User Manual

Battery Manager

Main Module (AP9922) & Expansion Module (AP9922S)

990-1824D-001
Publication Date: December 2014

Schneider Electric

Schneider Electric Legal Disclaimer

The information presented in this manual is not warranted by Schneider Electric to be authoritative, error free, or complete. This publication is not meant to be a substitute for a detailed operational and site specific development plan. Therefore, Schneider Electric assumes no liability for damages, violations of codes, improper installation, system failures, or any other problems that could arise based on the use of this Publication.

The information contained in this Publication is provided as is and has been prepared solely for the purpose of evaluating data center design and construction. This Publication has been compiled in good faith by Schneider Electric. However, no representation is made or warranty given, either express or implied, as to the completeness or accuracy of the information this Publication contains.

IN NO EVENT SHALL SCHNEIDER ELECTRIC, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF SCHNEIDER ELECTRIC OR THEIR RESPECTIVE OFFICERS, DIRECTORS, OR EMPLOYEES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF SCHNEIDER ELECTRIC HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

Table of Contents

Introduction

Product Features

The Schneider Electric Battery Manager provides automated monitoring and management of stationary battery backup systems of between 100 VDC and 560 VDC per string. The Battery Manager is capable of managing battery systems of various configurations and capacities, provided that all battery systems attached to one Battery Manager system are identical.

The battery systems can be comprised of nominal 2V, 4V, 8V, or 12V lead-acid batteries, or 1.2V or 2.4V nickel-cadmium batteries. The Battery Manager is designed to be agnostic to charger and load considerations, provided that the voltage source is of a constant voltage design.

The Battery Manager supports up to two strings of batteries. Systems managing one string of batteries can support up to 244 lead-acid cells, or up to 375 nickel-cadmium cells. Systems with two strings can manage strings of up to 244 lead-acid cells per string, or up to 256 nickel-cadmium cells per string.

The Battery Manager is controlled through the *Network Management Card* (*NMC*) within the *Networked Unit*.

The Battery Manager can:

- Optimize the charge state of individual batteries within a string; lower voltage cells are automatically boost-charged to bring the voltages up to approximately the string average level.
  - Managing batteries on an individual basis extends the useful life of otherwise undercharged or overcharged batteries and achieves full capacity of otherwise undercharged batteries.
- Monitor and manage batteries connected to one *Networked Unit* (AP9922) and up to seven *expansion units* (AP9922S); a maximum of eight units can be connected.
- Connect each unit to as many as 64 individual batteries
- Manage groups of batteries through a serial connection or IP address. The first unit, or *Networked Unit*, is the only unit of the group equipped with networking capabilities.
- Identify weak or defective batteries needing replacement.
- Issue alerts if various system conditions reach alarm status and require attention.

NOTE: Schneider Electric strongly recommends that you calibrate your Battery Manager during system start up and upon battery replacement in order to ensure accurate readings and measurements and to avoid false alarms.

See “System Calibration” on page 70 for more information.

The *NMC* of the *Networked Unit* utilizes the following standards:

- Hypertext Transfer Protocol (*HTTP*)
- HTTP over Secure Sockets Layer (*HTTPS*)
- File Transfer Protocol (*FTP*)
- Telnet
- Secure SHell (*SSH*)
- Simple Network Management Protocol (*SNMP*)
- Secure Copy (*SCP*)
- Modbus RS-485 RTU and Modbus TCP
- TCP/IP v4 and v6
- RS-232 serial connection
- SMTP-based email
- RADIUS (Remote Access Dial In User Service)

Environmental

The following values apply to the environment required for operation of the Battery Manager (AP9922 and AP9922S). These values do not apply to batteries.

Temperature

Operating Temperature:	0° - 45°C (32° - 113°F)
Storage Temperature:	-25° - 65°C (-13° - 149°F)

Humidity (without degradation)

Operating Humidity (non-condensing):	0 – 95%

Altitude (above sea level)

Operating Altitude:	0 - 3,000 m (0 - 9,843 ft)
Storage Altitude:	0 - 15,000 m (0 - 49,213 ft)

Getting Started

Initial Setup

You must configure the following TCP/IP settings before the Battery Manager Network Management Card (NMC) can operate on a network:

- IP address of the NMC
- Subnet mask
- IP address of the default gateway

NOTE: If a default gateway is unavailable, use the IP address of a computer that is located on the same subnet as the NMC and that is usually running. The NMC uses the default gateway to test the network when traffic is very light.

NOTE: Do not use the loop back address (127.0.0.1) as the default gateway address for the NMC. Doing so disables the card and requires you to reset TCP/IP settings to their defaults using a local serial login.

For more information on configuring the TCP/IP settings, see the *Installation Manual* in printed form, or available in PDF on the web site: www.apc.com.

Accessibility

Users can be logged on by the following methods:

1. Local access to the *Command Console* from a computer with a direct *serial* connection.
2. Telnet or *Secure SHell* (*SSH*) access to the *Command Console* from a remote computer.
3. Web access; either directly or through *StruxureWare*

User Account Overview

The Battery Manager arrives configured with three User Types, as well as associated User Names:

- *Super User* (User Name: *apc*)
- *Device* (User Name: *device*)
- *Read-Only* (User Name: *readonly*).

The initial default password for each of these is *apc*. All levels of access require user name and password permissions.

Both user name and password are case-sensitive, and have a 64 byte maximum, supporting up to 64 ASCII characters; less for multi-byte languages.

The *Super User* can define additional user accounts, as well as set other variables for the additional users. It is generally recommended that non-default user name and passwords be set.

In order to manage User settings from the web browser (accessed by entering the NMC IP address into the address bar), navigate to **Configuration > Security > Local Users > Management**.

- Click on Add User

The User types which can be added are:

- **Administrator:** The Administrator user has full access just as the Super User does, but this user type can be deleted.
- **Device:** The Device user has read-write access to the device-related menus only. The Administrator can enable or disable the Device user account.
- **Read-Only:** The Read-Only User account has read-only access, through the Web interface, to view status but not to control a device or change any configured value. The Administrator can enable or disable the Read-Only user account.
- **Network-Only:** The Network-Only user has read-write access to the network-related menus only. The Administrator can enable or disable the Network-Only user account.

NOTE: See “Local User Management” on page 72 for more information.

Recovering a Lost Password

Select a serial port at the local computer and disable any service that uses that port. Connect a local computer to the Battery Manager through the serial port.

1. At the Battery Manager, ensure that DIP switch #7 is in the OFF position.
2. Connect the configuration cable (part number 940-0103) to the selected port on the computer and to the serial port at the Battery Manager.
3. Open a terminal program, configure the port as follows, and press `ENTER`.

```
Default baud rate  : 9600 bps
Data Bits          : 8
Parity             : None
Stop Bits          : 1
Flow Control       : None
```

NOTE: Modbus and the *Command Console* share a common serial port. In some instances, the baud rate may be set to different speeds for other services, i.e. Modbus (19200 bps).

4. Press ENTER on the computer, repeatedly, until the User Name prompt is displayed. If User Name prompt is not displayed, verify the following:
   – The serial port is not in use by another application.
   – The terminal settings are correct.
   – The correct cable is being used.
5. Press the Reset button, on the rear panel of the Battery Manager, near the network connector. The Status LED will flash alternately orange and green. Press the Reset button a second time while the LED is flashing to temporarily reset the user name and password to their default values.
6. Press ENTER as many times as necessary to redisplay the User Name prompt, then use the default, apc, for the user name and password.

   NOTE: If you take longer than 30 seconds to log on, after pressing the reset button for the second time, you must repeat step 5 and log on again.
7. At the *Command Console*, use the following commands to change the password setting for the Super User account, for which the user name is always *apc*, and the password is now temporarily *apc*:

   ```
   user -n apc -pw yourNewSuperUserPassword
   ```

   Example: to change the *Super User's* password to p@ssword type:

   ```
   user -n apc -pw p@ssword
   ```

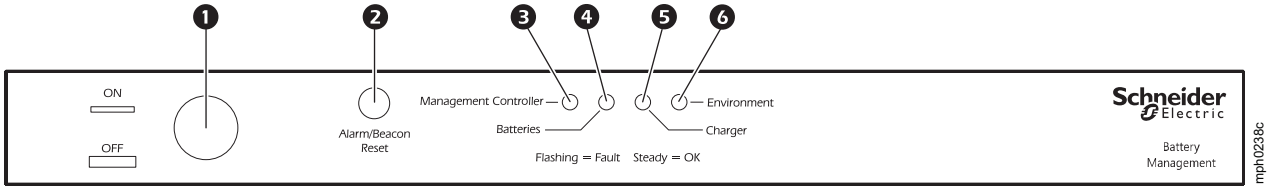
   NOTE: Because the *Super User* can also reset the password for any account, you can reset other user's passwords as well.

   Example: to change the password for user bmadmin to p@ssword type:

   ```
   user -n bmadmin -pw p@ssword
   ```

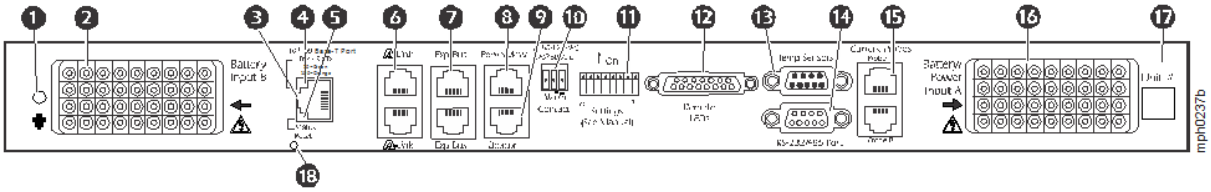
   NOTE: Changing user name information is no longer supported via the *Command Console*. If a user's user name needs to be changed, it must be deleted and re-created. The *Super User* will also have access now to log in and adjust any other user's password.
8. Type `quit`, `exit`, or `bye` to log off. Remember to reconnect any serial cable you may have disconnected, and to restart any service you may have disabled. Reset DIP switch #7 to the way that you found it.

Front Panel



	Item	Description	LED Behavior
❶	ON/OFF Button	Used to enable or disable the unit. The unit is “On” when the button is pressed in.	
❷	Alarm/Beacon Reset	Resets the alarm or beacon if either is active.	
❸	Management Controller LED	Indicates the status of the Battery Manager and its connections.	Off: The Battery Manager is not receiving power or the LED is not functioning properly. Solid: The associated status is OK. Flashing: The associated status is outside its configured limits and is in an alarm condition.
❹	Batteries LED	Indicates the status of the batteries.	
❺	Charger LED	Indicates the status of the charger’s voltage or ripple current.	
❻	Environment LED	Indicates the status of the battery environment (temperature) or external sensors.	

Rear Panel



	Item	Description
❶	Ground	Ground wire connection.
❷	Battery harness connector (B)	Connects the Battery Manager to the batteries.
❸	Network/Ethernet	Connects to the network using a CAT5 (or faster) cable.
❹	Link RX/TX LED	Indicates the status of the network connection. **Off:** • Cable from Battery Manager to network is disconnected or defective. • Device connecting Battery Manager to network is turned off or not functioning. • The Battery Manager is not receiving power, or needs to be repaired or replaced. • The Battery Manager itself is not operating properly. Contact Customer Support. **Solid Green:** connected to a network at 10 Megabits per second (Mbps). **Solid Orange:** connected to a network at 100 Mbps. **Flashing Green:** receiving or transmitting data at 10 Mbps. **Flashing Orange:** receiving or transmitting data at 100 Mbps.
❺	Status LED	Indicates the status of traffic over the network connection. **Off:** The Battery Manager is not receiving power or the NMC is in a Reboot Sequence. Contact Worldwide Customer Support. **Solid Green:** The Battery Manager has valid TCP/IP settings. **Flashing Green:** The Battery Manager does not have valid TCP/IP settings.[1] **Solid Orange:** The Battery Manager's Management Card has detected a hardware problem. Contact Customer Support. **Flashing Orange:** The Battery Manager is making BOOTP requests.[1] Alternating Green & Orange: either starting up or making DHCP requests.[1]
❻	A-Link Port (2)	Reserved for future use.
❼	Expansion Bus Ports (2)	Used to cascade one to seven AP9922S units to a single AP9922 unit.
❽	PowerView Port	Reserved for future use.
❾	Beacon	Connects to optional alarm beacon (AP9324).
❿	Alarm Contact Port	Used to connect external equipment such as an automatic dialer to signal an alarm. This is a summary alarm.
⓫	Settings (DIP Switch)	Configures the address, termination resistors and serial port mode.
⓬	Remote LEDs Port	Connects the Battery Manager to the remote alarm reset, or two auxiliary environmental inputs.
⓭	Temperature Sensors Port	Connects the temperature sensor assembly (part number 940-0089).
⓮	RS-232/485 Port	Connects to Modbus or the Command Console to configure the NMC.
⓯	Current sensor Ports (A and B)	Connects the Battery Manager to the charge/discharge string current sensors.
⓰	Battery harness connector (A)	Connects the Battery Manager to the batteries and to unit power.
⓱	Unit #	Use this space to write the number of the unit for easy identification.
⓲	NMC Reset Button	Push once to restart network interface, or use to reset the unit password.
	1) To configure the TCP/IP, BOOTP, or DHCP see "TCP/IP" on page 78.	

