully tested by APC.

Data verification, the event log, and the data log authentication require that you enable the following for your Web browser:

- JavaScript
- Java
- Cookies

In addition, the Battery Management System 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 Battery Management System.
- Configure the proxy server so that it does not proxy the specific IP address of the Battery Management System.

Getting Started

Initial Setup

Configuring TCP/IP settings

You must define three TCP/IP settings for the Battery Management System's built-in Management Card before the Battery Management System can be managed over the network:

- IP address of the Battery Management System
- Subnet mask
- IP address of the default gateway

Choose one of the following methods to configure the TCP/IP settings:

- With the Device IP Configuration Wizard, which you install from the CD. This method is available only for Windows[®] NT, Windows 2000, Windows 2003, and Windows XP.
- By a direct serial connection from the Network Configuration port on the controller to a serial port on your computer.
- Using ARP and Telnet, if your computer is on the same subnet as the Battery Management System.
- Through a BOOTP or DHCP server.



See also

For detailed instructions on these methods of configuring the TCP/IP settings, see “Quick Configuration” in the *Installation and Quick Start* manual ([.\doc\en\insguide.pdf](#)), provided in Portable Document Format (PDF) on the APC Battery Management System for High Voltage Applications *Utility* CD and in printed form.



To configure multiple Battery Management Systems, see [How to Export Configuration Settings](#).

Useful terms

Batteries: Single or multi-cell lead-acid or nickel-cadmium blocks that are connected together in series to create a string.

Battery Management System: One complete Battery Management System that is composed of one master unit and up to five expansion units.

Battery Management Unit: A single enclosure within a group of enclosures that operate together as a system.

Current acceptance: The amount of current that flows into an individual battery from the Battery Management System's electrically isolated DC boost supply.

Float charge: The power provided to a battery by the battery charger to sustain the charge.

Jar: An individual battery.

Management Controller: The Battery Management System and associated sensors, wiring, fuses, and cables.

Pilot battery: A single battery that is monitored as a representation of the entire string of batteries.

String current: The common current flowing through the string of batteries. The current polarity can be positive when flowing into the string, as during a charge, or negative when flowing from the string, as during a discharge. This current has the same value throughout the string.

Accessing the User Interfaces

Access Procedures

Access priorities among the interfaces

After the Battery Management System network settings are configured (as described in the *Installation and Quick Start Manual*), you can use the Battery Management System remotely through its Web, control console (Telnet or SSH), and SNMP interfaces.

Access priority for logging on

Only one user at a time can log on to the Battery Management System 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 Battery Management System always has the highest priority.
- Telnet or Secure SHell (SSH) access to the control console from a remote computer has priority over Web access.
- Web access, either directly or through the InfraStruXure Manager, has the lowest priority.



For information about how SNMP access to the Battery Management System is controlled, see [SNMP](#).

Web interface

To access and log on to the Battery Management System's Web interface:

1. In the URL Location field, do one of the following.
 - If the Battery Management System port is set to the default value of 80, type `http://` followed by the Battery Management System IP address. The following example shows a typical IP address:
`http://170.241.17.51` if HTTP is your access mode
`https://170.241.17.51` if HTTPS (SSL/TLS) is your access mode
 - If the Battery Management System Web port is set to a value other than the default of 80, enter the System IP address (the IP address of the Battery Management System) followed by a colon and the configured Web Port value (8000 in the following example):
`http://170.241.17.51:8000` if HTTP is your access mode
`https://170.241.17.51:8000` if HTTPS (SSL/TLS) is your access mode
 - If there is a DNS server entry for the Battery Management System, you can enter the DNS name. For example:
`http://DeviceNumber25` if HTTP is your access mode
`https://DeviceNumber25` if HTTPS (SSL/TLS) is your access mode
2. Respond to the **User Name** and **Password** prompts. The default Administrator user name and password are both **apc**, all lowercase.



Note

In the Web interface, data verification requires that you enable JavaScript or Java.

Control console interface

You can manage the Battery Management System through the control console, using either Telnet or the RS-232/485 port.

Structure. The control console provides menu options to manage the Battery Management System over the network.

To use an option, type its number and press ENTER.

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

While using a menu, you can also use the following keystrokes:

Keystrokes	Actions
Press ? and then ENTER	Provides brief menu option descriptions (if the menu has help available).
Press ENTER	Refreshes the menu.
Press ESC	Returns to the previous menu.
Press CTRL+C	Returns to the first menu.
Press CTRL+L	Accesses the Battery Management System event log.

Local access to the control console. You can use a local computer, a computer that connects to the Battery Management System through the serial port, to access the control console.

1. Select a serial port at the local computer and disable any service which uses that port.
2. Connect the serial cable (940-0103) that came with the Battery Management System to the RS-232/485 port on the Battery Management Unit and a serial port on your local computer.



Note

Modbus and the control console share a common serial port. You can use either one or the other to access the Battery Management System. If you reconfigure the DIP switches to switch from Modbus to the control console, you must restart the computer for the changed to take effect.



See also

If you are using Modbus to access the Battery Management System, you must configure the DIP switches. For DIP switch configuration, see "Configure the DIP Switches" in the *Installation and Quick Start Manual* ([.\doc\en\insguide.pdf](#)), provided in Portable Document Format (PDF) on the APC Battery Management System *Utility* CD and in printed form.

3. Run a terminal program (such as HyperTerminal) and configure the selected port for 9600 bps or 19200 (depending on the speed configured for Modbus), 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
4. Press ENTER twice to display the **User Name** prompt.
5. Enter your user name and password (**apc** by default).

Telnet. To access the Battery Management System's control console using Telnet:

1. Use the command `telnet` and the IP address of the Battery Management System. For example:

```
telnet 170.215.6.49
```
2. Press the ENTER key to open the Telnet session and display the **User Name** prompt.

Logging on. To log on to the control console, respond to the **User Name** and **Password** prompts. The default user name and password for the Administrator account are both **apc**, all lowercase. You can change the user name, password, and time-out values through the **System** menu.



See [User Manager](#).

SNMP interface

To use SNMP to configure the Management Card or to use the Battery Management System traps for event notification, you must use version 3.6.9 (or later) of the APC PowerNet MIB.



See also

See the APC MIB Reference Guide ([.\doc\en\mibguide.pdf](#)) provided on the APC Battery Management System *Utility*

CD.

Password-protected Accounts

Account types and access

The Battery Management System has three types of accounts, Administrator, Device Manager and Read-Only User.

- The Administrator account can use all the menus in the control console and in the Web interface. The default password and user name are both **apc**.
- The Device Manager account can use only the following menus:
 - In the Web interface, the **Battery System** menu and read-only access for the **Log** option of the **Events** menu.
 - In the control console, the **Device Manager** menu.The default user name is **device**, and the default password is **apc**.
- A Read-Only User has the following restricted access:
 - Access through the Web interface only.
 - Access to the same menus as a Device Manager, but without the capability to change configurations, control devices, or delete data. Links to configuration options may be visible but are 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 names and passwords for the three account types, see [User Manager](#).



Note

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

How to recover from a lost password

You can use a local computer that connects to the Battery Management System through the serial port on the rear of the master unit.

1. Select a serial port at a local computer, and disable any service that uses the port.
2. Reset the DIP switch #6 and #7 to the OFF position.
3. Use the configuration cable (APC part number 940-0103) to connect the selected port to the serial port on the rear panel of the master unit.



Note

Modbus and the control console share a common serial port. You can use either one or the other to access the Battery Management System. If you reconfigure the DIP switches to switch from Modbus to the control console, you must restart the computer for the changed to take effect



See also

If you are using Modbus to access the Battery Management System, you must configure the DIP switches. For DIP switch configuration, see “Configure the DIP Switches” in the *Installation and Quick Start Manual* ([.\doc\en\insguide.pdf](#)), provided in Portable Document Format (PDF) on the APC Battery Management System *Utility* CD and in printed form.

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



Note

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

5. 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 4.
 - The correct cable is being used as specified in step 3.
6. Press the RESET button on the rear panel of the master unit of the Battery Management System. The Status LED will flash alternately orange and green. Press the RESET button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
7. 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 6 and log on again.)
8. From the **Control Console** menu, select **System**, then **User Manager**.
9. Select **Administrator**, and change the **User Name** and **Password** settings, both of which are now defined as **apc**. Select **Accept Changes** to save your settings.
10. Press CTRL-C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.
11. Reset the DIP switches to the configuration you had prior to step 2. You must restart the Battery Management System if any changes are made to the DIP switches.

Watchdog Features

Network interface watchdog mechanism

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

Resetting the network timer

To ensure that the Management Card does not reboot if the network is quiet for 9.5 minutes, the Management Card attempts to contact the default gateway every 4.5 minutes. If the gateway is present, it responds to the Management Card, and that response restarts the 9.5-minute timer.

If your application does not require or have a gateway, specify the IP address of a computer that is running on the network most of the time and is on the same subnet. The network traffic of that computer will restart the seven-minute timer frequently enough to prevent the Management Card from rebooting.

Battery Management

Main Screen

General system information

When you log on to the Web interface or control console, the main screen provides basic information about the Battery Management System:

Information displayed in both interfaces. Both the Web and control console interfaces display the following information:

- **System Name**, **Contact**, and **Location** for the Battery Management System. To set these values, use the **Identification** option of the **System** menu.
- **Date** and **Time**: The date and time at which you logged on. To change the system date and time, use the **System** menu option, **Date & Time**.
- **User**: Whether you logged on as an Administrator, Device Manager, or Read-Only User.
- **Up Time**: How long the Management Card has been running since it was last turned on or reset.
- **Status**: The status of the master controller's built-in Management Card.



See also

For information on the display interface, see “How to use the display interface” in the *Installation and Quick Start Manual* ([.\doc\en\insguide.pdf](#)), provided in Portable Document Format (PDF) on the APC Battery Management System *Utility* CD and in printed form.

Information displayed in the control console only. The main screen of the control console displays the following additional information.

- **Version information:** (In the Web interface, select **About System** from the **Help** menu.)
 - **Battery Manager III APP:** The version of the application (APP).
 - **Network Management Card AOS:** The version of the APC operating system (AOS) of the master unit's built-in management card.
- **Status:** The status of the master unit's built-in Management Card.



Note

The status codes are displayed in the control console only.

P+	The APC operating system (AOS) is functioning properly.
N+	The network is functioning properly.
A+	The application firmware is functioning properly.
A-	The application firmware has a bad checksum.
A?	The application firmware is initializing.
A!	The application firmware is not compatible with the AOS.



Note

If you can access the control console through Telnet, the AOS reports P+, and the network reports N+.

Battery System and Device Manager Menus

Displaying data and alarms

You can display battery information and view alarms and their causes in the Web interface, control console, or display interface.

To configure values related to the batteries, such as changing the threshold values that define whether data are in-range (OK) or out-of-range (Alarm), you can use either the Web interface or the control console.



See [Configuration menu](#).

Web interface.

The screenshot shows the APC Battery Manager web interface. On the left is a dark blue navigation menu with the following items: Battery Manager, IP: 159.215.87.51, Battery System, Events, Data, Network, System, Logout, Help, and Links. The Links section includes APC's Web Site, Testdrive Demo, and APC Monitoring. The main content area has a blue header with the APC logo and a 'Summary' link with a green checkmark. Below the header, the 'Status' section shows 'Battery Management System' with four items: Environment, Charger, Batteries, and Management Controller, each followed by a green checkmark. A 'Configure Auto-Refresh Frequency For This Page' link is visible. The 'Reset Annunciators' section contains a button and a description: 'This feature will reset any annunciator devices connected to the 'Beacon' or 'Alarm Contact' ports.' The '10/100 Management Card Status' section displays the following information: Name: BMSHVA III, Date: 01/14/2005, Contact, Time: 10:30:48, Location, User: Administrator, UpTime: 0 Days 20 Hours 57 Minutes, and Status: OK.