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the Battery Manager uses internal, system-wide watchdog mechanisms. When it restarts to recover from an internal problem, a Network Interface Restarted event is recorded in the event log.

Network Interface Watchdog Mechanism

The Battery Manager implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Battery Manager 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 and restarts its network interface.

Resetting the network timer

To ensure that the Battery Manager does not restart if the network is quiet for 9.5 minutes, the Battery Manager attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the Battery Manager, 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 reset the 9.5-minute timer frequently enough to prevent the Battery Manager from restarting.

Automatic Logout

By default, users will be automatically logged out of the Battery Manager Web and CLI interfaces after 3 minutes of inactivity.

The default logout time can be adjusted through the web interface **Configuration > Security > Local Users > Management**.

– Click the hyperlink of the user name for the account you want to change.

– Under *Session Timeout,* modify the number of minutes.

Automatic Logout	Duration (min)
Default	3
Minimum	1
Maximum	60 (1 Hr)

Command Console Access

Introduction

The *Command Console* of the Battery Manager can be accessed locally through a *serial* connection, or remotely through a secured *Telnet* or *SSH* connection. *Telnet* provides the basic security of a user name and password; *SSH* encrypts all transmitted data, including user name and password. *Telnet* is enabled by default.

More information regarding *Telnet* and *SSH* is provided in subsequent sections. Access to the *Command Console* always requires providing an authentic user name and password. User name and password are case-sensitive.

Security Lockout

If a valid user name is used with an invalid password consecutively, for the number of times specified in **Configuration > Security > Local Users > Default Settings**, the account will be locked until a *Super User* re-enables the account.

NOTE: A *Super User* cannot be locked out.

Serial Port Access to the Command Console

1. Select a serial port at the local computer, and disable any service that uses that port.
2. At the Battery Manager, ensure that DIP switch #7 is in the OFF position.
3. Connect the provided cable (part number 940-0103) to the *serial* port on the Battery Manager and to the serial port of the computer.
4. Run a terminal program (HyperTerminal, etc.), configure the port as follows, and press `ENTER`, repeatedly if needed.

```
Default baud rate     : 9600 bps
Data Bits             : 8
Parity                : None
Stop Bits             : 1
Flow Control          : None
```

5. At the prompts, enter user name and password.
6. At the end of the session, log off. Remember to reconnect any serial cable you may have disconnected, and to restart any service you may have disabled. Reset DIP switch #7 to the way that you found it.

Remote Access to the Command Console through Telnet

1. Access a computer on the same network as the Network Management Card of the Battery Manager.
2. Open a terminal program that provides telnet support or type "`telnet`" and the IP address of the Battery Manager at a DOS or command prompt and press ENTER.

   Example:

   ```
   telnet 139.225.6.133
   ```

   NOTE: The Battery Manager uses Telnet port 23 by default. If the Battery Manager has been configured to use a non-default port number (between 5000 and 32768), you must include a colon or a space (depending on your *Telnet* client) between the IP address and the port number.
3. Enter user name and password.

Remote Access to the Command Console through SSH

The only way to securely access the *Command Console* remotely, is by using the *Secure Shell*, or SSH. Data transmitted over *SSH* is encrypted using SSL (Secure Sockets Layer) encryption.

The use of *SSH* is optional, and it is not enabled by default. A properly configured *SSH* client must be installed on your computer.

The interface, user accounts and user access rights are the same whether you access the *Command Console* through *SSH* or *Telnet*.

Saving a Configuration (.ini) File

Groups of settings can be specified, saved, and distributed through the use of a .ini file. Exporting saved configurations can have many purposes and benefits for an IT team.

Identifying the benefits and methodology of integrating .ini files into your system and work flow is outside of the scope of this document. See “Contents of the .ini file” on page 106.

Command Line Interface (CLI)

Syntax and Implementation Overview

The *Command Line Interface (CLI)* is used primarily to view system status, as well as issue commands to the system. Like DOS commands in Windows or the terminal session commands in Linux, the CLI handles word-like commands. These commands have parameters and options that can be specified at the Command Console prompt.

CLI Prompt - The Battery Manager CLI prompt is the fixed string “apc>” (apc<greater than>).

Example Login Screen

```
User Name :
Password :
American Power Conversion              Network Management Card AOS v6.0.X
(c) Copyright 2012 All Rights Reserved  Battery Manager App        v6.0.X
-------------------------------------------------
Name        : Unknown                          Date  : 01/16/2013
Contact     : Unknown                          Time  : 13:10:51
Location    : Unknown                          User  : Super User
Up Time     : 0 Days 11 Hours 43 Minutes       Stat  : P+ N4+ N6+ A+
Type ? for command listing
Use tcpip command for IP address(-i), subnet(-s), and gateway(-g)

apc>
```

• The operating system (Network Management Card AOS) and Application Module (Battery Manager App) firmware versions of the device can be seen.

```
Network Management Card AOS     v6.0.x
Battery Manager App             v6.0.x
```

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

```
Name             : Unknown
Contact          : Unknown
Location         : Unknown
```

• The Up Time refers to the duration of time since the last power cycle/reset of the Battery Manager network interface.

```
Up Time  : 0 Days 11 Hours 43 Minutes
```

• The two fields Date and Time identify when the screen most recently refreshed.

```
Date     : 01/16/2013
Time     : 13:10:51
```

• The User field reports your log-in status.

```
User     : Super User
```

• The Stat field reports the Battery Manager IPv4 & IPv6 status, as well as other system variables, as seen in the following Table: *Alarm Status Field*.

```
Stat     : P+ N4+ N6+ A+
```

Alarm Status Field

The Stat field displays any active alarms for the Battery Manager.

P+	The operating system (AOS) is functioning properly.
N4+ N6+	IPv4 AND IPv6 Network Status. The network is functioning properly.
N4? N6?	A BOOTP request cycle is in progress.
N4– N6–	The Battery Manager failed to connect to the network.
N4! N6!	Another device is using the IP address of the Battery Manager.
A+	The application is functioning properly.
A–	The application has a bad checksum.
A?	The application is initializing.
A!	The application is not compatible with the AOS.

NOTE: If the AOS status is not P+, contact “Worldwide Customer Support” even if you can still access the Battery Manager.

Capitalization and Case Sensitivity

1. CLI commands and arguments ARE NOT case sensitive.
   Example:
   `portSpeed = PoRTsPeeD`
2. CLI options ARE case sensitive.
   Example:
   `-p ≠ -P`

Command Detection

If an entered command is not known, the following error message is displayed:

```
E101: Command Not Found.

Type “?” for a list of available commands. Type “<command> ?” for help
on a specific command.
```

CLI Login and Logout

On initial access to the Battery Manager, the user is always prompted to login. The user shall supply their user name and password, each followed by a carriage return. Assuming the user name and password are valid, the user will be logged into the Command Console CLI.

User name prompt: “`User Name : `" (User<space>Name<space>:<space>).

Password prompt: “`Password  : `" (Password<space><space>:<space>).

Command Argument Syntax

Since each command varies in the number of arguments it supports, the following syntax is defined to indicate when/where arguments should/could be used.

Item	Description
-	Options are preceded by a hyphen
[...]	Square brackets […] denote optional arguments
<...>	greater/less than brackets <> denote user entered text
|	The “pipe symbol” denotes OR

Argument Quoting

Argument values may optionally be enclosed in double quote characters (ASCII 0x22). String values beginning or ending with spaces, or containing commas or semicolons, must be enclosed in quotes for both input and output. Quote and backslash ("\", decimal code 92) characters appearing inside strings should NOT be encoded using traditional escape sequences (see Escape Sequences below).

All binary characters (ASCII decimal ranges 0..31, 127..159) that appear inside strings will be treated as unreadable characters and rejected. When a quote or backslash character is supplied as a part of an input string, the input string must be enclosed in double quotes.

Escape Sequences

Escape sequences, traditionally consisting of a backslash followed by a lower case letter or by a combination of digits, are ignored and should not be used to encode binary data or other special characters and character combinations.

The result of each escape sequence is parsed as if it were both a backslash and the traditionally escaped character.

Example:

```
<command> <arg1> [<agr2> <arg3a | arg3b> [<arg4a | arg4b | arg4c>]]
```

- `arg1 must be used, but arg2 - 4 are optional.`
- `If arg2 is used, then arg3a or arg3b must also be used.`
- `arg4 is optional, but arg1 - 3 must precede arg4.`

With most commands, if the last argument is omitted, the command provides information to the user, otherwise the last argument is used to change/set new information.

Example:

`apc> ftp -p` (displays the port number when omitting the arg2)

```
E000: Success
FTP Port:       5001
```

`apc> ftp -p 21` (sets the port number to arg2)

```
E000: Success
```

Command Response Codes

Error Code Table

These response codes enable the ability for automated processes to detect error conditions without resorting to matching error text.

Code	Message	Notes
E000	Success	
E001	Successfully Issued	
E002	Success, Reboot Required	
E100	Command Failed	
E101	Command Not Found	
E102	Parameter Error	Reported when there is any problem with the arguments supplied to the command, too few, too many, wrong type, etc.
E103	Command Line Error	
E104	User Level Denial	
E105	Command Prefill	Not actually used in code but it is set aside.
E106	Data Not Available	Or the provided data cannot be read.
E107	Serial Lost Communications	Serial communications with Battery Manager has been lost
E200	Input error	Only reported when an error occurs during the execution of a command
E201	No Response	Reported when a sensor fails to respond
E202	User already exists	
E203	User does not exist	
E204	User does not have access to this command	
E205	Invalid target	User failed to input a target or target was out of range.

Prompting for User Input during Command Execution

Certain commands require additional user input (ex. transfer .ini prompting for baud rate). There is a fixed timeout of 1 minute for such prompts. Should the user not enter any text within the timeout period, then the command will print "E100: Command Failed.” and the command prompt will be redisplayed.

Command Editing

The <backspace> key will delete the last character of the command string the user is currently entering and is the only editing function available to the user during command entry.

History

The Battery Manager CLI implements a command history buffer, recalling the 10 previous commands. The user can navigate backwards and forwards through entered commands using the <up arrow> and <down arrow> keys respectively.

Auto Completion

The Battery Manager CLI supports command auto-completion. If a partial command is entered, then the <TAB> key can be used to complete the command to the first available matched command. If such a match exists, the command line shall be completed by the system.

Additional presses of the <TAB> key will select the next available command match. Once all available commands have been scrolled through, the original partially entered command is displayed.

Delimiter

The Battery Manager CLI will use <space> (ASCII 0x20) as the delimiter between commands and arguments. Extra white space between commands and arguments will be ignored.

Command responses will have all fields delimited with commas for efficient parsing.

Options and Arguments Inputs

Entering a command with *no options or arguments* returns the current value of all options available from that command.

Entering the command and an option with *no arguments* returns the current value of that option only. Any command followed by a question mark "?" returns help explaining the command.

```
<space> ::=  (" " | multiple" ")
<valid letter_number> ::=   (a-z | A-Z | 0-9)
<string> ::=   (1 - 64 consecutive printable valid ASCII characters
[ranging from hex 0x20 to 0x7E inclusive] )
```

NOTE: If the string includes a blank, the entire string MUST be surrounded by quotes (" ").

```
<option> ::= "-"(<valid letter_number> | <valid letter_number><valid
letter_number>)
<argument> ::=
<helpArg> | <alarmcountArg> | <bootArg> | <cdArg> | <consoleArg> |
<dateArg> | <deleteArg> | <ftpArg> | <pingArg> | <portspeedArg> |
<promptArg> | <radiusArg> | <resettodefArg> | <systemArg> |
<tcpipArg> | <userArg> | <webArg> | <string>
<optionArg> ::= <option><argument>
```

Command Console and CLI Response Format

All **CLI** commands will issue:

`<three digit response code><:><space>` (followed by a readable text (response message))

This can be followed by <cr><lf> and the output of the command (if applicable).