Alarm category	Alarms reported	Data causing the alarm
Environment	Ambient Temperature	The air temperature in the battery environment
Charger	String Voltage	The voltage (VDC) of an entire battery string, discharge, and high pilot temperature.
Batteries	Discharge Test	The lowest voltage (VDC) of individual batteries recorded during the last discharge
	Charge Test	The response of individual batteries to a boost charge
	Pilot Temperature	The surface temperature of the battery to which the pilot temperature sensor is attached
Management Controller	Blown Fuse/ Connections	No voltage is sensed from one or more batteries.

Control console.

You can use the control console to display battery information and alarms.



See [Web interface](#).

To display battery data and active alarms:

1. On the main screen of the control console, identify the battery string about which you want to display information. For each battery string a hyphen (-) indicates no alarms, W indicates a warning condition, and S indicates a severe condition.
2. Select **Device Manager**.
3. Select **String Details**.
4. Type the number for the data category.

Viewing details on alarms

You can display detailed information on active alarms for any battery string. The alarm message text displayed for a category indicates which alarm details to select.



Note

Silcon battery systems have a maximum of two strings.

All other battery systems have only one string.

Web interface example.

1. On the main screen, the Charger column for a battery string displays a red **ALARM** icon. Click on that icon or on the **String Details** option in the **Battery System** menu to display the **String Details** screen.
2. For the battery string, the alarm message text is `String voltage is high`. Under **Individual Battery Details**, click on **Voltage** (the reason for the alarm).

Control console example.

1. On the main screen, the **Charger** row in the column for the battery string displays S, indicating an active severe alarm for the category.
2. From the control console main screen, type 1 to select the **Device Manager** menu.
3. For the battery string, the alarm message text is `String voltage is high`. Type 1, for **Battery Voltage** (the reason for the alarm).

Interpreting alarm details

For an alarm category:

- The Web interface displays detailed alarm data and any configured threshold values on a single page. For the three types of battery alarms, bar graphs are displayed. To view or change the threshold values, you must use the **Configuration** menu option of the **Battery System** menu in the Web interface.
- The control console displays detailed alarm data through numbered menus.
 - Values below the low threshold are indicated by the < character, and values above the high threshold are indicated by the > character.
 - To view or change the threshold values, select **Device Manager** and then select **String Details** in the control console.



See [Configuration menu](#) to configure alarm details.

Environment alarms.

Category	Details	Diagnostics
Ambient Temperature	<p>The air temperature in the battery string environment is above or below configured thresholds.</p> <p><i>Default:</i></p> <p>50.0° F (10° C): low threshold</p> <p>95.0° F (35° C): high threshold.</p>	<p>Problem:</p> <ul style="list-style-type: none"> • Uncorrected high temperature can cause permanent damage to the batteries. • Uncorrected low temperature can cause a reduction in battery runtime. <p>Response: Check temperature control and ventilation systems in the room, and check for overheated batteries (usually caused by overcharging).</p>
Input Contacts	<p>Activation of input contacts triggers an alarm.</p>	<p>Check the status of the external monitoring device that sent the input signal.</p>

Charger alarms.

Category	Details	Diagnostics
String Voltages	The voltage of a battery string is above or below the threshold.	<p>Problem: High or low string voltage indicates that the string charger may be defective or improperly adjusted. If uncorrected, this condition can cause permanent damage to the batteries.</p> <p>Response: Adjust the DC string-charging voltage to the proper setting.</p>
String Current	The BMS has detected a sufficient flow in the discharge direction to indicate a loss of the charger value.	Investigate the loss of power to the charger and restore it as soon as possible.
Ripple Current	The detected ripple current exceeds the alarm threshold.	Investigate the source of high AC current in the charger output.

Battery alarms.

Category	Details	Diagnostics
Discharge Test	The voltage of individual batteries listed in the alarm text dropped below the configured minimum threshold during the last discharge.	<p>Problem: Recorded voltage below the minimum threshold indicates a battery that will not perform adequately in providing system backup in relation to others in the same string.</p> <p>Response: Replace failed batteries immediately so that system backup time is not reduced.</p>

Category	Details	Diagnostics
Charge Test	When the Battery Management System applied a test current, the batteries listed in the alarm message showed a higher than acceptable percentage deviation from the previous "benchmarked" values (which are reset after any discharge).	<p>Problem: A percentage deviation outside the acceptable range indicates unexplained changes that indicate the need to verify possible problems with the battery.</p> <p>Response: Identify the listed batteries immediately so that system backup time is not reduced. Test and verify status of the identified batteries immediately.</p>
Pilot Temperature s	<p>Sampling of the surface temperature of one battery in the string showed a temperature above the configured threshold.</p> <p><i>Default:</i> 95° F (35° C) (high threshold).</p>	<p>Problem: A high temperature alarm may indicate an overheated (overcharged) battery, usually caused by a faulty charger.</p> <p>Response: If uncorrected, this condition can cause permanent damage to the batteries. Replace failed batteries.</p>

Management Controller alarms.

Category	Details	Diagnostics
Blown Connection Fuse	The connections between the Management Controller and the batteries are open.	<p>Problem: One or more fuses or wires are open.</p> <p>Response: Replace the fuse or wire connection in the location indicated in the event log.</p>
Missing or Defective Sensors	Not all sensors are present and functional.	<p>Problem: The system operation is not reliable without sensor information.</p> <p>Response: Connect or replace the sensor indicated in the event log.</p>

Category	Details	Diagnostics
Monitor Relay Stuck	A relay is stuck in the master unit.	Reset the unit using the recessed reset button on the back of the master unit. If problem persists, contact APC Customer Support at the phone number located at the end of this manual.
Communication	One or more units are not reporting to the master unit.	Problem: The system cannot perform operations on all configured batteries. Response: Check that the cables on the expansion ports are in place and that the DIP switches are set correctly.

Configuration menu

Battery Type Selection. Choose nickel-cadmium or lead-acid batteries.

Battery Configuration.

Charger Type (Silcon/ Other)	A Silcon unit can have two strings per battery management master unit. Other requires a battery management master unit for each new string.
Number of Strings	The number of strings in the system. Silcon may have two battery strings, all other systems will have one.
Number of Batteries per String	The number of batteries in each string in the system. The maximum number of batteries per string is 244 lead-acid batteries or 375 nickel-cadmium batteries for a non-APC Silcon UPS..
Number of Cells per Battery	The number of cells per battery for nickel-cadmium batteries is 1 or 2. The number of cells per battery for lead-acid batteries is 1, 2, 4, or 6.
Monitor Wire Length	Choose either >50 feet or <50 feet.
Cell Max Voltage Limit	The maximum recommended voltage per individual battery cell. This number multiplied by the total number cells in a string equals the alarm value for the string. A charger alarm occurs if the string voltage exceeds the alarm value.
Cell Min Voltage Limit	The minimum recommended voltage per individual battery cell. This number multiplied by the number of total cells in a string equals the alarm value for the string. A charger alarm occurs if the string voltage falls below the alarm value.
Battery Capacity	Enter battery capacity in amp-hours for reference. The amp-hour capacity of a battery should be clearly marked on the actual battery.

Temperature Configuration.

Maximum Pilot Temperature Limit	The maximum surface temperature of the pilot battery in the string (the battery to which the pilot temperature sensor is attached). Because the Battery Management System equalizes the charge for all batteries in the string, the temperature of the pilot battery is likely to be typical of other batteries in the string. For example, an overheated pilot battery would probably indicate overcharging throughout the string.
Maximum Ambient Temperature Limit	The maximum and minimum allowable temperature of the air surrounding the batteries. See the specifications for your batteries before changing this value.
Minimum Ambient Temperature Limit	

Alarm Configuration.

Ripple Current Limit	Ripple current limit is the allowable AC measurement in the battery string. The default setting is 5 A for every 100 amp-hour of capacity.
Charge Current Limit	Percentage of change in the response current measurement that is allowed before an alarm is indicated.
Discharge Voltage Limit	The percentage of the lowest individual battery discharge voltage that is allowed relative to the other batteries in the string.
Automatic Annunciator Reset	When enabled, the external annunciator devices will reset automatically when the condition of an alarm clears. When disabled, the alarm must be reset manually.

Calibration menu

Select to calibrate either a **String** or a **Unit**.

String. Select the string you wish to calibrate.

String X	Each string will be listed. Select the string you wish to configure
Ohmic Correction	Set the overall Ohmic Correction value.

Unit. Select the unit you wish to calibrate.

Unit X (Web interface)	Each unit will be listed.
DC Voltage Zero	Set to zero with no string current.
DC Voltage Span	Set to 100, 200, 500, or 1000 A full scale.
AC Ripple Zero	Set to zero with no string current.
Ohmic Correction	Set to match calibrated instrument.
Current Sensor Range	Set to 100, 200, 500, or 1000 A full scale, based on current sensor specifications.
DC Current Sensor Zero	Set to zero with no string current.
AC Current Sensor Zero	Set to zero with no string current.
Tier Ohmic Value	Enter milliohms of cables and connectors within the string to match calibrated instrument.

Modbus

Modbus lets you view the Battery Management System through your building management services interface. It is read-only.

The Modbus interface supports 2-wire RS-485 with the following pin-out:

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

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

- Select **Modbus** from the **Battery System** menu.
- Enter your settings.

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

- Select **Device Manager**.
- Select **Modbus**.
- Enter your settings, including the baud rate at which your Modbus is operating, either 9600 or 19200.

To use Modbus, do the following:

- Configure the DIP switches for Modbus operation.



See also

To configure the DIP switches, see the Battery Management System *Installation and Quick Start* Manual ([.\doclen\insguide.pdf](#)), provided on the APC Battery Management System *Utility* CD.



See also

The data that is available through the Modbus interface is defined in a spreadsheet ([.\doclen\AP9920_MBRegMap_xx.xls](#)) provided on the APC Battery Management System *Utility* CD.

Reset Discharge Voltages

Reset Lowest Discharge Voltages (control console). The lowest discharge voltage is the lowest voltage measured for each battery in a string during discharge. To clear the stored lowest discharge voltage:

1. Select **Device Manager**
2. Select **Reset Discharge Voltages**
3. Select **Reset Lowest Discharge Voltages**

Reset Lowest Discharge Voltages (Web interface). Select this option from the **Detailed Status** menu of the **Battery Management System** menu.

Reset Charge Current Deviation Benchmark

Reset Charge Current Deviation Benchmark (control console). The response benchmark indicates the condition of the battery and the connections to it. It is established when the system is commissioned, when the batteries are replaced, or after a discharge.

1. The response benchmark is automatically cleared during a discharge. To clear the stored response benchmark value and force it to be reset, select **Device Manager**
2. Select **Reset Response Benchmark**
3. Select **Reset Lowest Response Benchmark**

Reset Charge Current Deviation Benchmark (Web interface). Select this option from the **Detailed Status** menu of the **Battery Management System** menu.

Network Menu

Access Restrictions and Menu Options

Access

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

Menu options

To use the **Network** menu options to configure the network settings of the Battery Management System, see the following descriptions:

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

Option Settings

TCP/IP

This option accesses the following settings:

- **Boot mode setting:** Selects the method used to define the TCP/IP values that a Battery Management System needs to operate on the network:
 - **System IP:** The IP address of the Battery Management System
 - **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](#).



See also

To configure the initial TCP/IP settings when you install the Battery Management System, see the Battery Management System *Installation and Quick Start* Manual ([.\doc\en\insguide.pdf](#)), provided on the APC Battery Management System *Utility* CD and in printed form.

- **Advanced settings:** Defines the Battery Management System's host and domain names, as well as Ethernet port speed, BOOTP, and DHCP settings used by the Battery Management System.

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

Boot mode setting. This setting selects which method will be used to define the Battery Management System's TCP/IP settings whenever the Battery Management System 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 Battery Management System 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 Battery Management System.



For information about the **After IP Assignment** setting and other settings that affect how the Battery Management System uses BOOTP and DHCP, see [Advanced settings](#); for more information on how to use DHCP, see [Boot Mode](#).

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

- Two settings are available for all **Boot mode** selections to define the Battery Management System's **Host Name** and **Domain Name** values.
 - **Host Name:** When an Administrator configures a host name here and a domain name in the **Domain Name** field, users can then enter a host name in any field in the Battery Management System 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 Battery Management System interface (except e-mail addresses) that accept domain names, the Battery Management System 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 Battery Management System recognizes a host name with a trailing period (such as `mySnmpServer.`) as if it were a fully qualified domain name and therefore does not append the domain name.
- A **Port Speed** setting is available for all **Boot mode** selections to define the TCP/IP port's communication speed (**Auto-negotiate**, by default).

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



Caution

If the **Client ID** is changed from the Battery Management System master unit's MAC address, the new value must be unique on the LAN. Otherwise, the DHCP or BOOTP server may act incorrectly.

- **User Class**: Uses the Battery Management System's application firmware module type, by default. For example, a Battery Management module sets the **User Class** to **BMS-HVA**.
- Two settings are available if **BOOTP only** is the Boot mode selection:
 - **Retry Then Fail**: Defines how many times the Battery Management System 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 Battery Management System when it fails to discover a BOOTP server (**Use Prior Settings**, by default).



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

DNS

Use this option to define the IP addresses of the primary and secondary Domain Name System (DNS) servers used by the Battery Management System's e-mail feature. The primary DNS server will always be tried first.



See [Email Recipients](#) and [DNS servers](#).

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

Use the 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** text field to identify the value to be used for the selected **Query Type**:
 - For **Host**, identify the URL.
 - For **IP**, identify the IP address.
 - For **FQDN**, identify the fully qualified domain name, formatted as *myserver.mydomain.com*.
 - For **MX**, identify the Mail Exchange address.

- Enable or disable **Reverse DNS Lookup**. This feature is disabled by default. Enabling this feature is the recommended configuration, 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 both the IP address and the domain name for the networked device associated with the event in the event log. If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change 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 Battery Management System's network connection 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**) 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. To configure SSH, see [Telnet/SSH](#). If you decide to use SCP for file transfer, be sure to disable the FTP server.



To configure SSH, see [Telnet/SSH](#). If you decide to use SCP for file transfer, be sure to disable the FTP server.

Use the **Port** setting to identify the TCP/IP port that the FTP server uses for communications with the Battery Management System. The default **Port** setting is **21**.

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

```
ftp 159.215.12.114:5000
```



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

Telnet/SSH

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

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



Note

When SSH is enabled and its port and encryption ciphers 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 APC Security Wizard and load it to the Battery Management System.



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 location **/sec** on the Battery Management System.

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



Note

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

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

Option	Description
Telnet/SSH Port Configuration	
Telnet Port	<p>Identifies the TCP/IP port used for communications by Telnet with the Battery Management System. The default is 23.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings. Then, according to the requirements of your Telnet client program, you must use either a colon (:) or a space in the command line to specify the non-default port number. For example, for a port number of 5000 and a Battery Management System IP address of 159.215.12.114, your Telnet client would require one or the other of the following commands:</p> <pre data-bbox="728 630 1201 699">telnet 159.215.12.114:5000 telnet 159.215.12.114 5000</pre>
SSH Port	<p>Identifies the TCP/IP port used for communications by the Secure SHell (SSH) protocol with the Battery Management System. The default is 22.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings. See the documentation for your SSH client for information on the command line format required to specify a non-default port number when starting SSH.</p>

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

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

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

SNMP

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

To define up to four NMSs as trap receivers, see **Trap Receivers**; to use SNMP to manage a UPS or an environmental monitor, see the *PowerNet[®] SNMP Management Information Base (MIB) Reference Guide (.\\doc\\en\\mibguide.pdf)* on the APC Battery Management System *Utility* CD.



Setting	Definition
Community Name	This setting defines the password (maximum of 15 characters) which an NMS that is defined by the NMS IP setting uses to access the channel.
NMS IP/ Domain Name	Limits access to the NMS specified by a domain name or to the NMSs specified by the format used for the IP address: <ul style="list-style-type: none">• A domain name allows only the NMS at that location to have access.• 159.215.12.1 allows only the NMS with that IP address to have access.• 159.215.12.255 allows access for any NMS on the 159.215.12 segment.• 159.215.255.255 allows access for any NMS on the 159.215 segment.• 159.255.255.255 allows access for any NMS on the 159 segment.• 0.0.0.0 or 255.255.255.255 allows access for any NMS.

Setting	Definition	
Access Type	Selects how the NMS defined by the NMS IP setting can use the channel, when that NMS uses the correct Community Name .	
	Read	The NMS can use GETs at any time, but it can never use SETs.
	Write	The NMS can use GETs at any time, and can use SETs when no one is logged on to the control console or Web interface.
	Disabled	The NMS cannot use GETs or SETs.
	Write+	The NMS can use GETs and SETs at any time, even when someone is logged on to the control console or Web interface.

Email

Use the **Email** option to do the following:

- Define the SMTP server.



See [SMTP settings](#).

- Configure e-mail recipients.



See [Email Recipients](#).



Note

In the Web Interface, you can click the link **Configure the Email Recipients** on the page displayed by the **Email** option, or go directly to the **Recipients** option of the **Events** menu.

Syslog

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

Syslog (and the event log) will also record discharge events including:

- Discharge time and date
- Discharge ambient and pilot battery temperature
- Discharge measured current
- Amp-hours removed from battery during discharge



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 assigned to the Battery Management System's Syslog messages (User , by default). 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 the Battery Management System.

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

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

1. Select the priority 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** below. For example, `APC: Test message`, meets the required message format.
3. Click **Apply** to have the Battery Management System send a Syslog message that uses the defined **Priority** and **Test Message** settings.

Syslog message format. A Syslog message has three parts:

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

Web/SSL

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

- Enable or disable the two protocols that provide access to the Web interface of the Battery Management System:
 - 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 Socket Layer (HTTPS). Secure Sockets Layer (SSL) encrypts user names, passwords, and data during transmission and provides authentication of the Battery Management System by means of digital certificates.



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

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



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 Battery Management System creates one when it reboots. **The Battery Management System can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.**

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

Option	Description
Web/SSL Network Configuration	
Access	Enables or disables the access method selected in Protocol Mode .
Protocol Mode	<p>Choose one of the following:</p> <ul style="list-style-type: none"> • HTTP: User names, passwords, and data are transmitted without encryption. • HTTPS (SSL): User names, passwords and data are transmitted in encrypted form, and digital certificates are used for authentication. <p>NOTE: To enable HTTPS (SSL), change the setting and then click Next>> in the Web interface, or choose Accept Changes in the control console. You must then agree to the license agreement that is displayed. To activate the changes you must log off and log back on to the interface. When SSL is activated, your browser displays a lock icon, usually at the bottom of the screen.</p> <div data-bbox="778 751 869 824" style="text-align: center;">  </div>

Option	Description
HTTP/HTTPS Port Configuration	
HTTP Port	<p>Identifies the TCP/IP port used for communications by HTTP with the Battery Management System. The default is 80.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings.</p> <p>You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 5000 and a Battery Management System IP address of 171.215.12.114, you would use this command:</p> <pre>http://171.215.12.114:5000</pre>
HTTPS Port	<p>Identifies the TCP/IP port used for communications by HTTPS with the Battery Management System. The default is 443.</p> <p>You can change the Port setting to the number of any unused port between 5000 and 32768 to enhance the protection provided by User Name and Password settings.</p> <p>You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 6502 and a Battery Management System IP address of 171.215.12.114, you would use this command:</p> <pre>https://171.215.12.114:6502</pre>

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

Option	Description
SSL Server Certificate	
Status:	<p>The Status field indicates whether a server certificate is installed. (To display the status in the control console, choose Web/SSL, then Advanced SSL Configuration.)</p> <ul style="list-style-type: none"> • Not installed: No certificate is installed on the Battery Management System. <p>NOTE: If you install a certificate by using FTP or SCP, you must specify the correct location (/sec) on the Battery Management System.</p> <ul style="list-style-type: none"> • Generating: The Battery Management System is generating a certificate because no valid certificate was installed. • Loading: A certificate is being loaded (activated on the Battery Management System). • Valid: A valid certificate was installed to or generated by the Battery Management System. (If you install an invalid certificate, the Battery Management System discards it and generates a valid one. However, a certificate that the Battery Management System generates has some limitations. See Method 1: Use the Battery Management System's auto-generated default certificate.)

Option	Description
SSL Server Certificate	
Filename:	<p>You can create a server certificate with the APC Security Wizard and then upload it to the Battery Management System by using the Web interface. Use the Browse button for the Filename field to locate the file, then click Apply. By default, the certificate is installed to the correct location.</p> <p>Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Battery Management System. However, you must specify the correct location (/sec) on the Battery Management System.</p> <p>NOTE: Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL). If no server certificate is loaded when you enable HTTPS (SSL), the Battery Management System creates one when it reboots. The Battery Management System can take up to 5 minutes to create this certificate, and the SSL server is not available during that time.</p>

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

Parameter	Description
Fingerprint:	<p>Each fingerprint is a long string of alphanumeric characters punctuated by colons. A fingerprint is a unique identifier that you can use to further authenticate the server. Record the fingerprints to compare with the fingerprints contained in the certificate, as displayed in the browser.</p> <ul style="list-style-type: none">• 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.

System Menu

Access Restrictions and Menu Options

Purpose and access

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 Battery Management System's real-time clock with a Network Time Protocol (NTP) server.
- Reset or restart the Battery Management System interface.
- Define the URL links available in the Web interface.
- Set the units (Fahrenheit or Celsius) used for temperature displays.
- Access hardware and firmware information about the Battery Management System.
- Download firmware files (control console only).
- Upload user configuration files to the Battery Management System (control console only).



Note

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

Menu options

See the following descriptions of the settings available from the **System** menu options:

- User Manager
- RADIUS
- Identification
- Date & Time
- Tools
- Preferences (Web interface)
- Links (Web interface)
- About System (control console)

Option Settings

User Manager

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

Setting	Definition
Auto Logout	Defines (in minutes) how long you can be inactive while logged on to the control console or Web interface before you are logged off automatically (3 minutes by default). NOTE: You can bypass the auto-logout feature of the Battery Management System by configuring the auto-refresh feature to keep the screen active.
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 (10 characters or less) always used to log on to the control console. (apc is the default for the Password settings for the three account types.) NOTE: A Read-Only User cannot log on through the control console.

RADIUS

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

When a user accesses the Battery Management System, an authentication request is sent to the RADIUS server to determine the user's permission level.



Note

RADIUS user names are limited to 32 characters.



For more information on user permission levels, see [Account types and access](#).



Note

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

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

Configuring the RADIUS server. You must configure your RADIUS server to work with the Battery Management System. The following example is specific to APC's RADIUS server.

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

Identification

Use this option to define the **System Name**, **Location**, and **Contact** values used by the SNMP agent for the management card that is built into the master controller of the Battery Management System. The values defined here are used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifications (OIDs).



For more information about the MIB-II OIDs, see the PowerNet® *SNMP Management Information Base (MIB) Reference Guide* (`.\doc\en\mibguide.pdf`) provided on the APC Battery Management System *Utility CD*.