Response Format and Message Codes

Successful command operations will have an error code less than 100. Any error code of 100 or greater, indicates a failure of some type.

```
E[0-9][0-9][0-9]: Error message
```

See the Error Code Table on “Error Code Table” on page 14 for more information regarding Message Code Notes.

Example:

`E000: Success` (followed by the output of the command, if applicable)

Battery Manager System Command Descriptions

Interface Commands

Courier font is used to show the text output of the Battery Manager. Italicized Courier font is used to show user input to the Battery Manager. Text enclosed in '< >' is a variable name. Each command is executable with Administrator and Device User level permissions, unless otherwise noted.The text '...' is used in several examples as a placeholder, shortening lengthy outputs. In these situations, the first two and last two lines of output will be shown.

? or help

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: View a list of all the CLI commands available to your account type. To view help text for a specific command, type the command followed by a question mark.

Parameters: `[<command>]`

Example 1:

```
apc> ?
Network Management Card Commands:
-------------------------------------------------------------------
?           about       alarmcount  boot        cd          date
delete      dir         eventlog    exit        format      ftp
help        ping        portspeed   prompt      quit        radius
reboot      resetToDef  system      tcpip       user        web
xferINI     xferStatus
```

Example 2:

```
apc> help boot
Usage: boot -- Configuration Options
   boot  [-b <dhcpBootp | dhcp | bootp | manual>] (Boot Mode)
         [-a <remainDhcpBootp | gotoDhcpOrBootp>] (After IP
Assignment)
         [-o <stop | prevSettings>] (On Retry Fail)
         [-c <enable | disable>]    (Require DHCP Cookie)
         [-s <retry then stop #>]   (Note: 0 = never)
         [-f <retry then fail #>]   (Note: 0 = never)
         [-v <vendor class>]
         [-i <client id>]
         [-u <user class>]
```

Error Message: `E000, E102`

about

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: Displays system information (Model Number, Serial Number, Manufacture Dates, etc.)

Parameters: None

Example: `apc> about`

```
E000: Success
Hardware Factory
---------------
Model Number:           AP9XXX
Serial Number:          ST0913012345
Hardware Revision:      HW05
Manufacture Date:       3/4/2013
MAC Address:            00 05 A2 18 00 01
Management Uptime:      0 Days 1 Hour 42 Minutes
```

Error Message: `E000`

alarmcount

Access: Super User, Administrator, Device User, Read Only

Description: Displays alarms present in the system.

Option	Argument	Description
-p	all	View the number of active alarms reported by the Battery Manager. Information about the alarms is provided in the event log.
	warning	View the number of active warning alarms.
	critical	View the number of active critical alarms.

Example: To view all active warning alarms, type:

```
apc> alarmcount
E000: Success
AlarmCount: 0
```

Error Message: `E000, E102`

boot

Access: Super User, Administrator

Description: Allows the user to get/set the network startup configuration of the device, such as setting boot mode (DHCP vs BOOTP vs MANUAL).

Option	Argument	Description
-b <boot mode>	dhcp | bootp | manual	Define how the TCP/IP settings will be configured when the Battery Manager turns on, resets, or restarts. See “TCP/IP” on page 78 for information about each boot mode setting.
-c	[<enable|disable>] (Require DHCP Cookie)	dhcp and dhcpBootp boot modes only. Enable or disable the requirement that the DHCP server provide the APC cookie.
-v	[<vendor class>]	Vendor Class is APC
-i	[<client id>]	The MAC address of the NMC, Which uniquely identifies it on the network.
-u	[<user class>]	The name of the application firmware module.

Example:

```
apc> boot
E000: Success

Boot Mode:              manual
DHCP Cookie:            enable
Vendor Class:           <device class>
Client ID:              XX XX XX XX XX XX
User Class:             <user class>
```

Error Message: E000, E102

bye

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: Exit the CLI

Example:

```
bye

Connection Closed - Bye
```

Error Message: None

cd

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: Allows the user to set the working directory of the file system. The working directory is set back to the root directory '/' when the user logs out of the CLI.

Parameters: `<directory name>`

Example:

```
apc> cd logs
E000: Success

apc> cd /
E000: Success
```

Error Message: `E000, E102`

clrrst

Access: Super User, Administrator

Description: Clear reset reason.

Example: None

Error Message: None

console

Access: Super User, Administrator

Description: Define whether users can access the command line interface using Telnet, which is enabled by default, or Secure SHell (SSH), which provides protection by transmitting user names, passwords, and data in encrypted form. You can change the Telnet or SSH port setting for additional security. Alternately, disable network access to the command line interface.

Parameters:

Option	Argument	Description
-S	disable | telnet | ssh	Configure access to the command line interface, or use the `disable` command to prevent access. Enabling SSH enables SCP and disables Telnet.
-t	<enable | disable>] (telnet)	
-pt	<telnet port n>	Define the Telnet port used to communicate with the Battery Manager (23 by default).
-ps	<SSH port n>	Define the SSH port used to communicate with the Battery Manager (22 by default).
-b	2400 | 9600 | 19200 | 38400	Configure the speed of the serial port connection (9600 bps by default).

Example 1: To enable SSH access to the command line interface, type:

```
console -S ssh
```

Example 2: To change the Telnet port to 5000, type:

```
console -pt <5000>
Telnet:      enabled
SSH:         disabled
Telnet Port: 23
SSH Port:    22
Baud Rate:   9600Parameters:
```

date

Access: Super User, Administrator

Definition: Get and set the date and time of the system.

To configure an NTP server to define the date and time for the Battery Manager, see “Set the Date and Time” on page 102.

Parameters:

Option	Argument	Description
-d	<"datestring">	Set the current date. The format must match the current -f setting.
-t	<00:00:00>	Configure the current time, in hours, minutes, and seconds. Use the 24-hour clock format.
-f	mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Select the numerical format in which to display all dates in this user interface. Each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.
-z	<time zone offset>	Set the difference with GMT in order to specify your time zone. This enables you to synchronize with other people in different time zones.

Example 1: To display the date using the format yyyy-mm-dd, type:

```
date -f yyyy-mm-dd
```

Example 2: To define the date as July 4, 2014, type:

```
date -d "2014-07-04"
```

Example 3: To define the time as 5:21:03 p.m., type:

```
date -t 17:21:03
```

Error Message: E000, E100, E102

delete

Access: Super User, Administrator

Description: Delete a file in the file system.

Parameters:

Argument	Description
<file name>	Type the name of the file to delete.

Example:

```
apc> delete /db/prefs.dat
E000: Success
```

Error Messages: E000, E102

dir

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: Displays the content of the working directory.

Example:

```
apc> dir
E000: Success
--wx-wx-wx  1 apc      apc      3145728 Mar 3  2013 aos.bin
--wx-wx-wx  1 apc      apc      3145728 Mar 4  2013 app.bin
-rw-rw-rw-  1 apc      apc        45000 Mar 6  2013 config.ini
drwxrwxrwx  1 apc      apc            0 Mar 3  2013 ssl/
drwxrwxrwx  1 apc      apc            0 Mar 3  2013 ssh/
drwxrwxrwx  1 apc      apc            0 Mar 3  2013 logs/
drwxrwxrwx  1 apc      apc            0 Mar 3  2013 sec/
drwxrwxrwx  1 apc      apc            0 Mar 3  2013 dbg/
drwxrwxrwx  1 apc      apc            0 Mar 3  2013 fwl/
drwxrwxrwx  1 apc      apc            0 Mar 3  2013 rms/
```

Error Messages: `E000`

dns

Access: Super User, Administrator, Network Only User

Definition: Configure the manual Domain Name System (DNS) settings.

Parameter	Argument	Description
`-OM`	`<enable | disable>`	Override the manual DNS.
`-p`	`<primary DNS server>`	Set the primary DNS server.
`-s`	`<secondary DNS server>`	Set the secondary DNS server.
`-d`	`<domain name>`	Set the domain name.
`-n`	`<domain name IPv6>`	Set the domain name IPv6.
`-h`	`<host name>`	Set the host name.
`-y`	`<enable | disable>`	System-hostname sync

Example: None

Error Message: `E000`

email

Access: Super User, Administrator, Network Only User

Description: View email

Parameters:

Parameters	Argument
-g[n]	<enable | disable> (Generation)
-t[n]	<To Address>
-o[n]	<long | short> (Format)
-l[n]	<Language Code>
-r [n]	<Local | recipient | custom> (Route)
Custom Route Option	
-f[n]	<From Address>
-s{n}	<SMTP Server>
-p[n]	<Port>
-a[n]	<enable | disable> (Authentication)
-u[n]	<User Name>
-w[n]	<Password>
-e[n]	<none | ifsupported | always | implicit> (Encryption)
-c[n]	<enable | disable > (Required Certificate)
-i[n]	<Certificate File Name>
n=	Email Recipient Number 1,2,3 or 4)

Example: None

Error Message: None

eventlog

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: View the date and time you retrieved the event log, the status of the Battery Manager, and the status of sensors connected to the Battery Manager. View the most recent device events and the date and time they occurred. Use the following keys to navigate the event log:

Key	Description
ESC	Close the event log and return to the command line interface.
ENTER	Update the log display. Use this command to view events that were recorded after you last retrieved and displayed the log.
SPACEBAR	View the next page of the event log.
B	View the preceding page of the event log. This command is not available at the main page of the event log.
D	Delete the event log. Follow the prompts to confirm or deny the deletion. Deleted events cannot be retrieved.

Example:

```
apc> eventlog
---- Event Log -------------------------------------------------
     Date: 03/06/2009      Time: 13:22:26
     ----------------------------------

Date        Time      Event
     ------------------------------------------------------------
     03/06/2009  13:17:22  System: Set Time.
     03/06/2009  13:16:57  System: Configuration change. Date format
                           preference.
     03/06/2009  13:16:49  System: Set Date.
     03/06/2009  13:16:35  System: Configuration change. Date format
                           preference.
     03/06/2009  13:16:08  System: Set Date.
     03/05/2009  13:15:30  System: Set Time.
     03/05/2009  13:15:00  System: Set Time.
     03/05/2009  13:13:58  System: Set Date.
     03/05/2009  13:12:22  System: Set Date.
     03/05/2009  13:12:08  System: Set Date.
     03/05/2009  13:11:41  System: Set Date.
<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

Error Message: E000, E100

exit or quit

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: Exit from the CLI session.

Parameters: None

Example:

```
apc> exit
Bye
```

Error Message: None

firewall

Access: Super User, Administrator

Description: Establishes a barrier between a trusted, secure internal network and another network.

Parameters:

Parameters	Argument	Description
-S	<enable | disable>	Enable or disable the Firewall.
-f	<file name to activate>	Name of the firewall to activate.
-t	<file name to test> <duration time in minutes>	Name of firewall to test and duration time in minutes.
-fe	No argument. List only	Shows active file errors.
-te	No argument. List only	Shows test file errors.
-c	No argument. List only	Cancel a firewall test.
-r	No argument. List only	Shows active firewall rules.
-l	No argument. List only	Shows firewall activity log.

Error Message: None

format

Access: Super User, Administrator

Description: Allows the user to format the FLASH file system. This will delete all configuration data, event and data logs, certificates and keys.

Example:

```
apc> format

Format FLASH file system

Warning: This will delete all configuration data,
event and data logs, certs and keys.