Date & Time

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

Set Manually. Use this option in the Web interface, or **Manual** in the control console, to define the date and time for the Battery Management System.



Note

An **Apply Local Computer Time to System** 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 Battery Management System 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 Battery Management System's time zone.
Update Interval	Defines how often, in hours, the Battery Management System 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 Battery Management System, 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 Battery Management System.
Reset to Defaults	Resets all configuration settings. NOTE: For information about how this affects the Boot mode setting, see this table's description of Reset Only TCP/IP to Defaults .
Reset to Defaults Except TCP/IP	Resets all configuration settings except the TCP/IP settings.
Reset Only TCP/IP to Defaults	Resets the TCP/IP settings only. NOTE: With Boot mode set to DHCP & BOOTP , its default setting, the Battery Management System's TCP/IP settings must be defined by a DHCP or BOOTP server. See TCP/IP .
Delete SSH Host Keys and SSL Certificates	Removes any SSH host key and server certificate on the Battery Management System 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 Battery Management System master controller to the current Battery Management System master controller, export the .ini file from the configured Battery Management System, select the **Tools** menu on the current Battery Management System, browse to the file, and click **Upload**. The current Battery Management System imports the file and uses it to set its own configuration. The **Status** field reports the progress of the upload.



See [How to Export Configuration Settings](#) for information on the content of the .ini file, how to preserve comments you add to the file, and how to export settings to multiple Battery Management System master controllers.

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 Battery Management System.

Option	Description
XMODEM	Allows you to transfer either an .ini file or a firmware upgrade file to a Battery Management System master controller using a terminal-emulation program only when you use a local connection to the control console. To connect to the control console locally, see Local access to the control console .
FTP Client	Use one of these two options to transfer either an .ini file or a firmware upgrade file from an FTP or TFTP server of your organization (company, agency, or department) to the current Battery Management System. These options assume that your organization has a centralized system for configuring or upgrading APC Management Cards (such as the one contained in the Battery Management System's master unit). 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 Battery Management System transfers the file.
TFTP Client	



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

Preferences (Web interface)

Use this option to select either Fahrenheit or Celsius for the Battery Management System's temperature display.

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: <ul style="list-style-type: none">• http://www.apc.com (APC's Web Site)• http://testdrive.apc.com (Testdrive Demo)
Access Links	
APC Home Page	Defines the URL address used by the APC logo at the top of all Web interface pages (by default, http://www.apc.com).

About System (control console)

This option identifies hardware information for the Management Card, including **Model Number**, **Serial Number**, **Manufacture Date**, **Hardware Revision**, **MAC Address**, and **Flash Type**. The hardware information will never change.

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



Note

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

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](#) and [Options to configure individual events](#).

- 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.
 - Use CTRL-L to access the event log from any menu.



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

- [Event Log](#)
- [Actions Option \(Web interface only\)](#)
- [Email Recipients](#)
- [Email Option](#)
- [How to Configure Individual Events](#)

Event Log

Overview

The Battery Management System supports event logging.

Use any of the following to view the Event Log:

- Web interface
- Control console
- FTP
- SCP
- Display interface

Logged events

The event log records normal and abnormal Management Card (system) events and Battery Management events. Any conditions that cause an SNMP trap, except for SNMP authentication failures, are logged as events. The event log will also log information regarding discharge events by the Battery Management System.

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



For a list of all events, see [Management Card events](#) and [Battery Management System events](#).

Accessing the log



Note

The Web interface and control console display events in the event log in reverse chronological order.

To view or clear the Battery Management System's event log, use the Web interface, control console, or FTP.

Web interface. To display the events in reverse chronological order, use the **Log** option in the **Events** menu.

To clear all events from the log, use the **Delete Log** button.

Control console. Use the control console over the network (using Telnet) to do the following:

- To display the event log, in reverse chronological order, press CTRL+L.
- To scroll through the events, use the space bar.
- To clear all events from the log, type `d` and press ENTER while viewing the log.

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-delimited 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 and 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 Battery Management System
 - The unique **Event Code** for each recorded event (*event.txt* file only)



Note

The Battery Management System 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** 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 file. To use SCP to retrieve the *event.txt* file, use the following command:

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

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

1. At a command prompt, type `ftp` and the Battery Management System's IP address, 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](#).

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 for **User Name** and **Password**.
 - For Device Manager, **device** is the default for **User Name**, and **apc** is the default for **Password**.
3. Use the **get** command to transmit the text version of the event log or data log to your local drive.

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

or

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

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

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

or

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

You will not be asked to confirm the deletion.

- If you clear the data log, the event log records a deleted-log event.
 - If you clear the event log, a new *event.txt* file is created to record the deleted-log event.
5. Type `quit` at the `ftp>` prompt to exit from FTP.

Actions Option (Web interface only)

Enabling and disabling event actions

Use the **Actions** option of the **Events** menu to enable or disable the following for events that have a specified severity level:

- Events Log
- SNMP Traps
- Email

Some Management Card (system) events do not have a severity level, and you cannot disable actions for those events.

Severity levels of events

All Battery Management System events and some Management Card events have a default severity level of Severe, Warning, or Informational.



See [Severity levels defined](#).

To use an evntlist.htm page to change the default severity level of an event, see [Event list access](#).

Event Log action

Disable this action to prevent the logging of all events that have a severity level. By default, all events are logged.

SNMP Traps action

By default, the **SNMP Traps** action is enabled for all Battery Management System events and for Management Card events that have a severity level (Informational, Warning, or Severe).

To use SNMP traps for event notifications, you must first identify the trap receivers (up to four) by their specific IP addresses.



See [Trap Receivers](#).

Email action

By default, the Email action is enabled for severe events only. To use e-mail for event notification, you must first define the e-mail recipients.



See [Email Recipients](#).

Related topics



See [Management Card events](#) and [Battery Management System events](#) for a description and the default severity level (if any) for each event.

Recipients Option

Trap Receivers

You can define up to four NMSs to be used as trap receivers when an event occurs that has SNMP traps enabled.

In the Web interface, use the **Trap Receiver** settings, available through the **Recipients** option of the **Events** menu.

In the control console, use the **SNMP** option of the **Network** menu.

Item	Definition
Community Name	The password (15 characters or less) 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 to which traps are sent. If this setting is 0.0.0.0 (the default), no traps are 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 Recipients

To identify up to four e-mail recipients to be notified of events, use one of the following:

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

Setting	Description
To Address	<p>Defines the user and domain names of the recipient.</p> <p>To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, myacct100@skytel.com). The pager gateway pages the recipient.</p> <p>Note: The recipient's pager must be able to use text-based messaging.</p>
Send via	<p>Selects one of the following methods for routing e-mail:</p> <ul style="list-style-type: none">• Through the Battery Management System's SMTP server (the recommended option, Local SMTP Server). E-mail is sent before the Battery Management System's 20-second timeout, and, if necessary, is retried several times.• Directly to the recipient's SMTP server (the Recipient's SMTP Server option). On a busy remote SMTP server, the timeout may prevent some e-mail from being sent, and with this option, the Battery Management System tries to send the e-mail only once. <p>When the recipient uses the Battery Management System's SMTP server, this setting has no effect.</p>
Email Generation	<p>Enables (by default) or disables sending e-mail to the defined recipient.</p>

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

- Make sure that forwarding is enabled at that server so that the server can route e-mail to external SMTP servers. (See your SMTP server's administrator before changing the configuration of your SMTP server.)
- Set up a special e-mail account for the Battery Management System. This account then forwards the e-mail to an external account.

Email Test

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

Email Option

Requirements for using SMTP

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

- The IP address of the domain name service (DNS) server.
- The DNS name of the SMTP server and the **From Address** settings for SMTP.
- The e-mail addresses for a maximum of four recipients.



Note

To page an e-mail recipient who uses a text-based pager gateway, see the description of the **To Address** setting in **Email Recipients**.

DNS servers

The Battery Management System cannot send any e-mail messages unless at least the IP address of the primary DNS server is defined.



See [DNS](#).

The Battery Management System 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 Battery Management System 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 Battery Management System, or on a nearby segment (but not across a wide-area network).

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 the computer.

SMTP settings

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

Setting	Description
SMTP Server	The DNS name of the SMTP server.
From Address	The contents of the From field in the e-mail messages sent by the Battery Management System. Note: See the documentation for your SMTP server to determine whether you must use a valid user account on the server for this setting.

How to Configure Individual Events

Options to configure individual events

You can configure individual events using the eventlist.htm page. See [Event list access](#).



To configure the actions for events based on their default severity levels instead of individually, see [Actions Option \(Web interface only\)](#).

Event list access

To access the event list, add /evntlist.htm to the Battery Management System's URL address value (IP address or DNS name). You can access the event list directly from the Web interface menus by selecting **Actions** from the **Events** menu.

- For an IP address of 149.205.12.114, and the default TCP port of 80, the URL is:
`http://149.205.12.114/evntlist.htm`
- For an IP address of 149.205.12.114, and a TCP port other than 80 (in this example, 5000), the URL is:
`http://149.205.12.114:5000/evntlist.htm`
- For a DNS name of writers, the URL is:
`http://writers/evntlist.htm`

Event list format

The evntlist.htm page defines the following for each event:

- **Code:** The event's unique event code.
- **Description:** The text used for the event.
- **Severity:** The event's default severity level.
- **Configuration:** The hexadecimal code that defines the actions to occur for the event and provides a link to the event mask that you use to configure the event.



See [Event mask settings](#).

Event mask settings

From the evntlist.htm page, to reconfigure actions for an event:

1. Click the link (the current hexadecimal code) for the event.
2. Enter a new hexadecimal code as an event mask to reconfigure the bits that control the actions for the event.
3. Click **Apply**.

The bits are numbered 0 to 23, from left to right.



Note

Bit 5 and bits 14 through 23 are unused. Make sure these bits are always set to 0.

Bits 0 to 3. These bits represent the event's severity:

Settings for Bits 0 to 3	Severity
0000	No severity
0001	Informational
0010	Warning
0011	Severe

Bit 4 and bits 6 to 9. These bits enable (1) or disable (0) event logging and trap receivers for the event:

Bit number	Action enabled or disabled for the event
4	Logging the event.
6	Sending traps to Trap Receiver 1
7	Sending traps to Trap Receiver 2
8	Sending traps to Trap Receiver 3
9	Sending traps to Trap Receiver 4

Bits 10 to 13. These bits enable (1) or disable (0) e-mail recipients for the event:

Bit number	Action enabled or disabled for the event
10	Sending e-mail to recipient 1
11	Sending e-mail to recipient 2
12	Sending e-mail to recipient 3
13	Sending e-mail to recipient 4

Event mask example

You enter the hexadecimal code 3B0800 as an event mask.

The event mask configures the following bit settings:

```
0011 1011 0000 1000 0000 0000
```

The event is configured as follows:

- The severity level is severe.
- The event will be logged.
- Traps generated by the event will be sent to trap receivers 1 and 2.
- When the event occurs, e-mail will be sent to recipient 3 only.

Management Card and Battery Manager Events

Event generation

The Management Card and Battery Management System both generate events, which are logged in the event log.

Any event of either type generates a unique code, which you can use in applications to identify the event.

To use SNMP traps for event notifications, you must first identify the trap receivers (up to four) by their specific IP addresses.



See [Trap Receivers](#).

Discharge cycle counter

Battery management event 0x0814 alerts you that a battery string is discharging, and displays the string current (rate of discharge), ambient and pilot battery temperatures. Battery management event 0x0815 indicates that the battery string is no longer discharging.

The system automatically records the ampere-hours lost by the battery string during the discharge.

Severity levels defined

Severity	Definition
Severe	Requires immediate action. Severe events can cause incorrect operation of the Battery Management System or can cause loss of power protection during a power failure.
Warning	Needs action if the condition worsens, but does not require immediate attention.
Informational	Requires no action.



Note

All Battery Management System events and some Management Card events have a severity level.



For information about how severity levels define the actions associated with events, see [Actions Option \(Web interface only\)](#).

Management Card events

Code	Severity	Description
0x0001	Severe	System: Coldstart. (The Management Card was turned on.)
0x0002	Severe	System: Warmstart. (The Management Card was reset after it was already turned on.)
0x0003	Warning	System: SNMP configuration change.
0x0004	Informational	System: Detected an unauthorized user attempting to access the SNMP interface.
0x0005	Warning	System: Detected an unauthorized user attempting to access the control console interface.
0x0006	Warning	System: Detected an unauthorized user attempting to access the Web interface.
0x0007	None	System: Network service started.
0x0008	Warning	System: Password changed.
0x0009	None	System: Restarting.
0x000C	None	System: File transfer started. (FTP)
0x000D	None	System: File transfer started. (TFTP)
0x000F	None	System: File transfer failed.
0x0014	None	System: control console user logged on.
0x0015	None	System: Web user logged on.
0x0016	None	System: FTP user logged on.
0x0018	None	System: Reset to Defaults.
0x0019	None	System: Initializing data in the file.
0x001A	None	System: E-mail information.
0x001D	None	System: TCP/IP stack failure.

Code	Severity	Description
0x001E	None	System: control console user logged out.
0x001F	None	System: Web user logged out.
0x0020	None	System: FTP user logged out.
0x0021	None	System: Set date or time.
0x0024	None	System: Trace information.
0x0025	Warning	System: Modem dial-out failed.
0x002A	None	System: Network service information.
0x002B	None	System: Network service could not start.
0x002C	None	System: Network service stopped.
0x002D	None	System: SSL error: invalid certificate.
0x002E	None	System: New certificate loaded.
0x002F	None	System: SSL enabled (now using HTTPS).
0x0030	None	System: SSL disabled (now using HTTP).
0x0031	None	System: Web server could not start.
0x0032	None	System: DNS network error.
0x0033	None	System: Configuration change.
0x0034	None	System: Configuration file upload complete.
0x0035	None	System: Paging: Failed to send message.
0x0036	None	System: SSL information.
0x0037	None	System: SSH/SCP information.
0x0038	None	System: Certificate, host key, and log store information.



Note

You cannot configure actions for Management Card events that have no severity level.



Note

Not all of the “System” events listed in the table are supported by the Battery Management System.

Battery Management System events

Code	Severity	Description
0x0801	Informational	System: Communication established.
0x0802	Severe	System: Communication lost.
0x080D	Informational	System: Configuration has been changed.
0x080E	Severe	Charger: String voltage is low.
0x080F	Informational	Charger: Low string voltage returned to normal.
0x0810	Severe	Charger: String voltage is high.
0x0811	Informational	Charger: High string voltage returned to normal.
0x0812	Warning	Charger: High ripple current.
0x0813	Informational	Charger: High ripple current returned to normal.
0x0814	Severe	Charger: String discharging. See Discharge cycle counter .
0x0815	Informational	Charger: String no longer discharging.
0x0816	Severe	Battery: Cell shorted.
0x0817	Informational	Battery: Cell short cleared.
0x0818	Warning	Management Controller: Open fuse or connection.
0x0819	Informational	Management Controller: Open fuse or connection normal.
0x081A	Severe	Battery: Capacity is low.
0x081B	Informational	Battery: Low capacity is now normal.
0x081C	Warning	Battery: Ohmic value is high.
0x081D	Informational	Battery: High ohmic value is now normal.
0x081E	Severe	Battery: Thermal runaway in progress.
0x081F	Informational	Battery: Thermal runaway no longer in progress.
0x0820	Warning	Battery: Dryout/sulfation present.

Code	Severity	Description
0x0821	Informational	Battery: Dryout/sulfation no longer present.
0x0822	Severe	Battery: Pilot temperature high.
0x0823	Informational	Battery: High pilot temperature returned to normal.
0x0824	Severe	Environment: Ambient temperature high.
0x0825	Informational	Environment: High ambient temperature returned to normal.
0x0826	Warning	Environment: Ambient temperature low.
0x0827	Informational	Environment: Low ambient temperature returned to normal.
0x0828	Severe	Management Controller: System is not configured correctly.
0x0829	Informational	Management Controller: System is configured correctly.
0x082A	Warning	Management Controller: Ripple current sensor is disconnected.
0x082B	Informational	Management Controller: Ripple current sensor is present.
0x082C	Severe	Management Controller: Current sensor is disconnected.
0x082D	Informational	Management Controller: Current sensor is present.
0x082E	Severe	Management Controller: Pilot temperature sensor is disconnected.
0x082F	Informational	Management Controller: Pilot temperature sensor is present.
0x0830	Warning	Management Controller: Ambient temperature sensor is disconnected.
0x0831	Informational	Management Controller: Ambient temperature sensor is present.
0x0832	Informational	System: Response benchmark established.
0x0833	Informational	System: Response test complete.

Data Logging (Web interface)

Description

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

- Access the data log.
- Define the **Discharge** and **Charge Data Log** intervals.

The **Data Log** displays information logged by each Battery Management unit. Each log entry displays the following data points:

Date and Time	The date and time the entry was logged.
Unit Number	The number assigned to the unit of the Battery Management System.
Mode	The mode in which the data was logged.
Ambient Temperature and Pilot Temperature	The temperature of the environment.
String current	The common current that is discharging into the load. It ranges from 0 to -1000 amps. Each string has its own current sensor.
Voltage	Voltage of each individual battery in the string.
Ripple current	The AC portion of the string current.

To clear all events from the log, use the **Delete Log** button.

Configuration

Use this option to change the **Discharge** and **Charge Log Interval** settings which define how often data will be sampled and recorded in the data log.

Boot Mode

Introduction

Overview

In addition to using a BOOTP server or manual settings, the Management Card that the Battery Management System master controller contains can use a dynamic host configuration protocol (DHCP) server to provide the settings it needs to operate on a TCP/IP network.

To use a DHCP server to provide the Management Card's network settings, 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**.



See also

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

DHCP & BOOTP boot process

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

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



Note

To configure the Management Card that the Battery Management System master controller contains 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 [Management Card settings](#).

3. If the Management Card 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 every 32 seconds for 12 minutes, and so forth.



Note

If a DHCP server responds with an invalid offer (for example, the offer does not contain the APC Cookie), the Management Card 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, see [DHCP response options](#).

DHCP Configuration Settings

Management Card 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 Management Card that the Battery Management System master controller contains.

- 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](#).

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](#).

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 Management Card 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 Management Card 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 Management Card needs to operate on a network and other information that affects the Battery Management System's operation.

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

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

APC Cookie. Tag 1, Len 4, Data "1APC"

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



To disable the requirement of an APC cookie, see [Management Card settings](#) for information on the **DHCP Cookie Is** setting.

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

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

Boot Mode Transition. Tag 2, Len 1, Data 1/2

This option 43 setting enables or disables the **After IP Assignment** option which, by default, causes the **Boot mode** option to 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 Management Card reboots, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.



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

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



For more information about the **After IP Assignment** option, see [Management Card settings](#).

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

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

TCP/IP options. A Management Card contained in the Battery Management System master controller 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 Management Card.
- **Subnet Mask** (option 1): The Subnet Mask value, which the Management Card needs to operate on the network.
- **Default Gateway** (option 3): The default gateway address, which the Management Card 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 Management Card must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): The time that the Management Card must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other options. A Management Card contained in the Battery Management System master controller 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 Management Card.
- **NTP Time Offset** (option 2): The offset of the Management Card'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 Management Card.
- **Host Name** (option 12): The host name to be used by the Management Card (32-character maximum length).
- **Domain Name** (option 15): The domain name to be used by the Management Card (64-character maximum length).

Security Features

Planning and implementing security features

As a network device that passes information across the network, the Network Management Card in the master controller of the Battery Management System is subject to the same exposure as other devices on the network.

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

Summary of access methods

Serial control console.

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

Remote control console.

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

SNMP.

Security Access	Description
Available methods: <ul style="list-style-type: none">• Community Name• Domain Name• NMS IP filters• Agent Enable/Disable• 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. <ul style="list-style-type: none">• 162.245.12.1 allows only the NMS with that IP address to have access.• 162.245.12.255 allows access for any NMS on the 162.245.12 segment.• 162.245.255.255 allows access for any NMS on the 162.245 segment.• 162.255.255.255 allows access for any NMS on the 162 segment.• 0.0.0.0 or 255.255.255.255 allows access for any NMS.

File transfer protocols.

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

Web Server.

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

Changing default user names and passwords immediately

As soon as you complete the installation and initial configuration of the Battery Management System, 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 server uses a non-standard port, a user must specify the port when using the client interface, such as a Web browser. The non-standard port address becomes an extra “password,” hiding the server to provide an additional level of security. The TCP ports for which these servers listen are initially set at the standard “well known ports” for the protocols. To hide the interfaces, use any port numbers from 5000 to 32768.

User names, passwords, 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 Battery Management System. 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 versus encryption

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

To ensure that data and communication between the Battery Management System 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).
- 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 \(SCP\)](#) and [Secure Sockets Layer \(SSL\)](#).

Encryption

Secure SHell (SSH) and Secure CoPy (SCP)

The Secure SHell (SSH) protocol provides a secure mechanism to access computer consoles or *shells* remotely. The protocol authenticates the server (in this case, the Battery Management System) 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 Battery Management System) to the SSH client, SSH uses a host key that is unique to the SSH server and that provides an identification that cannot be falsified. Therefore, an invalid server on the network cannot obtain a user name and password from a user by presenting itself as a valid server.



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

- The Battery Management System 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 Management Card, and version 2 provides improved protection from attempts to intercept, forge, or change data that are transmitted.
- When you enable SSH, Telnet is automatically disabled.
- The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet.



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

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

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

Secure Sockets Layer (SSL)

For secure Web communication, you enable Secure Sockets Layer (SSL) by selecting HTTPS (SSL) as the protocol mode to use for access to the Web interface of the Battery Management System. 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 Battery Management System supports SSL version 3.0. 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 Battery Management System). The browser verifies the following:

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

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

You can use the APC Security Wizard, provided on the APC Battery Management System *Utility* 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 an APC root certificate to upload to a browser's certificate store (cache). You can also use the Wizard to create a server certificate to upload to the Battery Management System.



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



To create certificates and certificate requests, see [Using the APC Security Wizard](#).

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



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



Note

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

Creating and Installing Digital Certificates

Purpose

For network communication that requires a higher level of security than password encryption, the Web interface of the Battery Management System supports the use of digital certificates with the Secure Sockets Layer (SSL) protocol. Digital certificates can authenticate the Battery Management System (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 Battery Management System's auto-generated default certificate.
- **Method 2:** Use the APC Security Wizard to create a CA certificate and a server certificate.
- **Method 3:** Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate.



Note

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

Choosing a method for your system

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

Method 1: Use the Battery Management System's auto-generated default certificate. When you enable SSL, you must reboot the Management Card in the Battery Management System master controller. During rebooting, if no server certificate exists on the Management Card, the Management Card 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 Battery Management System access and all data to and from the Battery Management System 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 Management Card in the Battery Management System master controller 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 Battery Management System, 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 Battery Management System has the Management Card's serial number in place of a valid *common name* (the DNS name or the IP address of the Management Card). Therefore, although the Battery Management System can control access to its Web interface by user name, password, and account type (e.g., **Administrator**, **Device Manager**, or **Read-Only User**), the browser cannot authenticate what master controller's Management Card is sending or receiving data.
- The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is only 768 bits. (The public key used in Methods 2 and 3 is 1024 bits, providing more complex encryption and consequently a higher level of security.)

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

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

The Web browser authenticates the Management Card in the Battery Management System master controller sending or requesting data:

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

This method has the following advantages and disadvantages.

- **Advantages:**
 - Before they are transmitted, the user name and password for Management Card access and all data to and from the Management Card 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 Management Card enables SSL to authenticate that data are being received from and sent to the correct Management Card. 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 Management Card's server certificate to provide additional protection from unauthorized access.
- **Disadvantage:**

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

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



Note

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

This method has the following advantages and disadvantages.

- **Advantages:**

- Before they are transmitted, the user name and password for Management Card access and all data to and from the Management Card 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 Battery Management System.
- 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 Management Card enables SSL to authenticate that data are being received from and sent to the correct Management Card. 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 Management Card with the signature on the CA root certificate that is already in the browser's certificate cache to provide additional protection from unauthorized access.
- **Disadvantages:**
 - Setup requires the extra step of requesting a signed root certificate from a Certificate Authority.
 - An external Certificate Authority may charge a fee for providing signed certificates.

Firewalls

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

Using the APC Security Wizard

Overview

Authentication

Authentication verifies the identity of a user or a network device (such as an APC Network Management Card in the Battery Management System master controller). Passwords typically identify computer users. However, for transactions or communications requiring more stringent security methods on the Internet, the Battery Management System 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 Management Card.
- Secure SHell (SSH), used for remote terminal access to the Battery Management System's control console, uses a public *host key* for authentication rather than a digital certificate.

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

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

- Each Battery Management System with SSL enabled must have a server certificate on the Management Card itself.
- Any browser that is used to access the Battery Management System's Web interface 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 Management Card generates automatically. The default certificate's digital signature will not be recognized by browsers, but a default certificate enables you to use SSL for the encryption of transmitted user names, passwords, and data. (If you use the default certificate, the browser prompts you to agree to unauthenticated access before it logs you on to the Web interface of the Battery Management System.)

How SSH host keys are used. An SSH *host key* authenticates the identity of the server (the Management Card in the Battery Management System master controller) each time an SSH client contacts the Battery Management System. Each Battery Management System with SSH enabled must have an SSH host key on the Management Card itself.

Files you create for SSL and SSH security

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

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

- An SSH host key that your SSH client program uses to authenticate the Management Card in the Battery Management System master controller 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 APC Security Wizard are 1024-bit RSA keys. If you do not create and use SSL server certificates and SSH host keys with the APC Security Wizard, the Management Card generates 768-bit RSA keys.

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

Create a Root Certificate & Server Certificates

Summary

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



Note

The public RSA key that is part of a certificate generated by the APC Security Wizard is 1024 bits. (The default key generated by the Management Card, 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 Battery Management Systems. During this task, two files are created.
 - The file with the **.p15** extension is an encrypted file which contains the Certificate Authority's private key and public root certificate. This file signs the server certificates.
 - The file with the **.crt** extension, which contains only the Certificate Authority's public root certificate. You load this file into each Web browser that will be used to access the Battery Management System so that the browser can validate the server certificate of the Management Card.
- 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 Battery Management System.
- For each Battery Management System that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

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

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



Note

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

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



Note

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

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

Load the CA root certificate to your browser. Load the **.crt** file to the browser of each user who needs to access the Management Card.



See also

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

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

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

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



Note

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

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



Note

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

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

Load the server certificate to the Management Card on the Battery Management System master controller. Perform these steps:

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



Note

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Management Card. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Management Card. For SCP, the command to transfer a certificate named **cert.p15** to a Management Card 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 Management Card's private key.
 - The file with the **.csr** extension contains the certificate signing request, which you send to an external Certificate Authority.
- When you receive the signed certificate from the Certificate Authority, import that certificate. Importing the certificate combines the **.p15** file containing the private key and the file containing the signed certificate from the external Certificate Authority. The output file is a new encrypted server certificate file with a **.p15** extension.
- Load the server certificate onto the Management Card in the Battery Management System master controller.
- For each Management Card that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the Certificate Signing Request (CSR). Perform these steps.
(Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC Battery Management System *Utility* CD.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled "Step 1," select **Certificate Request** as the type of file to create.
4. Enter a name for the file that will contain the Management Card's private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. On the screen labeled Step 2, provide the information to configure the certificate signing request (CSR) with the information that you want the signed server certificate to contain. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter the IP Address or DNS name of the Battery Management System.



Note

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

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



Note

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

7. The last screen verifies that the certificate signing request has been created and displays the location and name of the file, which has a **.csr** extension.
8. Send the certificate signing request to an external Certificate Authority, either a commercial Certificate Authority or, if applicable, a Certificate Authority managed by your own company or agency.



See also

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

Import the signed certificate. When the external Certificate Authority returns the signed certificate, perform these steps to import the certificate. This procedure combines the signed certificate and the private key into an SSL server certificate that you then upload to the Management Card in the Battery Management System master controller. (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)**. This file has a **.p15** extension, contains the Management Card's private key, and, by default, is located in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. Specify a name for the output file that will be the signed server certificate that you upload to the Management Card. The file must have a **.p15** extension.
6. Click **Next** to generate the server certificate. The certificate's **Issuer Information** on the summary screen confirms that the external Certificate Authority signed the certificate.
7. The last screen verifies that the certificate has been created and instructs you on the next task, to load the server certificate to the Battery Management System. It displays the location and name of the server certificate, which has a **.p15** file extension and contains the Management Card's private key and the public key obtained from the **.cer** or **.crt** file.

Load the server certificate to the Management Card. Perform these steps:

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



Note

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Management Card. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Management Card. For SCP, the command to transfer a certificate named **cert.p15** to a Management Card 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 Battery Management System generates a 768-bit RSA key when it reboots. Host keys for SSH that are created with the APC Security Wizard are 1024-bit RSA keys.

- Use the APC Security Wizard to create a host key, which is encrypted and stored in a file with **.p15** extension.
- Load the host key onto the Management Card on the Battery Management System master controller.

The procedure

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

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC Battery Management System *Utility* CD.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled Step 1, select **SSH Server Host Key** as the type of file to create.
4. Enter a name for the file that will contain the host key. The 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. 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 Management Card, you can verify that the correct host key was uploaded by verifying that the fingerprints displayed here match the SSH fingerprints on the Battery Management System, 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 Battery Management System. It displays the location and name of the host key, which has a **.p15** file extension.

Load the host key to the Management Card on the Battery Management System master controller. Perform these steps:

1. On the **Network** menu of the Web interface of the Battery Management System, select the **Telnet/SSH** option.
2. In the **SSH User Host Key File** section of the page, browse to the host key, the **.p15** file you created in the procedure [Create the host key](#). (The default location is **C:\Program Files\American Power Conversion\APC Security Wizard**.)
3. On the **SSH Host Key Fingerprint** section of the page, note the fingerprint for the version (or versions) of SSH you are using. Log on to the Battery Management System 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 Management Card. You must specify the correct location, **\sec**, on the Management Card. For SCP, the command to transfer a host key named **hostkey.p15** to a Management Card with an IP address of 156.205.6.185 would be:

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

How to Export Configuration Settings

Retrieving and Exporting the .ini file

Summary of the procedure

As an Administrator, you can retrieve a dynamically generated .ini file of a Battery Management System Management Card's current configuration and export that file to another Battery Management System Management Card or to multiple Battery Management System Management Cards.

1. You configure the Management Card on a Battery Management System master controller to have the settings you want to export.
2. You retrieve the .ini file from that Management Card.
3. You then customize the .ini file (to change at least the TCP/IP settings) and make a copy to export.
4. You use any of the file transfer protocols supported by the Battery Management System to transfer the copied file to one or more additional Management Cards. (To transfer the file to multiple Management Cards simultaneously, write an FTP or SCP script that repeats the steps for transferring the file to a single Management Card.)
5. Each receiving Battery Management System Management Card stores the file temporarily in its flash memory, uses it to reconfigure its own Management Card settings, and then deletes the file.

Contents of the .ini file

The config.ini file that you retrieve from a Battery Management System Management Card contains the following:

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



Note

Only section headings and keywords supported for the specific device associated with the Management Card from which you retrieve the file are included.

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



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

Detailed procedures

Use the following procedures to retrieve the settings of one Battery Management System Management Card and export them to one or more other Battery Management System Management Card(s).

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

1. Configure a Management Card with the settings you want to export.



Note

To avoid errors, configure the Management Card by using its Battery Management System 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 Management Card you configured:
 - a. Open a connection to the Battery Management System's Management Card, 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 Battery Management System.
- c. Retrieve the config.ini file containing the Management Card's current settings:

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

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



See also

To create batch files and use an APC utility to retrieve configuration settings from multiple Battery Management System Management Cards and export them to other Battery Management System Management Cards, see *Release Notes: ini File Utility, version 1.0 (.doc\en\ininotes.pdf)* on the APC Battery Management System *Utility* 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 Battery Management Systems 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 Battery Management System Management Cards, can have any file 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 Battery Management System Management Card. To export the .ini file to another Management Card, use any of the file transfer protocols supported by Battery Management Systems (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 Battery Management System 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 Battery Management System Management Card 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 Battery Management System Management Cards. To export the .ini file to multiple Management Cards:

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



See also

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

The event and its error messages

The following system event occurs when the receiving Battery Management System 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 Management Card succeeds even if there are errors.

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

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

Errors generated by overridden values

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



See [Contents of the .ini file](#) for information about which values are overridden.

The overridden values are device-specific and not appropriate to export to other Battery Management System Management Cards. 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, you can choose to update the basic TCP/IP settings of the Battery Management System's Management Card by using the APC Device IP Configuration Wizard.

APC Device IP Configuration Wizard

Purpose and Requirements

Purpose: configure basic TCP/IP settings

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

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

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

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



Note

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

System requirements

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

Install the Wizard

Download the wizard

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

Use the Wizard

Launch the Wizard

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

Configure the basic TCP/IP settings remotely

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

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

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

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

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

Configure or reconfigure the TCP/IP settings locally

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

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

File Transfers

Introduction

Overview

The Battery Management System Management Card 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 Management Card, the program code is updated and new features become available.

This chapter describes how to transfer firmware files to Battery Management System Management Cards.



Note

To transfer a firmware file to a Management Card, see [Upgrading Firmware](#).



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

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.

Benefits of upgrading firmware

Upgrading the firmware on the Battery Management System has the following benefits:

- New firmware has the latest bug fixes and performance improvements.
- New features become available for immediate use.
- Keeping the firmware versions consistent across your network ensures that all Battery Management Systems support the same features in the same manner.

Obtain the latest firmware version

To determine if updated firmware is available to download, go to the “Software Downloads” page, www.apc.com/tools/download, on the APC Web site.

The firmware upgrade consists of the two modules: An APC Operating System (AOS) module and an application module.



See [Firmware files \(Battery Management System\)](#).



Note

To upgrade the firmware module of an APC device on a Microsoft platform, use the firmware upgrade tool, a self-extracting executable file available on the APC Battery Management System *Utility* CD or available at no cost from the support section of the APC Web site (www.apc.com/support).

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

Firmware files (Battery Management System)

The APC Operating System (AOS) and application module files used with the Battery Management System share the same basic format:

```
apc_hw0x_type_version.bin
```

- *apc*: Indicates that this is an APC file.
- *hw0x*: Identifies the version of the Battery Management System that will run this binary file.
- *type*: Identifies whether the file is for the APC Operating System (AOS) or the application module (APP) for the Battery Management System.
- *version*: The version number of the application file. For example, a code of 264 would indicate version 2.6.4.
- *bin*: Indicates that this is a binary file.



Note

For the most recent versions of the AOS and application modules for the Battery Management System, go to the “Software Downloads” page, www.apc.com/tools/download, on the APC Web site.

On Linux, you must upgrade the two firmware modules separately.

On Windows operating systems, you can use the firmware upgrade tool, also available on the “Software Downloads” page.



See [Obtain the latest firmware version](#).

Firmware file transfer methods

You can use FTP or SCP to upgrade the firmware of one or more Battery Management System Management Cards over the network.

You can use XMODEM to upgrade the firmware for a Management Card that is not on the network.

When you use FTP or XMODEM to upgrade the firmware for a Management Card, the APC Operating System (AOS) module must be transferred to the Management Card before you transfer the application module.



For more information about the firmware modules, see [Firmware files \(Battery Management System\)](#).

Use FTP or SCP to upgrade one Battery Management System Management Card

For you to be able to use FTP to upgrade a single Battery Management System over the network:

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

To use FTP to upgrade the Management Card:

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

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

Files listed for a Battery Management System, for example, might be the following:

- `apc_hw02_aos_264.bin`
- `apc_hw02_app_260.bin`



Note

If your APC device is running version 2.0.1 or later of the AOS firmware already, you may upgrade directly to version 2.1.0 or a later version

2. Open an FTP client session:

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

3. Type `open` and the Battery Management System's IP address, 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 Battery Management System Management Card's **FTP Server Port** setting has been changed from its default of **21**, such as to **21000**, you would use the following command for a Windows FTP client transferring a file to a Battery Management System Management Card with an IP address of 150.250.6.10.

```
ftp> open 150.250.6.10 21000
```
4. Log on using the Administrator user name and password. (**apc** is the default for both.)
5. Upgrade the AOS. For example:

```
ftp> bin  
ftp> put apc_hw02_aos_264.bin
```
6. When FTP confirms the transfer, type **quit** to close the session.
7. Repeat **step 2** through **step 6** 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 Battery Management System Management Card:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the Battery Management System. The following example assumes a Battery Management System IP address of 158.205.6.185, and an AOS module of **apc_hw02_aos_264.bin**.)

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

3. Use a similar SCP command line, with the name of the application module instead of the AOS module, to transfer the application module to the Battery Management System.

Use FTP or SCP to upgrade multiple Battery Management System Management Cards

To upgrade multiple Battery Management System Management Cards using an FTP client or using SCP, write a script which automatically performs the procedure. For FTP, use the steps in [Use FTP or SCP to upgrade one Battery Management System Management Card](#).

Use XMODEM to upgrade one Battery Management System Management Card

To use XMODEM to upgrade the firmware for a single Battery Management System Management Card 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 serial cable that came with the Battery Management System to the selected port and to the serial port at the Management Card.



Note

Modbus and the control console share a common serial port. You can use either one or the other to access the Battery Management System.



See also

If you are using Modbus to access the Battery Management System, you must configure the DIP Switches. For DIP switch configuration, see “Configure the DIP Switches” in the *Installation and Quick Start Manual* ([.\doc\en\insguide.pdf](#)), provided in Portable Document Format (PDF) on the APC Battery Management System *Utility* CD and in printed form.

3. Run a terminal program (such as HyperTerminal), and configure the selected port for 9600 bps (or 19200 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 you selected, and press ENTER.
8. From the terminal program's menu, select the binary AOS file to transfer via XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600. The Management Card 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 \(Battery Management System\)](#).

Verifying Upgrades and Updates

Overview

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

Last Transfer Result codes

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

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

Alarms

Fault Alarm Criteria

Fault	LED	Fault Criteria
Charger Voltage Low	Charger	Less than 2.1 volts per cell for lead-acid batteries, or as set by user.
Charger Voltage High	Charger	Greater than 2.4 volts per cell for lead-acid batteries or as set by user.
Shorted Cell	Batteries	Less than $((\#Cells/Batt)-1) \times (Vstring)$ $(\#Cells/Batt) \times (\#Batt/String)$
Blown Fuse/Open Connections or Wiring	Management Controller	Less than 1/2 volt on first or last battery in a string or two consecutive batteries within a string.
Low Capacity	Batteries	Any individual battery with more than 20% lower voltage than the highest battery in the same string during a discharge.
Thermal Runaway	Batteries	Greater than 20% more response current than the benchmark, or greater than 95° F battery temperature, or as set by the user.
Dryout/Sulfation/Opens	Batteries	Greater than 20% less response current than benchmark, or as set by user.
High or Low Operating Temperature	Environment	Less than 50° F or greater than 95° F or as set by the user.
High Ripple Current	Charger	Greater than 5 amps RMS per ampere-hour or as set by the user.

Alarm Relay and LED Operation

Situation/Condition	Alarm Relay	Status LEDs			
NOTE: Alarm Relay operates as a “Fail-Safe” device that is energized during non-alarmed periods.	Normally Open Contacts (de-energized)	Management Controller	Batteries	Charger	Environment
Normal Operations	Closed (energized)	On	On	On	On
Management System Fault	Open (de-energized)	Flash	On	On	On
High or low environment temperature or auxiliary environment sensor alarm	Open (de-energized)	On	On	On	Flash
Charger Fault - High or low charging voltage or high ripple current	Open	On	On	Flash	On
Connection fuse or wiring fault	Open	Flash	On	On	On
Battery Fault - Low capacity, high ohmic value, shorted cell or thermal runaway	Open	On	Flash	On	On
Missing or Faulty Sensor	Open	Flash	On	On	On
System off or loss of input power	Open	Off	Off	Off	Off

Troubleshooting

Management Card

Access problems (Battery Management System Management Card)

Problem	Solution
Unable to ping the Management Card	<p>Is the Management Card's Status LED (on the front panel of the master controller) green, indicating it is running its SNMP agent on the network? If yes, try to ping another node on the same network segment as the Management Card. If that fails, it is not a Management Card problem.</p> <p>If the Status LED is not green, or if the ping test of another node succeeds, perform the following checks:</p> <ul style="list-style-type: none">• Verify all network connections.• Verify the IP addresses of the Management Card and the NMS.• Verify the default gateway (or router) IP address if the NMS is on a different physical network (or subnetwork) from the Management Card.• Verify the number of subnet bits for the Management Card's subnet mask.
The terminal program cannot allocate the communications port when you try to configure the Battery Management System	<p>Before you can use a terminal to configure the Battery Management System, you must shut down any application, service, or program using the communications port.</p>

Problem	Solution
Cannot access the control console through a serial connection	Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.
Cannot access the control console remotely	<ul style="list-style-type: none"> • 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 Battery Management System may be creating a host key. The Battery Management System can take up to 5 minutes to create this host key, and SSH is not accessible during that time.
Cannot access the Web interface	<ul style="list-style-type: none"> • 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 Battery Management System. 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 Battery Management System. See Supported Web browsers. • If the Battery Management System has just restarted and SSL security is being set up, the Battery Management System may be generating a server certificate. The Battery Management System can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.
Cannot access the Web interface	<ol style="list-style-type: none"> 1. Verify that HTTP access is enabled. 2. Verify that you can ping the adapter. 3. Verify that you are using a Web browser that is supported for the Battery Management System. See Supported Web browsers.

SNMP issues (Battery Management System Management Card)

Problem	Solution
Unable to perform a GET	<ol style="list-style-type: none">1. Verify the read (GET) community name.2. Use the Control Console or Web interface to ensure that the NMS has access. See Telnet/SSH.
Unable to perform a SET	<ol style="list-style-type: none">1. Verify the read/write (SET) community name.2. Use the control console or Web interface to ensure that the NMS has write (SET) access. See Telnet/SSH.
Unable to receive traps at the NMS	Query the MIB mconfigTrapReceiverTable OIDs to verify that the NMS IP address is listed correctly, and that the community name defined for the NMS matches the community name in the table. If necessary, use SETs to the OIDs, or use the control console or Web interface to correct the trap receiver definition problem. See Telnet/SSH .
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.

Product Information

Warranty and Service

Limited warranty

APC warrants the Battery Management System to be free from defects in materials and workmanship for a period of two years from the date of purchase. Its obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. This warranty does not apply to equipment that has been damaged by accident, negligence, or misapplication or has been altered or modified in any way. This warranty applies only to the original purchaser.

Warranty limitations

Except as provided herein, APC makes no warranties, expressed or implied, including warranties of merchantability and fitness for a particular purpose. Some jurisdictions do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser.

Except as provided above, in no event will APC be liable for direct, indirect, special, incidental, or consequential damages arising out of the use of this product, even if advised of the possibility of such damage.

Specifically, APC is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise. This warranty gives you specific legal rights and you may also have other rights, which vary according to jurisdiction.

Obtaining service (service contracts)

If you could not resolve the problem using the information in [Troubleshooting](#), contact APC Worldwide Customer Support at a phone number listed at the end of this manual, and be ready to provide the following:

- The Battery Management System's serial number, which is on the top of the unit
- A description of the problem
- Information about your service contract.

If phone consultation cannot solve the problem, you need on-site service by an APC technician. See your service contract for information.



Do not attempt to remove the Management Card. The terms of your warranty and service contract require that service be performed by an authorized APC technician only.

Life-Support Policy

General policy

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

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

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

Examples of life-support devices

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

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

Index

A

About menu option 73

Access

Access Type setting for SNMP 48

FTP Server 39

limiting NMS SNMP access by

IP address 47

locally to the control console 11

security options for each interface 110

troubleshooting 172

Account types

administrator 13

default user names and passwords 13

device manager 13

read-only user 13

Advanced settings

Client ID 36, 104

Domain Name 35, 104

Host Name 35, 104

On Retry Failure 36

Port Speed 35, 104

Retry Then Fail 36

TCP/IP settings 35

User Class 36, 104

Vendor Class 36, 104

Alarms

batteries 24

charger 24

details 22, 23

environment 23

management controller 25

APC security wizard

authentication 127

procedure if your company

does not have its own

certificate authority 131

procedure if your company has its own

certificate authority 137

SSH 127

host keys 128

SSL 127

certificates 127

Apply Local Computer Time 67

Authentication

with SSL 117

Authentication traps 83

Auto logout 63

B

Batteries

alarms 24

definition 7

Battery management system

capacity 2

events 97

features 3

main screen 17

unit 7

Boot mode 34

DNS servers 109

NTP servers 109

NTP time offset 109

process 101

settings 34

TCP/IP options 108

BOOTP

- After IP Assignment setting 105
 - Communication settings 36
 - DHCP & BOOTP boot process 102
 - Remain in DHCP & BOOTP mode setting 105
- BOOTP Only boot mode setting 34

Browsers

- CA certificates in browser's store (cache) 117
- supported 5

C

- Cell max voltage limit 27
- Cell min voltage limit 27
- Certificate authority
 - if your company does not have its own 131
 - if your company has its own 137
- Certificates
 - choosing which method to use 119
 - creating and installing for SSL 119
 - methods
 - APC Security Wizard creates all certificates 122
 - Use a Certificate Authority (CA) 124
 - Use the APC default certificate 120
- Charger alarms 24
- CipherSuite
 - Choosing SSL encryption ciphers and hash algorithms 56
 - purpose of the algorithms and ciphers 118
- Client ID setting 36, 104
- Community name
 - for SNMP access control 47
 - for trap receiver settings 83
- config.ini file 146

Configuration

- cell max voltage limit 27
- cell min voltage limit 27
- maximum ambient temperature 28
- maximum pilot temperature 28
- menu 27
- minimum ambient temperature 28
- reset lowest discharge voltages 31
- reset response benchmark 31

Configuring

- SSH 40

Control console interface 10

Current acceptance 7

Customizing user configuration files 148

D

Data log

- importing into spreadsheet 78
- using FTP or SCP to retrieve 78

Data logging

- configuration 100
- description 99

Date & time 67

- set manually 67
- synchronize with NTP server 67

Date & Time settings

- Apply Local Computer Time 67
- GMT Offset (Time Zone) 68
- Manual 67
- Network Time Protocol (NTP) 67
- Primary NTP Server 68
- Secondary NTP Server 68
- Set Manually 67
- Synchronize with NTP Server 67
- Update Interval 68

Delete SSH Host Keys and SSL

- Certificates 69

Device IP Configuration Wizard 152

Device manager user 13

DHCP

- After IP Assignment setting 105
- APC cookie 106
- Communication settings 36
- Configuration 101
- Cookie Is setting 105
- DHCP & BOOTP boot process 102
- Management Card settings 102
- Remain in DHCP & BOOTP mode setting 105
- Require vendor specific cookie to accept DHCP Address setting 105
- response options 106
- Retry Then Stop setting 105
- DHCP & BOOTP boot mode setting 34
- DHCP Only boot mode setting 34
- Digital certificates 119
 - methods 120
- DIP switches 11
- Discharge cycle counter 92
- DNS 34
 - email 87
 - sending DNS query 37
 - sending query 37
 - servers 109
 - testing the network connection to the DNS server 37
- Domain names 35
 - configuring 35, 104
 - overriding expansion of host name to domain name 35

E

- Email menu option 48
- Email recipients 84
 - DNS 87
 - e-mail test 85
 - reason to use local DNS server 87
 - SMTP settings 87
 - using SMTP 86

Encryption

- with SSH and SCP 115
- with SSL 52
- Environment alarms 23
- Error messages
 - from overridden values during .ini file transfer 151
- Event generation 92
- Event list access and format 88
- Event log 76
 - accessing 77
 - errors from overridden values during .ini file transfer 151
 - using FTP del command 80
 - using FTP or SCP to retrieve 78
- Event mask settings 89
- event.txt file
 - contents 78
 - importing into spreadsheet 78
- Events
 - battery management system 97
 - management card 94
- Events menu 74
 - actions 81
 - e-mail 82
 - enabling and disabling 81
 - event log 81
 - severity level 81
 - SNMP trap 81
 - configure individual events 88
 - discharge cycle counter 92
 - email recipients 84, 86, 87
 - email test 85
 - event generation 92
 - event list access and format 88
 - event log 76
 - accessing 77, 81
 - event mask settings 89
 - management card events 94
 - recipients 83
 - trap receivers 83
 - severity levels 93

F

- Facility (Syslog setting) 49
- File transfers 71, 158
 - firmware files 161
 - methods 162
 - using FTP or SCP 163
 - using XMODEM 166
 - upgrading firmware 159
 - obtaining latest firmware 160
 - verifying upgrades and updates 168
- Firewall, as essential to security 126
- Firmware upgrade utility 160
- Flash type 73
- Float charge 7
- FTP 39
 - disabling when SCP is used 39
 - using to retrieve text version of event or data log 78
- FTP client 71

G

- GMT Offset (Time Zone) 68

H

- Hardware revision 73
- Host key
 - file name 45
 - file status 45
 - fingerprints
 - displaying for versions 1 and 2 46
 - generated by the Management Card 41
 - transferring to the Management Card 41, 45
- Host Name setting 35, 104
- HTTP Port 55
- HTTP protocol mode 54
- HTTPS Port 55

- HTTPS protocol mode 54
- Hyperlinks, defining 71

I

- Identification
 - system 67
 - contact 67
 - location 67
 - system name 67
- Informational severity level 93
- ini files, *See* User configuration files
- IP addresses
 - to limit access to specified NMSs 47

J

- Jar 7

K

- Keywords, in the user configuration file 146

L

- Links 72
 - redirecting 71
- Lock icon indicating SSL is enabled 54

M

- MAC address 73
- Management card 4
 - events 94
 - port assignment 112
 - resetting network timer 16
 - watchdog mechanism 16

- Management controller 7
 - alarms 25
- Manual boot mode setting 34
- Manual option to set date and time 67
- Manufacture date 73
- Map to Syslog's Priorities 50
- Master controller
 - status codes 18
- Maximum ambient temperature 28
- Maximum pilot temperature 28
- Menus
 - Battery System 18
 - Configuration 27
 - Data 99
 - Device Manager 18
 - Events 74
 - Links 71
 - Network 32
 - System 61
- Minimum ambient temperature 28
- Modbus 11, 30
 - DIP switches 14
 - serial port 11, 14
- Model number 73

N

- Network connections 4
- Network Management Card,
See Management Card
- Network menu 32
 - access 32
 - DNS 34, 37
 - email 48
 - FTP 39
 - FTP Server 39
 - ping utility 38
 - SNMP 47
 - Syslog 49
 - TCP/IP 33

- Telnet/SSH 40
- Web/SSL 52
- Network Time Protocol (NTP) 67
- Network timer, resetting the 16
- NMS IP/Domain Name setting 47
- NTP 67
 - servers 109
 - time offset 109

O

- On Retry Failure setting 36
- Override keyword in user
configuration file 146

P

- Password 63
 - change for security 112
 - how to recover from a lost password 14
 - using non-standard ports as
extra passwords 112
- Passwords
 - default 13
- Ping utility 38
- Port (Syslog setting) 50
- Port Speed setting 35, 104
- Ports
 - assigning 112
 - default
 - for FTP Server 39
 - for HTTP 55
 - for HTTPS 55
 - for SSH 43
 - for Telnet 43
 - using a non-default port
 - for FTP 39
 - for HTTP 55
 - for HTTPS 55
 - for SSH 43
 - for Telnet 43

- Preferences 71
- Primary NTP Server 68
- Protocol Mode
 - selecting for control console access 42
 - selecting for Web access 54

R

- RADIUS
 - settings 64
- Read access by an NMS 48
- Read-only user 13
- Reboot Management Interface 69
- Receiver NMS IP/domain name 83
- Recipients, of traps 83
- Resetting
 - lowest discharge voltages 31
 - only TCP/IP to Defaults 69
 - response benchmark 31
 - to Defaults 69
 - to Defaults Except TCP/IP 69
- Retry Then Fail setting 36
- Retry Then Stop setting (DHCP) 105
- Reverse DNS Lookup 38

S

- SCP
 - enabled and
 - configured with SSH 40
 - enabled and configured with SSH 116
 - using to retrieve text version of event or data log 78
- Secondary NTP Server 68
- Section headings, user configuration file 146
- Secure CoPy. See SCP.
- Secure Hash Algorithm (SHA) 56
- Secure SHell. See SSH.

Security

- authentication
 - authentication vs. encryption 114
 - through digital certificates
 - with SSL 117
 - certificate-signing requests 118
 - digital certificates 119
 - methods 120
 - disabling less secure
 - interfaces 114, 116
 - encryption with SSH and SCP 115
 - features 110
 - firewalls 126
 - immediately changing username and password 112
 - options for each interface 110
 - planning and implementing 110, 114
 - SCP as alternative to FTP 116
 - SSL 119, 120
 - choosing a method
 - to use certificates 119
 - CipherSuite algorithms and ciphers 118
 - supported SSH clients 40
 - using non-standards ports as extra passwords 112
- Serial number 73
 - Server certificates
 - creating an SSL
 - server user certificate 134
 - creating the CA root certificate 132
 - loading the CA root certificate 133
 - loading the server certificate to the Management card 135
 - Server IP/Domain Name (Syslog setting) 50
 - Severity levels 93
 - informational 93
 - severe 93
 - warning 93
 - SMTP

- e-mail 86
 - e-mail settings 87
 - SNMP 47
 - Access Type setting 48
 - Community name setting 47
 - enabling and disabling 47
 - interface 12
 - NMS IP/Domain Name setting 47
 - SSH 127
 - configuring 40
 - enabling 40, 42
 - encryption 115
 - host key
 - as identifier that cannot be falsified 115
 - file name 45
 - file status 45
 - transferring to the
 - Management Card 41
 - host keys 128
 - modifying the Port setting 43, 55
 - network connections 4
 - obtaining an SSH client 40
 - server configuration 44
 - v1 Encryption Algorithms 44
 - v2 Encryption Algorithms 44
 - SSL 127
 - authentication through digital certificates 117
 - certificate signing requests 118
 - certificates 127
 - digital certificates 119
 - methods 120
 - encryption ciphers
 - and hash algorithms 56
 - String current 7
 - Synchronize with NTP Server 67
 - sysContact 67
 - sysLocation 67
 - Syslog 49
 - enabling and disabling 49
 - mapping event severity to Syslog priorities 50
 - settings 49
 - test 51
 - sysName 67
 - System menu 61
 - about 73
 - access restrictions 61
 - date and time 67
 - identification 67
 - links 72
 - preferences 71
 - RADIUS settings 65
 - Tools 69
 - user manager
 - auto logout 63
 - password 63
 - user name 63
- ## T
- TCP/IP 33
 - Advanced settings 35
 - Boot mode 34
 - Client ID setting 36, 104
 - configuring settings 6
 - Current Settings fields 33
 - default gateway 33, 34
 - defining settings for the Management Card 33
 - Domain Name setting 35, 104
 - Host Name setting 35, 104
 - On Retry Failure setting 36
 - options 108
 - Port Speed setting 35, 104
 - restoring default settings 69
 - Retry Then Fail setting 36

- setting port assignments for extra security 112
- subnet mask 33, 34
- system IP address 33, 34
- User Class setting 36, 104
- Vendor Class setting 36, 104
- Telnet
 - enabling 42
- Telnet interface 12
- Telnet/SSH
 - Access option 42
 - host key fingerprints
 - displaying 46
 - modifying the Port settings 43
 - option in Network menu 40
 - selecting the protocol mode 42
 - SSH host key file name 45
 - SSH host key file status 45
 - SSH Port option 43
 - SShv1 Encryption Algorithms 44
 - SShv2 Encryption Algorithms 44
 - Telnet Port option 43
- Testing the network connection to the DNS server 37
- TFTP client 71
- Time Zone 68
- Tools menu 69
 - Delete SSH Host Keys and SSL Certificates 69
 - file transfers 71
 - FTP client 71
 - Reboot Management Interface 69
 - Reset only TCP/IP to Defaults 69
 - Reset to Defaults 69
 - Reset to Defaults Except TCP/IP 69
 - TFTP client 71
 - XMODEM 71
- Trap receivers 83

U

- Unit
 - definition 7
- Update Interval 68
- Upgrading firmware 159
 - obtaining latest firmware 160
 - using an APC utility 160
- UPS not discovered message 151
- User Class setting 36, 104
- User configuration files
 - contents 146
 - customizing 148
 - exporting system time separately 148
 - messages for
 - undiscovered devices 151
 - retrieving and exporting 145
 - using the APC utility to retrieve and transfer the files 147
- User interfaces
 - access priorities 8
 - control console 10
 - SNMP 12
 - Telnet 12
 - web 9
- User manager
 - auto logout 63
 - password 63
 - user name 63
- User name 63
 - change immediately for security 112
 - default 13

V

Vendor Class setting 36, 104

W

Warning, severity level 93

Web interface 9

 enable or disable protocols 54

 Modifying the Port setting

 for FTP 39

 for HTTP 55

 for HTTPS 55

 for SSH 43

 for Telnet 43

 troubleshooting access problems 172

Web/SSL 52– 60

 Secure Sockets Layer. See SSL

X

XMODEM 71

APC Worldwide Customer Support

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

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

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

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

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

Copyright

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

990-1824A

02/2005



Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>