Enter 'YES' to continue or <ENTER> to cancel:
apc>
```

Error Message: None

ftp

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: Get/set the ftp configuration data,

NOTE: The system will reboot if any configuration is changed.

Option	Argument	Definition
-p	<port number> (valid ranges are: 21 and 5000-32768)	Define the TCP/IP port that the FTP server uses to communicate with the Battery Manager (21 by default). The FTP server uses both the specified port and the port one number lower than the specified port.
-S	enable | disable	Configure access to the FTP server.

Example: To change the TCP/IP port to 5001, type:

```
apc> ftp -p 5001
E000: Success

apc> ftp
E000: Success

Service: Enabled
Ftp Port: 5001

apc> ftp -p 21
E000: Success
```

Error Message: E000, E102

help

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: View a list of all the CLI commands available to your account type. To view help text for a specific command, type the command followed by `help`.

Example 1: To view a list of commands available to a Device User, type:

```
help
```

Example 2: To view a list of options that are accepted by the `alarmcount` command, type:

```
alarmcount help
```

Error Message: None

lang

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: Language in use

Example: `Languages enUs - English`

Error Message: None

lastrst

Access: Super User, Administrator

Description: Last reset reason

Parameters: `Usage: lastrst -- Last reset reason`

Example:

```
09 Coldstart Reset
E000: Success
```

Error Message: None

ledblink

Access: Super User, Administrator

Description: Sets the blink rate to the LED on the Battery Manager.

Parameters: None

Example:

```
usage: ledblink -- Configuration Options ledblink
```

Error Message: None

logzip

Access: Super User, Administrator

Description: Places large logs into a zip file before sending.

Parameters:

```
Usage: logzip --  Configuration Options
logzip [-m <email recipient>] (email recipient number (1-4))
```

Example:

```
Generating files
Compressing files into /dbg/debug_ZA1023006009.tar
E000: Success
```

Error Message: `E000`

netstat

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: Displays incoming and outgoing network connections.

Parameters:

```
Usage: netstat -- Configuration Options netstat
```

Example:

```
Current IP Information:
Family mHome Type   IPAddress
Status
IPv6   4     auto   FE80::2C0:B7FF:FE51:F304/64
configured
IPv6   0     manual ::1/128
configured
IPv4   0     manual 127.0.0.1/32
configured
```

Error Message: None

ntp

Access: Super User, Administrator, Network Only User

Description: Synchronizes the time of a computer client or server.

Option	Argument	Definition
-OM	enable | disable	Override the manual settings.
-p	<primary NTP server>	Specify the primary server.
-s	<secondary NTP server>	Specify the secondary server.

Example 1: To enable the override of manual setting, type:

```
ntp -OM enable
```

Example 2: To specify the primary NTP server, type:

```
ntp -p 150.250.6.10
```

Error Message: E000

ping

Access: Super User, Administrator, Device User, Network Only User

Description Perform a network 'ping' to any external network device.

Argument	Description
<IP address or DNS name>	Type an IP address with the format *xxx.xxx.xxx.xxx*, or the DNS name configured by the DNS server.

Example:

```
apc> ping 192.168.1.50
E000: Success
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
```

Error Message: E000, E100, E102

portSpeed

Access: Super User, Administrator, Network Only User

Description: Allows the user to get/set the network port speed.

NOTE: The system will reboot if any configuration is changed.

Option	Arguments	Description
-s	auto | 10H | 10F | 100H | 100 F	Define the communication speed of the Ethernet port. The auto command enables the Ethernet devices to negotiate to transmit at the highest possible speed. See “Port Speed” on page 79 for more information about the port speed settings.
H = Half Duplex F = Full Duplex		10 = 10 Meg Bits 100 = 100 Meg Bits

Example:

```
apc> portspeed
E000: Success
Port Speed: 10 Half_Duplex

apc> portspeed -s 10h
E000: Success

apc> portspeed
E000: Success
Port Speed: 10 Half_Duplex

apc> portspeed -s auto
E000: Success
```

Error Message: E000, E102

prompt

Access: Super User, Administrator, Device User, Network Only User

Description: Allows the user to change the format of the prompt, either short or long.

Option	Argument	Description
-s	long	The prompt includes the account type of the currently logged-in user.
	short	The default setting. The prompt is four characters long: APC>

Example:

```
apc> prompt –s long
E000: Success

Administrator@apc>prompt –s short
E000: Success
```

Error Message: E000, E102

pwd

Access: Super User, Administrator, Device User, Read Only, Network Only User

Description: Used to output the path of the current working directory.

Parameters: `pwd`

Example: `Usage: pwd --  Configuration Options`

Error Message: None

radius

Access: Super User, Administrator

Description: View the existing RADIUS settings, enable or disable RADIUS authentication, and configure basic authentication parameters for up to two RADIUS servers.

Additional authentication parameters for RADIUS servers are available at the Web interface of the Battery Manager.

For a summary of RADIUS server configuration and a list of supported RADIUS servers, see “TCP/IP” on page 78.

For detailed information about configuring your RADIUS server, see the *Security Handbook*, available at **www.apc.com**.

Option	Argument	Description
`-a`	`local | radiusLocal | radius`	Configure RADIUS authentication: `local`—RADIUS is disabled. Local authentication is enabled. `radiusLocal`—RADIUS, then Local Authentication. RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used. `radius`—RADIUS is enabled. Local authentication is disabled.

`-p1`
`-p2`
`-o1`
`-o2`
	`<server IP>`	The server name or IP address of the primary or secondary RADIUS server.
		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. The Battery Manager supports ports 1812, 5000 to 32768.

`-s1` `-s2`	`<server secret>`	The shared secret between the primary or secondary RADIUS server and the Battery Manager.
`-t1` `-t2`	`<server timeout>`	The time in seconds that the Battery Manager waits for a response from the primary or secondary RADIUS server.

Example 1: To view existing RADIUS settings for the Battery Manager, type `radius` and press ENTER.

Example 2: To enable RADIUS and local authentication, type:

```
radius -a radiusLocal
```

Example 3: To configure a 10-second timeout for a secondary RADIUS server, type:

```
radius -t2 10
```

Error Message: `E000, E102`

reboot

Access: Super User, Administrator, Network Only User

Description: Restart the Battery Manager interface only. Forces the network device to reboot. User must confirm this operation by entering a “YES” after the command has been entered.

Parameters: None

Example:

```
apc> reboot
E000: Success
Reboot Management Interface
Enter 'YES' to continue or <ENTER> to cancel : <user enters ‘YES’>
Rebooting...
```

Error Message: E000, E100

resetToDef

Access: Super User, Administrator

Description: Reset all parameters to their default.

Option	Arguments	Description
-p	all | keepip	all = all configuration data, including the IP address. keepip -= all configuration data, except the IP address. Reset all configuration changes, including event actions, device settings, and, optionally, TCP/IP configuration settings.

Example: To reset all of the configuration changes *except* the TCP/IP settings for the Battery Manager, type:

```
resetToDef -p keepip
Enter 'YES' to continue or <ENTER> to cancel : : <user enters ‘YES’>
all User Names, Passwords.
Please wait...
Please reboot system for changes to take effect!
```

Error Message: E000, E100

session

Access: Super User, Administrator

Description: Records who is logged in(user), the interface, the Address, time and ID.

Parameters:

Option	Arguments
Session	[-d <session nID>] (Delete)
-m	<Enable | disable> (Multi-User Enable)
-a	<enable | disable (Remote Authentication Override)

Example:

```
User              Interface         Address           Logged In Time    ID
-------------------------------------------------------------------------

apc               Serial                              00:00:05          1
```

Error Message: E000

smtp

Access: Super User, Administrator

Description: Internet standard for electronic mail.

Option	Argument
-f	<From Address
-s	<SMTP Server>
-p	<Port> [1]
-a	<enable | disable> (Authentication)
-u	<User Name>
-w	<Password>
-e	<none | ifavail | always | implicit> (Encryption)
-c	<enable | disable> (Require Certificate)
-i	<Certificate File Name>
[1]Port options are 25, 465, 587, 5000 to 32768	

Example:

```
From:          address@example.com
Server:        mail.example.com
Port:          25
Auth:          disabled
User:          User
Password:      <not set>
Encryption:    none
Req. Cert:     disabled
Cert File:     <n/a>
```

Error Message: E000

snmp

Access: Super User, Administrator,Network Only User

Description: Enable or disable SNMP.

Option	Arguments	Description
-c	<Community>	Identify the group of Battery Managers
-a	<read | write | writeplus | disable>	Set the access level
-n	<IP or Domain Name>	The host's name or address
-S	enable | disable	Enable or disable the respective version of SNMP

Example: To enable SNMP version 1, type:

```
Access Control #:     1
Community:            public
Access Type:          read
Address:              0.0.0.0

Access Control #:     2
Community:            private
Access Type:          write +
Address:              0.0.0.0
```

Error Message: None

snmpv3

Access: Super User, Administrator, Network Only User

Description: Enable or disable SNMP 3

.

Option	Arguments	Description
-S	enable | disable	Enable or disable the respective version of SNMP
-u[n]	<User Name>	User Name
-a[n]	<Auth phrase>	Authphrase of User profile
-c[n]	<Crypth phrase>	Crypthphrase of User profile
-ap[n]	<sha | md5 | none>	Authentication Protocol
-pp[n]	<aes | des | none>	Privacy Protocol
-ac[n]	<enable | disable>	Access
-au[n]	<User Profile Name>	Access User Profile
-n[n]	<IP or Domain Name>	The host's name or address

Example: To enable SNMP version 3, type:

```
Access Control #:     3
Community:            public
Access Type:          read
Address:              0.0.0.0

Access Control #:     2
Community:            private
Access Type:          write +
Address:              0.0.0.0
```

Error Message: None

snmptrap

Access: Super User, Administrator, Network Only User

Description: Enable or disable SNMP trap generation

Parameters:

Option	Arguments
-c{n}	<Community>
-r[n]	<Receiver NMS IP>
-l[n]	<Language> [language code]
-t[n]	<Trap Type> [snmpV1 | snmpV3]]
-g[n]	<Generation> [enable | disable]
-a[n]	<Auth Trap> [enable | disable]
-u[n]	<profile1 | profile2 | profile3 | profile4> (User Name)
n=Trap receiver # = 1,2,3,4,5 or 6	

Error Message: None

system

Access: Super User, Administrator

Description: View and set the system name, the contact, the location and view up time as well as the date and time, the logged-on user, and the high-level system status P, N, A (see “Syntax and Implementation Overview” on page 11 for more information about system status).

Option	Argument	Description
-n	<system-name>	Define the device name, the name of the person responsible for the device, and the physical location of the device. **NOTE:** These values are also used by StruxureWare and the Battery Managers SNMP agent.
-c	<system-contact>	
-l	<system-location>	
-m	<system-message>	When defined, a custom message will appear on the log on screen for all users.
-s	<enable | disable>] (system-hostname sync)	Allow the host name to be synchronized with the system name so both fields automatically contain the same value. **NOTE:** When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the host name field).

Example 1: To set the device location as `Test Lab`, type:

```
system -l “Test Lab”
```

Example 2: To set the system name as `Rack 5`, type:

```
system -n “Rack 5”
```

tcpip

Access: Super User, Administrator, Network Only User

Description: View and manually configure these network settings for the Battery Manager:

Option	Argument	Description
-i	<IP address>	Type the IP address of the Battery Manager using the format *xxx.xxx.xxx.xxx*
-s	<subnet mask>	Type the subnet mask for the Battery Manager.
-g	<gateway>	Type the IP address of the default gateway. **Do not** use the loopback address (127.0.0.1) as the default gateway.
-d	<domain name>	Type the DNS name configured by the DNS server.
-h	<host name>	Type the host name that the Battery Manager will use.
-S	enable | disable	Enable or disable IPv4.

Example 1: To view the network settings of the Battery Manager, type `tcpip` and press ENTER.

Example 2: To manually configure an IP address of `150.250.6.10` for the Battery Manager, type:

```
tcpip -i 150.250.6.10
```

tcpip6

Access: Super User, Administrator, Network Only User

Description: Enable IPv6 and view and manually configure these network settings for the Battery Manager:

Option	Argument	Description
-S	enable | disable	Enable or disable IPv6.
-man	enable | disable	Enable manual addressing for the IPv6 address of the Battery Manager.
-auto	enable | disable	Enable the Battery Manager to automatically configure the IPv6 address.
-i	<IPv6 address>	Set the IPv6 address of the Battery Manager.
-g	<IPv6 gateway>	Set the IPv6 address of the default gateway.
-d6	router | statefull | statelss | never	Set the DHCPv6 mode, with parameters of router controlled, statefull (for address and other information, they maintain their status), stateless (for information other than address, the status is not maintained), never.

Example 1: To view the network settings of the Battery Manager, type:

`tcpip6` and press ENTER.

Example 2: To manually configure an IPv6 address of `2001:0:0:0:0:FFD3:0:57ab for the` Battery Manager, type:

```
tcpip6 -i 2001:0:0:0:0:FFD3:0:57ab
```

user

Access: Super User, Administrator

Description: Configure the user name, password, and inactivity timeout for each account types. You can't edit a user name, you must delete it and then create a new user. For information on the permissions granted to each account type, see "User Account Overview" on page 4.

Option	Argument	Description
-n	<user>	Specify these options for a user.
-pw	<user password>	
-pe	<user permission>	
-d	<user description>	
-e	enable | disable	Enable overall access.
-st	<session timeout>	Specify how long a session lasts waits before logging off a user when the keyboard is idle.
-sr	enable | disable	Bypass RADIUS by using the serial console (CLI) connection, also known as Serial Remote Authentication Override
-el	enable | disable	Indicate the Event Log color coding.
-lf	tab | csv	Indicate the format for exporting a log file.
-ts	us | metric	Indicate the temperature scale, fahrenheit or celsius.
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd>	Specify a date format.
-lg	<language code (e.g. enUs)>	Specify a user language.
-del	<user name>	Delete a user.
-l		Display the current user list.

Example: To change the log off time to 10 minutes, type:

```
user -n <user> -st 10
```

userdflt

Access: Super User, Administrator

Description: Complimentary function to “user” establishing default user preferences. There are two main features for the default user settings:

- Determine the default values to populate in each of the fields when the Super User or Administrator-level account creates a new user. These values can be changed before the settings are applied to the system.
- For remote users (user accounts not stored in the system that are remotely authenticated such as RADIUS) these are the values used for those that are not provided by the authenticating server.

  For example, if a RADIUS server does not provide the user with a temperature preference, the value defined in this section will be used.

Parameters:

Options	Argument	Description
-e	<enable | disable> (Enable)	By default, user will be enabled or disabled upon creation. Remove (Enable) from the end
-pe	<Administrator | Device | Read-Only | Network-Only> (user permission)	Specify the user's permission level and account type.
-d	<user description>	Provide a user description.
-st	<session timeout> minute(s)	Provide a default session timeout.
-bl	<bad login attempts>	Number of incorrect login attempts a user has before the system disables their account. Upon reaching this limit, a message is displayed informing the user the account has been locked. The Super User or an Administrator-level account is needed to re-enable the account to allow the user to log back in. **NOTE:** A Super User account cannot be locked out, but can be manually disabled if necessary.
-el	<enable | disable> (Event Log Color Coding)	Enable or disable event log color coding.
-lf	<tab | csv> (Export Log Format)	Specify the log export format, tab or CSV.
-ts	<us | metrics> (Temperature Scale)	Specify the user's temperature scale. This setting is also used by the system when a user preference is not available (for example, email notifications).
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd> (Date Format)	Specify the user's preferred date format.
-lg	<language code (enUs, etc)>	User language
-sp	<enable | disable>	Strong password
-pp	<interval in days>	Required password change interval

Error Message: None

web

Access: Super User, Administrator, Network Only User

Description: Enable access to the Web interface using HTTP or HTTPS.

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

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

Parameters:

Option	Argument	Definition
-h	enable | disable	Enable or disable access to the user interface for HTTP.
-s	enable | disable	Enable or disable access to the user interface for HTTPS. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate.
-ph	<http port #>	Specify the TCP/IP port used by HTTP to communicate with the Battery Manager (80 by default). The other available range is 5000–32768.
-ps	<https port #>	Specify the TCP/IP port used by HTTPS to communicate with the Battery Manager (443 by default). The other available range is 5000–32768.

Example 1: To prevent all access to the web interface, type:

```
web -s disable
```

Example 2: To define the TCP/IP port used by HTTP, type:

```
apc> web
E000: Success
Service:        http
Http Port:      5000
Https Port:     443

apc> web -ph 80
E000: Success
```

Error Message: E000, E102

whoami

Access: Super User, Administrator, Device Only, Read Only, Network Only User

Description: Provides login information on the current user.

Parameters: None

Example:

```
apc> whoami
E000: Success
apc>
```

Error Message: None

xferINI

Access: Super User, Administrator

Description: Use XMODEM to upload an INI file while you are accessing the command line interface through a serial connection. After the upload completes:

- If there are any system or network changes, the command line interface restarts and you must log on again.
- If you selected a baud rate for the file transfer that is not the same as the default baud rate for the Battery Manager, you must reset the baud rate to the default to reestablish communication with the Battery Manager.

Parameters: None

Example:

```
apc> xferINI
Enter 'YES' to continue or <ENTER> to cancel : <user enters 'YES'>
------- File Transfer Baud Rate------------------------------
       1- 2400
       2- 9600
       3- 19200
       4- 38400
> <user enters baudrate selection>
Transferring at current baud rate (9600), press <ENTER>...
<user presses <ENTER>>
Start XMODEM-CRC Transfer Now!
CC
<user starts sending INI>
150 bytes have successfully been transmitted.
apc>
```

Error Message: None

xferStatus

Access: Super User, Administrator

Description: View the result of the last file transfer. See “Verifying Upgrades” on page 114 for descriptions of the transfer result codes.

Parameters: None

Example:

```
apc> xferStatus
E000: Success
Result of last file transfer: Failure unknown
```

Error Message: `E000`

Battery Manager Device Command Descriptions

Interface Commands

Courier font is used to show the text output of the Battery Manager. Italicized Courier font is used to show user input to the Battery Manager. Text enclosed in '< >' is a variable name. Each command is executable with Administrator and Device User level permissions, unless otherwise noted.The text '...' is used in several examples as a placeholder, shortening lengthy outputs. In these situations, the first two and last two lines of output will be shown.

almBat

Description: Display Batteries Alarm Status. (Normal, Warning, Critical, CritWarn, Informational)

Parameters: None

Example:

```
apc> almBat
Batteries Alarm Status
  Batteries Alarm Status: Normal
E000: Success
```

Error Messages: `E000, E102`

almChr

Description: Display Charger Alarm Status. (Normal, Warning, Critical, CritWarn, Informational)

Parameters: None

Example:

```
apc> almChr
Charger Alarm Status
  Charger Alarm Status: Normal
E000: Success
```

Error Messages: `E000, E102`

almCont

Description: Display Management Controller Alarm Status, (Normal, Warning, Critical, CritWarn, Informational)

Parameters: None

Example:

```
apc> almCont
Management Controller Alarm Status
  Management Controller Alarm Status: Normal
E000: Success
```

Error Messages: `E000, E102`

almEnv

Description: Display Environment Alarm Status (Normal, Warning, Critical, CritWarn, Informational)

Parameters: None

Example:

```
apc> almEnv
Environment Alarm Status
  Environment Alarm Status: Normal
E000: Success
```

Error Messages: E000, E102

ambientTemp

Description: Display Ambient Temperature

Parameters: None

Example:

```
apc> ambientTemp
Ambient Temperature
  Ambient Temperature: 22.2 C
E000: Success
```

Error Messages: E000, E102

batCharge

Description: Display String # Battery # Response Percent Change

Parameters: [string# [battery#]]

Example 1:

```
apc> batCharge
String # Battery # Response Percent Change
  String 1 Battery 1 Response Percent Change: 0 %
  String 1 Battery 2 Response Percent Change: 0 %
  ...
  String 2 Battery 243 Response Percent Change: 0 %
  String 2 Battery 244 Response Percent Change: 0 %
E000: Success
```

Example 2:

```
apc> batCharge 1 1
String # Battery # Response Percent Change
  String 1 Battery 1 Response Percent Change: 0 %
E000: Success
```

Error Messages: E000, E102

batChrAlrm

Description: Display String # Battery # Response Alarm Status (Normal, High)

Parameters: [string# [battery#]]

Example 1:

```
apc> batChrAlrm
String # Battery # Response Alarm Status
  String 1 Battery 1 Response Alarm Status: Normal
  String 1 Battery 2 Response Alarm Status: Normal
  ...
  String 2 Battery 243 Response Alarm Status: Normal
  String 2 Battery 244 Response Alarm Status: Normal
E000: Success
```

Example 2:

```
apc> batChrAlrm 1
String # Battery # Response Alarm Status
  String 1 Battery 1 Response Alarm Status: Normal
E000: Success
```

Example 3:

```
apc> batChrAlrm 1 4
String # Battery # Response Alarm Status
  String 1 Battery 4 Response Alarm Status: Normal
E000: Success
```

Error Messages: E000, E102

batDisAlrm

Description: Display String # Battery # Discharge Voltage Alarm Status (Normal, Low)

Parameters: [string# [battery#]]

Example 1:

```
apc> batDisAlrm
String # Battery # Discharge Voltage Alarm Status
  String 1 Battery 1 Discharge Voltage Alarm Status: Normal
  String 1 Battery 2 Discharge Voltage Alarm Status: Normal
  ...
  String 2 Battery 243 Discharge Voltage Alarm Status: Normal
  String 2 Battery 244 Discharge Voltage Alarm Status: Normal
E000: Success
```

Example 2:

```
apc> batDisAlrm 1 1
String # Battery # Discharge Voltage Alarm Status
  String 1 Battery 1 Discharge Voltage Alarm Status: Normal
E000: Success
```

Error Messages: E000, E102

batDisVolt

Description: Display String # Battery # Lowest Discharge Voltage

Parameters: [string# [battery#]]

Example 1:

```
apc> batDisVolt
String # Battery # Lowest Discharge Voltage
  String 1 Battery 1 Lowest Discharge Voltage: 1.800 Vdc
  String 1 Battery 2 Lowest Discharge Voltage: 1.800 Vdc
  ...
  String 2 Battery 243 Lowest Discharge Voltage: 1.800 Vdc
  String 2 Battery 244 Lowest Discharge Voltage: 1.800 Vdc
E000: Success
```

Example 2:

```
apc> batDisVolt 1 1
String # Battery # Lowest Discharge Voltage
  String 1 Battery 1 Lowest Discharge Voltage: 1.800 Vdc
E000: Success
```

Error Messages: E000, E102

batOhms

Description: Display String # Battery # Ohmic Value

Parameters: [string# [battery#]]

Example 1:

```
apc> batOhms
String # Battery # Ohmic Value
  String 1 Battery 1 Ohmic Value: 2 mOhms
  String 1 Battery 2 Ohmic Value: 2 mOhms
  ...
  String 2 Battery 243 Ohmic Value: 2 mOhms
  String 2 Battery 244 Ohmic Value: 2 mOhms
E000: Success
```

Example 2:

```
apc> batOhms 1 1
String # Battery # Ohmic Value
  String 1 Battery 1 Ohmic Value: 2 mOhms
E000: Success
```

Error Messages: E000, E102

batVolt

Description: Display String # Battery # Voltage

Parameters: [string# [battery#]]

Example 1:

```
apc> batVolt
String # Battery # Voltage
  String 1 Battery 1 Voltage: 2.200 Vdc
  String 1 Battery 2 Voltage: 2.200 Vdc
  ...
  String 2 Battery 243 Voltage: 2.200 Vdc
  String 2 Battery 244 Voltage: 2.200 Vdc
E000: Success
```

Example 2:

```
apc> batVolt 1
String # Battery # Voltage
  String 1 Battery 1 Voltage: 2.200 Vdc
  String 1 Battery 2 Voltage: 2.200 Vdc
  ...
  String 1 Battery 244 Voltage: 2.200 Vdc
  String 1 Battery 245 Voltage: Err.34 data error
E100: Command Failed
```

Example 3:

```
apc> batVolt 1 1
String # Battery # Voltage
  String 1 Battery 1 Voltage: 2.200 Vdc
E000: Success
```

Error Messages: E000, E102

batVoltAlrm

Description: Display String # Battery # Voltage Alarm Status (Normal, Chemistry_High, User_High, Chemistry_Low, User_Low)

Parameters: [string# [battery#]]

Example 1:

```
apc> batVoltAlrm
String # Battery # Voltage Alarm Status
  String 1 Battery 1 Voltage Alarm Status: Normal
  String 1 Battery 2 Voltage Alarm Status: Normal
  ...
  String 2 Battery 243 Voltage Alarm Status: Normal
  String 2 Battery 244 Voltage Alarm Status: Normal
E000: Success
```

Example 2:

```
apc> batVoltAlrm 1 1
String # Battery # Voltage Alarm Status
  String 1 Battery 1 Voltage Alarm Status: Normal
E000: Success
```

Error Messages: E000, E102

calACCurZ

Description: Display or Change String # AC Current Zero Calibration

Parameters: [string# [value]]

Example 1:

```
apc> calACCurZ
String # AC Current Zero Calibration
  String 1 AC Current Zero Calibration: 0.0 A
  String 2 AC Current Zero Calibration: 0.0 A
E000: Success
```

Example 2:

```
apc> calACCurZ 2 1
String # AC Current Zero Calibration
  String 2 AC Current Zero Calibration: 1.0 A
E000: Success
```

Error Messages: `E000, E102`

calBatTrOhm

Description: Display or Change String # Battery # Inter-Tier Ohmic Value

Parameters: [string# [battery# [value]]]

Example 1:

```
apc> calBatTrOhm
String # Battery # Inter-Tier Ohmic Value
  String 1 Battery 1 Inter-Tier Ohmic Value: 0 mOhms
  String 1 Battery 2 Inter-Tier Ohmic Value: 0 mOhms
  ...
  String 2 Battery 243 Inter-Tier Ohmic Value: 0 mOhms
  String 2 Battery 244 Inter-Tier Ohmic Value: 0 mOhms
E000: Success
```

Example 2:

```
apc> calBatTrOhm 1 1
String # Battery # Inter-Tier Ohmic Value
  String 1 Battery 1 Inter-Tier Ohmic Value: 0 mOhms
E000: Success
```

Error Messages: `E000, E102`

calDCCurZ

Description: Display or Change String # DC Current Zero Calibration

Parameters: [string# [value]]

Example 1:

```
apc> calDCCurZ
String # DC Current Zero Calibration
  String 1 DC Current Zero Calibration: 0.0 A
  String 2 DC Current Zero Calibration: 0.0 A
E000: Success
```

Example 2:

```
apc> calDCCurZ 2 1
String # DC Current Zero Calibration
  String 2 DC Current Zero Calibration: 1.0 A
E000: Success
```

Error Messages: E000, E102

calDCVoltS

Description: Display or Change Unit # DC Voltage Span Calibration

Parameters: [unit# [value]]

Example 1:

```
apc> calDCVoltS
Unit # DC Voltage Span Calibration
  Unit 1 DC Voltage Span Calibration: 100.00 %
  Unit 2 DC Voltage Span Calibration: 100.00 %
  ...
  Unit 7 DC Voltage Span Calibration: 100.00 %
  Unit 8 DC Voltage Span Calibration: 100.00 %
E000: Success
```

Example 2:

```
apc> calDCVoltS 1 99
Unit # DC Voltage Span Calibration
  Unit 1 DC Voltage Span Calibration: 99.00 %
E000: Success
```

Error Messages: E000, E102

calDCVoltZ

Description: Display or Change Unit # DC Voltage Zero Calibration

Parameters: [unit# [value]]

Example 1:

```
apc> calDCVoltZ
Unit # DC Voltage Zero Calibration
  Unit 1 DC Voltage Zero Calibration: 0.000
  Unit 2 DC Voltage Zero Calibration: 0.000
  ...
  Unit 7 DC Voltage Zero Calibration: 0.000
  Unit 8 DC Voltage Zero Calibration: 0.000
E000: Success
```

Example 2:

```
apc> calDCVoltZ 1 1
Unit # DC Voltage Zero Calibration
  Unit 1 DC Voltage Zero Calibration: 1.000
E000: Success
```

Error Messages: `E000, E102`

calOhmicCor

Description: Display or Change Ohmic Correction Factor

Parameters: [value]

Example 1:

```
apc> calOhmicCor
Ohmic Correction Factor
  Ohmic Correction Factor: 100 %
E000: Success
```

Example 2:

```
apc> calOhmicCor 98
Ohmic Correction Factor
  Ohmic Correction Factor: 98 %
E000: Success
```

Error Messages: `E000, E102`

calPrbType

Description: Display or Change String # Current Sensor Type (1000A, 500A, 200A, 100A, 2000A)

Parameters: [string# [value]]

Example 1:

```
apc> calPrbType
String # Current Sensor Type
  String 1 Current Sensor Type: 1000A
  String 2 Current Sensor Type: 1000A
E000: Success
```

Example 2:

```
apc> calPrbType 1 100A
String # Current Sensor Type
  String 1 Current Sensor Type: 100A
E000: Success
```

Example 3:

```
apc> calPrbType 1 10004~A    0A
String # Current Sensor Type
  String 1 Current Sensor Type: 1000A
E000: Success
```

Error Messages: E000, E102

cfgAtoAnRst

Description: Display or Change Automatic Annunciator Reset (Disabled, Enabled)

Parameters: [value]

Example 1:

```
apc> cfgAtoAnRst
Automatic Annunciator Reset
  Automatic Annunciator Reset: Enabled
E000: Success
```

Example 2:

```
apc> cfgAtoAnRst Disabled
Automatic Annunciator Reset
  Automatic Annunciator Reset: Disabled
E000: Success
```

Error Messages: E000, E102

cfgBatAH

Description: Display or Change Battery Rating

Parameters:[value]

Example 1:

```
apc> cfgBatAH
Battery Rating
  Battery Rating: 121 Ah
E000: Success
```

Example 2:

```
apc> cfgBatAH 120
Battery Rating
  Battery Rating: 120 Ah
E000: Success
```

Error Messages: E000, E102

cfgBatType

Description: Display or Change Battery Chemistry (LeadAcid,NiCd)

Parameters: [value]

Example 1:

```
apc> cfgBatType
Battery Chemistry
  Battery Chemistry: LeadAcid
E000: Success
```

Example 2:

```
apc> cfgBatType NiCd
Battery Chemistry
  Battery Chemistry: NiCd
E000: Success
```

Error Messages: E000, E102

cfgBatsStr

Description: Display or Change Batteries Per String

Parameters: [value]

Example 1:

```
apc> cfgBatsStr
Batteries Per String
  Batteries Per String: 244
E000: Success
```

Example 2:

```
apc> cfgBatsStr 244
Batteries Per String
  Batteries Per String: 244
E000: Success
```

Error Messages: E000, E102

cfgCelSuspV

Description: Display or Change Cell Voltage Suspend Limit

Parameters: [value]

Example 1:

```
apc> cfgCelSuspV
Cell Voltage Suspend Limit
  Cell Voltage Suspend Limit: 1.700 V
E000: Success
```

Example 2:

```
apc> cfgCelSuspV 1.7
Cell Voltage Suspend Limit
  Cell Voltage Suspend Limit: 1.700 V
E000: Success
```

Error Messages: `E000, E102`

cfgCellMaxV

Description: Display or Change Cell Voltage Upper Limit

Parameters: [value]

Example 1:

```
apc> cfgCellMaxV
Cell Voltage Upper Limit
  Cell Voltage Upper Limit: 2.400 V
E000: Success
```

Error Messages: `E000, E102`

cfgCellMinV

Description: Display or Change Cell Voltage Lower Limit

Parameters: [value]

Example 1:

```
apc> cfgCellMinV
Cell Voltage Lower Limit
  Cell Voltage Lower Limit: 2.150 V
E000: Success
```

Example 2:

```
apc> cfgCellMinV 2.15
Cell Voltage Lower Limit
  Cell Voltage Lower Limit: 2.150 V
E000: Success
```

Error Messages: `E000, E102`

cfgCellsBat

Description: Display or Change Cells Per Battery (1,2,4,6)

Parameters: [value]

Example 1:

```
apc> cfgCellsBat
Cells Per Battery
  Cells Per Battery: 1
E000: Success
```

Example 2:

```
apc> cfgCellsBat 6 1
Cells Per Battery
  Cells Per Battery: 1
E000: Success
```

Error Messages: E000, E102

cfgCharMax

Description: Display or Change Charge (Response) Upper Limit

Parameters: [value]

Example 1:

```
apc> cfgCharMax
Charge (Response) Upper Limit
  Charge (Response) Upper Limit: 30 %
E000: Success
```

Example 2:

```
apc> cfgCharMax 30
Charge (Response) Upper Limit
  Charge (Response) Upper Limit: 30 %
E000: Success
```

Error Messages: E000, E102

cfgCurMaxR

Description: Display or Change Ripple Current Upper Limit

Parameters: [value]

Example 1:

```
apc> cfgCurMaxR
Ripple Current Upper Limit
  Ripple Current Upper Limit: 5 %
E000: Success
```

Example 2:

```
apc> cfgCurMaxR 5
Ripple Current Upper Limit
  Ripple Current Upper Limit: 5 %
E000: Success
```

Error Messages: E000, E102

cfgMaxDis

Description: Display or Change Discharge (Capacity) Limit

Parameters: [value]

Example 1:

```
apc> cfgMaxDis
Discharge (Capacity) Limit
  Discharge (Capacity) Limit: 15 %
E000: Success
```

Example 2:

```
apc> cfgMaxDis 15
Discharge (Capacity) Limit
  Discharge (Capacity) Limit: 15 %
E000: Success
```

Error Messages: E000, E102

cfgNumBsts

Description: Display or Change Number of boosts

Parameters: [value]

Example 1:

```
apc> cfgNumBsts
Number of boosts
  Number of boosts: 1
E000: Success
```

Example 2:

```
apc> cfgNumBsts ? 1
Number of boosts
  Number of boosts: 1
E000: Success
```

Error Messages: E000, E102

cfgNumStr

Description: Display or Change Number Of Strings

Parameters: [value]

Example 1:

```
apc> cfgNumStr
Number Of Strings
  Number Of Strings: 2
E000: Success
```

Example 2:

```
apc> cfgNumStr 2
Number Of Strings
  Number Of Strings: 2
E000: Success
```

Error Messages: E000, E102

cfgOhmTsTm

Description: Display or Change Ohmic Test Time

Parameters: [value]

Example 1:

```
apc> cfgOhmTsTm
Ohmic Test Time
  Ohmic Test Time: 60 sec
E000: Success
```

Example 2:

```
apc> cfgOhmTsTm 60
Ohmic Test Time
  Ohmic Test Time: 60 sec
E000: Success
```

Error Messages: E000, E102

cfgTmpMaxA

Description: Display or Change Ambient Temperature Upper Limit

Parameters: [value]

Example 1:

```
apc> cfgTmpMaxA
Ambient Temperature Upper Limit
  Ambient Temperature Upper Limit: 35.0 C
E000: Success
```

Example 2:

```
apc> cfgTmpMaxA 35
Ambient Temperature Upper Limit
  Ambient Temperature Upper Limit: 35.0 C
E000: Success
```

Error Messages: E000, E102

cfgTmpMaxP

Description: Display or Change Pilot Temperature Upper Limit

Parameters: [value]

Example 1:

```
apc> cfgTmpMaxP
Pilot Temperature Upper Limit
  Pilot Temperature Upper Limit: 35.0 C
E000: Success
```

Example 2:

```
apc> cfgTmpMaxP 35
Pilot Temperature Upper Limit
  Pilot Temperature Upper Limit: 35.0 C
E000: Success
```

Error Messages: E000, E102

cfgTmpMinA

Description: Display or Change Ambient Temperature Lower Limit

Parameters: [value]

Example 1:

```
apc> cfgTmpMinA
Ambient Temperature Lower Limit
  Ambient Temperature Lower Limit: 10.0 C
E000: Success
```

Error Messages: E000, E102

cfgWireLen

Description: Display or Change Monitor wire length (Short, Long)

Parameters: [value]

Example 1:

```
apc> cfgWireLen
Monitor wire length
  Monitor wire length: Long
E000: Success
```

Example 2:

```
apc> cfgWireLen Short
Monitor wire length
  Monitor wire length: Short
E000: Success
```

Error Messages: E000, E102

inpDlyTime

Description: Display or Change Input # Contact Delay Time

Parameters: [input# [value]]

Example 1:

```
apc> inpDlyTime
Input # Contact Delay Time
  Input 1 Contact Delay Time: 0 sec
  Input 2 Contact Delay Time: 0 sec
E000: Success
```

Example 2:

```
apc> inpDlyTime 2
Input # Contact Delay Time
  Input 2 Contact Delay Time: 0 sec
E000: Success
```

Example 3:

```
apc> inpDlyTime 2 1
Input # Contact Delay Time
  Input 2 Contact Delay Time: 1 sec
E000: Success
```

Error Messages: E000, E102

inpName

Description: Display or Change Input # Contact Name

Parameters: [input# [value]]

Example 1:

```
apc> inpName
Input # Contact Name
  Input 1 Contact Name: Contact 0
  Input 2 Contact Name: Contact 1
E000: Success
```

Example 2:

```
apc> inpName 2
Input # Contact Name
  Input 2 Contact Name: Contact 0
E000: Success
```

Example 3:

```
apc> inpName 2 2
Input # Contact Name
  Input 2 Contact Name: Contact 2
E000: Success
```

Error Messages: E000, E102

inpNrmState

Description: Display or Change Input # Contact Normal State (Open, Closed)

Parameters: [input# [value]]

Example 1:

```
apc> inpNrmState
Input # Contact Normal State
  Input 1 Contact Normal State: Open
  Input 2 Contact Normal State: Open
E000: Success
```

Example 2:

```
apc> inpNrmState 1
Input # Contact Normal State
  Input 1 Contact Normal State: Open
E000: Success
```

Error Messages: E000, E102

inpState

Description: Display Input # Contact State (Open, Closed)

Parameters: [input#]

Example 1:

```
apc> inpState
Input # Contact State
  Input 1 Contact State: Open
  Input 2 Contact State: Open
E000: Success
```

Example 2:

```
apc> inpState 1
Input # Contact State
  Input 1 Contact State: Open
E000: Success
```

Error Messages: E000, E102

pilotTemp

Description: Display Pilot Temperature

Parameters: None

Example 1:

```
apc> pilotTemp
Pilot Temperature
  Pilot Temperature: 22.2 C
E000: Success
```

Error Messages: E000, E102

resetAnn

Description: Remote UI Annunciator Reset

Parameters: None

Example:

```
apc> resetAnn
Remote UI Annunciator Reset
E000: Success
```

Error Messages: E000, E102

resetBench

Description: Reset Charge Current Deviation Benchmark

Parameters: None

Example:

```
apc> resetBench
Reset Charge Current Deviation Benchmarks
E000: Success
```

Error Messages: E000, E102

resetDisV

Description: Reset Lowest Discharge Voltages

Parameters: None

Example:

```
apc> resetDisV
Reset Lowest Discharge Voltages
E000: Success
```

Error Messages: E000, E102

strCurrent

Description: Display String # Current

Parameters: [string#]

Example 1:

```
apc> strCurrent
String # Current
  String 1 Current: 0.0 Adc
  String 2 Current: 0.0 Adc
E000: Success
```

Example 2:

```
apc> strCurrent 1
String # Current
  String 1 Current: 0.0 Adc
E000: Success
```

Error Messages: E000, E102

strDisCtr

Description: Display String # Discharge counter for time period #

Parameters: [string# [period#]]

Example 1:

```
apc> strDisCtr
String # Discharge counter for time period #
  String 1 Discharge counter for time period Less than 5 seconds: 0
  String 1 Discharge counter for time period 5 to 10 seconds: 0
  ...
  String 2 Discharge counter for time period 10 seconds to 1 minute: 1
  String 2 Discharge counter for time period More than 1 minute: 1
E000: Success
```

Example 2:

```
apc> strDisCtr 1
String # Discharge counter for time period #
  String 1 Discharge counter for time period Less than 5 seconds: 0
  String 1 Discharge counter for time period 5 to 10 seconds: 0
  String 1 Discharge counter for time period 10 seconds to 1 minute: 1
  String 1 Discharge counter for time period More than 1 minute: 1
E000: Success
```

Example 3:

```
apc> strDisCtr 1 1
String # Discharge counter for time period #
  String 1 Discharge counter for time period Less than 5 seconds: 0
E000: Success
```

Example 4:

```
apc> strDisCtr 1 1 2
String # Discharge counter for time period #
  String 1 Discharge counter for time period 5 to 10 seconds: 0
E000: Success
```

Error Messages: E000, E102

strRipple

Description: Display String # Ripple Current

Parameters: [string#]

Example 1:

```
apc> strRipple
String # Ripple Current
  String 1 Ripple Current: 0.0 Aac
  String 2 Ripple Current: 0.0 Aac
E000: Success
```

Example 2:

```
apc> strRipple 1
String # Ripple Current
  String 1 Ripple Current: 0.0 Aac
E000: Success
```

Error Messages: E000, E102

strVoltage

Description: Display String # Voltage

Parameters: [string#]

Example 1:

```
apc> strVoltage
String # Voltage
  String 1 Voltage: 536.8 Vdc
  String 2 Voltage: 536.8 Vdc
E000: Success
```

Example 2:

```
apc> strVoltage 1
String # Voltage
  String 1 Voltage: 536.8 Vdc
E000: Success
```

Error Messages: E000, E102

unitFWVer

Description: Display Unit # Firmware Version

Parameters: [unit#]

Example 1:

```
apc> unitFWVer
Unit # Firmware Version
  Unit 1 Firmware Version: 100
  Unit 2 Firmware Version: 100
  ...
  Unit 7 Firmware Version: 100
  Unit 8 Firmware Version: 100
E000: Success
```

Example 2:

```
apc> unitFWVer 1
Unit # Firmware Version
  Unit 1 Firmware Version: 100
E000: Success
```

Error Messages: E000, E102

unitHWVer

Description: Display Unit # Hardware Version

Parameters:[unit#]

Example 1:

```
apc> unitHWVer
Unit # Hardware Version
  Unit 1 Hardware Version: 1
  Unit 2 Hardware Version: 1
  ...
  Unit 7 Hardware Version: 1
  Unit 8 Hardware Version: 1
E000: Success
```

Example 2:

```
apc> unitHWVer 1
Unit # Hardware Version
  Unit 1 Hardware Version: 1
E000: Success
```

Error Messages: E000, E102

unitSerNum

Description: Display Unit # Serial Number

Parameters: [unit#]

Example 1:

```
apc> unitSerNum
Unit # Serial Number
  Unit 1 Serial Number: SJ04370123450
  Unit 2 Serial Number: SJ04370123451
  ...
  Unit 7 Serial Number: SJ04370123456
  Unit 8 Serial Number: SJ04370123457
E000: Success
```

Example 2:

```
apc> unitSerNum 1
Unit # Serial Number
  Unit 1 Serial Number: SJ04370123450
E000: Success
```

Error Messages: E000, E102

Web Access

Overview

The web user interface (UI) provides options to view the status of, and to manage the Battery Manager.

Supported Web Browsers

Modern web browsers will be compatible with the Battery Manager web interface. Using a current software release for your browser is encouraged to mitigate the risk of software security vulnerabilities.

Getting Started

To access the Battery Manager through a web browser, first the user must disable any *proxy server* services in use. Access to the Battery Manager through a *proxy server* is not available at this time; if use of a proxy is required, it must be configured so that the IP address of the Battery Manager is not proxied.

Type the IP address of the Battery Manager in the web browser's address field.

For a System IP address of 139.225.6.133, when the Battery Manager uses the default port (80) at the Web server, the entry would be one of the following:

  – `http://139.225.6.133` if HTTP is your access mode

  – `https://139.225.6.133` if HTTPS is your access mode

- For a System IP address of 139.225.6.133, when the Battery Manager uses a non-default port (5000, in this example) at the Web server, the entry would be one of the following:

  – `http://139.225.6.133:5000` if HTTP is your access mode

  – `https://139.225.6.133:5000` if HTTPS is your access mode

- If your DNS system has been configured with entries for the Battery Manager, Web1 in this case, the entry would be one of the following:

  – `http://Web1` if HTTP is your access mode

  – `https://Web1` if HTTPS is your access mode

The Web Interface

When logging into the Web Interface of the Battery Manager, a menu bar is displayed at the top of the screen. Below the navigation tabs, popup menus list options related to the selected section. The status field displays information about the system.

Limited Status Access

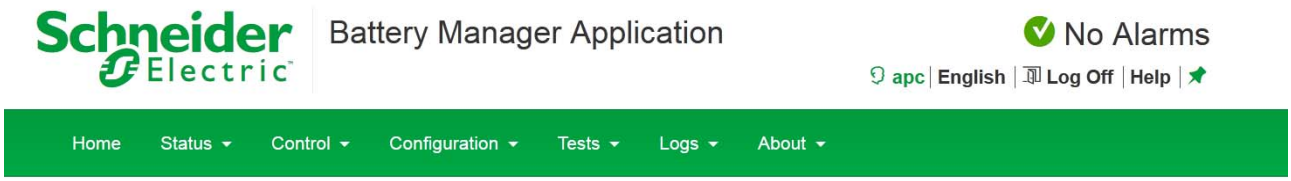
The *App Limited Status* (**Configuration > Network > Web > Access**) page provides limited information, without requiring a login. Using a web browser, access the Battery Manager's IP address, to view the log in page. There is a "Limited Status" hyperlink, towards the lower left corner of the frame.

Clicking on "Limited Status," instead of the regular user name / password fields, a limited summary of Device and System Information is made available to viewing. A "Log On" hyper link, as seen immediately above, allows for easy access to the standard *Log In* page.

Web Interface Introduction

Home

This is the default tab when you log on. To change the login page to a different page, click on the green pushpin at the top right side of the browser window while on the desired page.



❶ Quick Status Links

The *Quick Status* area, displayed in the upper right corner of every screen, displays a warning of any alarms. Clicking on any of the *Quick Status* icons will take you to the home screen.

Green “device operating normally” check mark icon

“Attention required” cautionary yellow icon

Red “alarm detected” icon

❷ Current Session Preferences

More useful information and links can be found immediately beneath the *Quick Status* row. User-Level Management settings and preferences can be accessed by clicking on the first link, “apc” as seen above. See “Security” on page 72 for more Local User settings.

Help

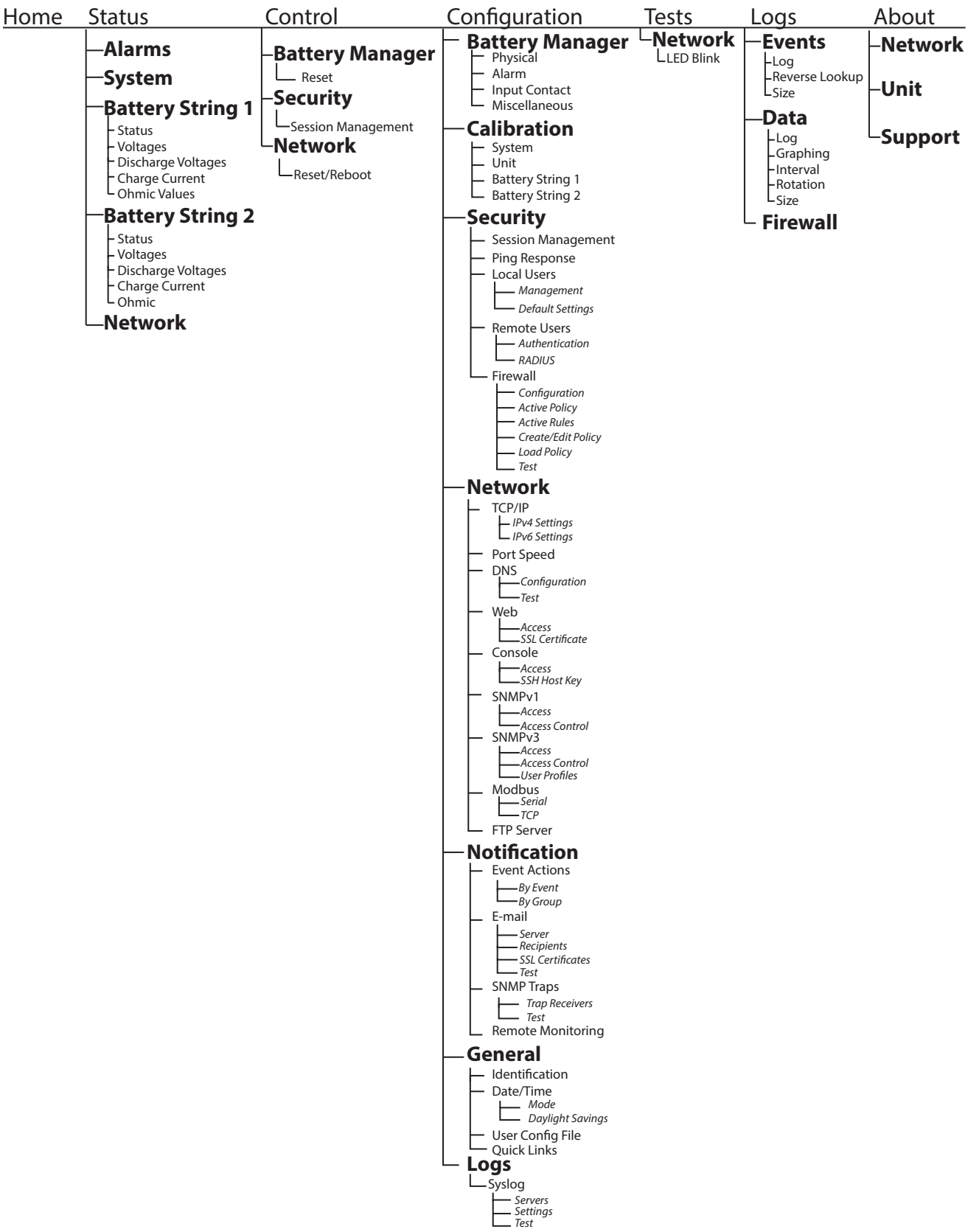
Click **Help**, located in the upper right hand corner of the Web Interface to view context-sensitive information.

Quick Links

At the lower left of each page, there are three user configurable links. By default, the links access the following web pages:

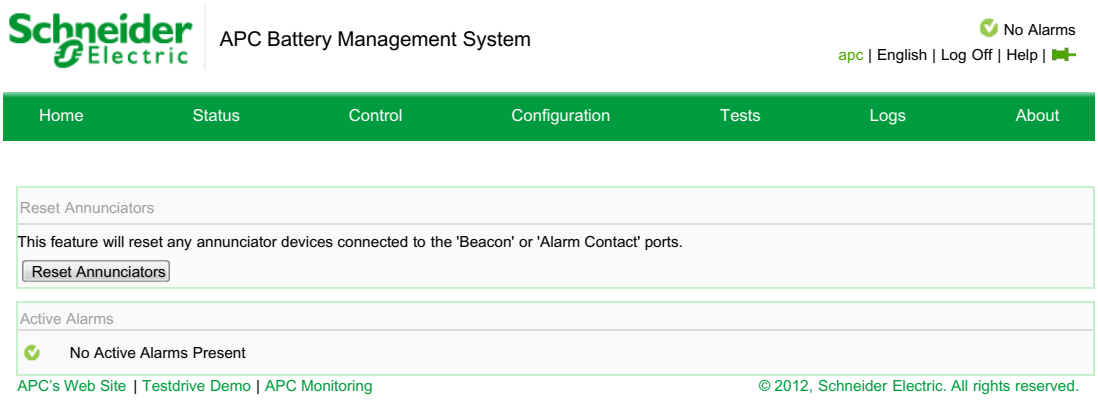
- **Link 1:** Website homepage
- **Link 2:** Demonstrations of Schneider Electric web-enabled products
- **Link 3:** Information on Schneider Electric Remote Monitoring Services

Display Menu Tree



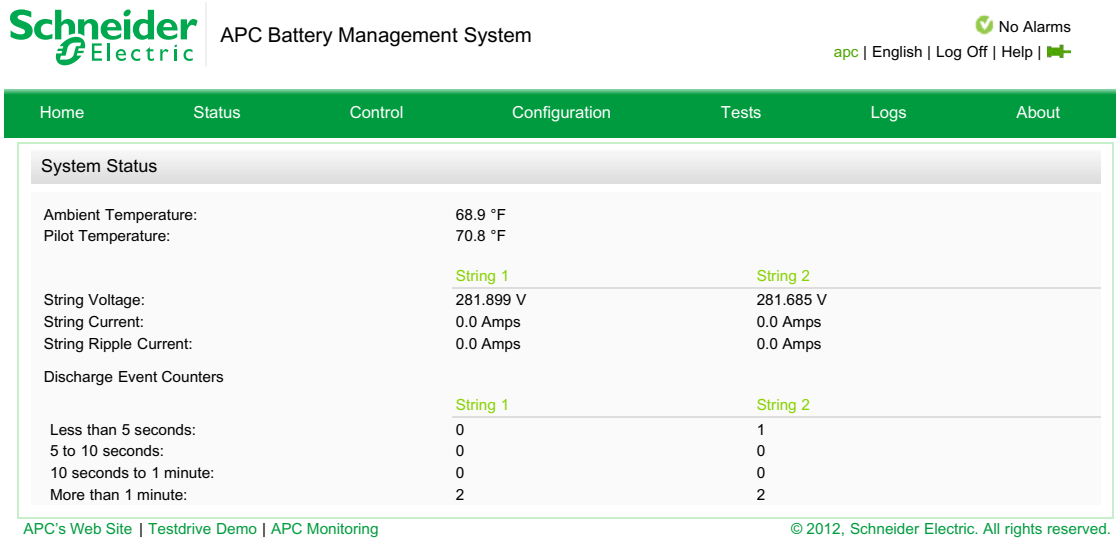
Status

Alarms



This page shows any *Active Alarms* for the system. This page also allows for the user to *Reset Annunciators*.

System



- Ambient Temperature - The air temperature in the battery environment.
- Pilot Temperature - The surface temperature of the battery to which the pilot temperature sensor is attached.
- String Voltage - The voltage (VDC) of an entire battery string
- String Current - The rate of charge/discharge for a battery string, in amps
- String Ripple Current - The amount of AC current detected in a battery string, in amps
- Discharge Event Counters -
  - Each discharge counter records the number of discharge events that have lasted for the specified length of time: Less than 5 seconds, 5 to 10 seconds, 10 seconds to 1 minute, or More than 1 minute.

NOTE: For a Battery Manager configured to manage two strings of batteries, all status information except ambient and pilot temperatures is displayed in columns labeled ‘String 1’ and ‘String 2.’

Status Battery String 1

Status > Battery

- **Status** - *Voltage*, *Lowest Discharge Voltage*, *Charge Current Deviation*, and *Ohmic Value* of each battery can be found at this page. To view an individual battery's status or to configure its ohmic value correction, click the battery number.
  - **Sorting Battery Data:** By default, the batteries are sorted by status. A small arrow in the column heading indicates the column by which information is being sorted, and whether the data is in ascending or descending order. To sort by another column, or to change the sort order, click the column heading.
  - **Filtering Battery Data:** A filter causes an alarms, that meeting a defined criteria, is displayed on the interface. Click **Create Filter**. Enter the information to filter, and click **Apply**. To modify the filter, click the filter icon in the column heading of the information being filtered, or click **Create Filter** again. To remove the filter, click **Clear Filter**. The filter settings are valid for one user session only.
- **Voltages:** Lists the individual voltages for every battery in the attached string, and presents this information in a bar graph. The last-measured voltages are listed in ascending order.

Color	Description
Green	Battery voltage is normal.
Yellow	Warning alarm. The voltage of this battery is violating the user-defined minimum or maximum voltage threshold. (See **Cell Max Voltage Limit** and **Cell Min Voltage Limit** to configure the voltage thresholds.)
Red	Critical alarm. The voltage of this battery is violating the minimum or maximum voltage threshold defined by the chemistry of the battery.

- **Discharge Voltages:** The discharge voltages are recorded during the most recent discharge. Select this option to view a bar graph of the discharge voltage of each battery connected to the system. The batteries and their last-measured discharge voltages are listed in ascending order. See “Discharge Voltage Alarm Level” on page 68 to configure the discharge voltage alarm.
- **Charge Current:** The Charge Current is the percentage of change in the charge current test from the stored Benchmark values (Deviation from Benchmark).
  - The batteries and their last-measured charge current test deviation percentages are listed in ascending order. Each battery is tested with a charge current and the individual values of current are stored as benchmarks.
  - Subsequent tests of each battery result in a difference between the benchmark value and the most recent test. See “Charge Current Deviation From Benchmark” on page 68 to configure the acceptable deviation percentage.
- **Ohmic Values:** Changes in **Ohmic Values** indicate the gradual deterioration of batteries.
  - Calculated during the last discharge event, all batteries in a system and their last-measured ohmic values are listed in ascending order in a bar graph.

Status Battery String 2

If available, *Battery String 2* contains the same variables which can be monitored as in Battery String 1.

Network

Configuration > Network

An overview of critical network status information is available here. All configurable network settings can be modified here.

Control

Battery Manager - Reset Actions

Control > Battery Manager > Reset

Parameters	Description
Reset Annunciators	Reset any devices connected to the ‘Beacon’ or ‘Alarm Contact’ ports.
Reset Lowest Discharge Voltages	Reset the lowest voltages recorded during the last discharge. This parameter is updated during the next discharge test. This may be desirable if the user knows the readings were faulty for some reason.
Reset Charge Current Deviation Benchmark	Reset the benchmark value used to calculate charge current deviation alarms. This parameter is updated during the next charge test. This may be desirable if the user knows the value was faulty for some reason and would like another benchmark to be calculated.
Reset Discharge Event Counters	Reset all discharge event counters. This will allow the user to reset all discharge event counters.

NOTE: Any time system batteries are removed, added, or reconfigured, it is suggested that applicable parameters are reset, using the methods described above.

Session Management

Control > Security > Session Management

This section lists all of the currently logged in users, the interface from which they are logged in, their IP address, and the amount of time they have been logged in. A specific user session can be terminated (with the appropriate authority) by selecting the user name.

Network Reset/Reboot

Control > Network > Reset/Reboot

Action	Definition
Reboot Management Interface	Restarts the management interface of the device without turning off and restarting the device itself.
Reset All	• If you do not select “Exclude TCP/IP,” all configured values and settings are reset to their default values, including the setting that determines how this device must obtain its TCP/IP configuration values. The default for that setting is DHCP. • If you select “Exclude TCP/IP,” all configured values and settings except the setting that determines how this device must obtain its TCP/IP configuration values are reset to their default values.
Reset Only	You can select one or more of the following options: TCP/IP: Resets only the setting that determines how this device must obtain its TCP/IP configuration values. The default for that setting is DHCP. Event Configuration: Resets events to their default configuration. Any specially configured event or group will also revert to the default value.

Configuration

Physical Configuration

Configuration > Battery Manager > Physical

Identify the type of batteries (Lead-Acid or Nickel-Cadmium) connected to the Battery Manager. Changing the battery type resets the battery configuration parameters to their default settings and deletes the benchmark values, data about the individual batteries, and the data log.

Physical Parameters - Number of Strings, Number of Batteries per string, Number of Cells per battery, Rated Battery Capacity, Monitor Wire Length.

NOTE: The total string voltage of the batteries connected to the system must not exceed 560 VDC per string.

Parameters	Description
Number of Strings	The number of battery strings in the system, 1 or 2
Number of Batteries per String	The number of batteries in each string in the system. This setting is limited by the maximum voltage of the system (560 VDC) and by the maximum number of batteries per string. • Systems with one or two strings of lead-acid batteries—244 batteries • Systems with one string of nickel-cadmium batteries—375 batteries • Systems with two strings of nickel-cadmium batteries—256 batteries per string
Number of Cells per Battery	The number of cells per battery: • 1, 2, 4, or 6 for lead-acid batteries • 1 or 2 for nickel-cadmium batteries
Rated Battery Capacity	Enter the battery capacity in amp-hours for reference. The amp-hour capacity of a battery is generally clearly marked on the actual battery or on the battery specification sheet. Valid values are 5–4000 amp-hours (AH).
Monitor Wire Length	The length of wire between the Battery Manager and the batteries it is monitoring. The boost voltage level is adjusted based on the length of the wire. Valid values are **50 feet or less** and **Greater than 50 feet**.

Alarm Configuration

Configuration > Battery Manager > Alarm

AC Ripple Current Limit	The maximum allowable AC Current measurement in the battery string.
Cell Max Voltage Limit	The maximum recommended voltage per individual battery cell. Set the **Cell Max Voltage Limit** to the highest float charge voltage of the battery as specified by the manufacturer. This number is multiplied by the total number of cells in a string to define the **High String Voltage Alarm** threshold. A charger alarm occurs if the string voltage exceeds this alarm value.
Cell Min Voltage Limit	The minimum recommended voltage per individual battery cell. Set the **Cell Min Voltage Limit** to the fully-charged open-circuit voltage of the installed battery. This number, multiplied by the total number of cells in a string, defines the **Low String Voltage Alarm** threshold. A charger alarm occurs if the string voltage falls below this alarm value.
Suspend Cell Voltage (lead-acid battery systems only)	A voltage used to determine whether a battery string has violated the low-voltage limit. The calculation also includes the number of cells per battery and number of batteries per string. If the system has violated the low voltage limit, the Battery Manager will enter suspend mode, limiting the current drawn by the Battery Manager.
Max Pilot Temperature Limit	The maximum surface temperature of the pilot battery (the battery to which the pilot temperature sensor is attached). Because current flow is constant throughout a series of batteries, the pilot battery temperature is likely to be typical of other batteries in the system. For example, an overheated pilot battery would probably indicate overcharging throughout the system.
Max Ambient Temperature Limit	The maximum allowable temperature of the air surrounding the batteries. ***See the specifications for your batteries before changing this value.***
Min Ambient Temperature Limit	The minimum allowable temperature of the air surrounding the batteries. ***See the specifications for your batteries before changing this value.***
Charge Current Deviation From Benchmark	The percentage of change in the response-current measurement that is allowed, when the batteries are being charged, before an alarm occurs.
Discharge Voltage Alarm Level	The maximum allowable variation between the highest-voltage battery and the lowest-voltage battery in the string during a discharge. If the threshold is violated when the batteries are being discharged (e.g., during a power failure), a Battery Low Capacity alarm occurs.
Automatic Annunciator Reset Enabled	An external annunciator device can be a beacon or other device connected to the alarm contact port. • Enabled— Devices reset automatically when the condition that caused an alarm clears. • Disabled—Devices must be manually reset.

Input Contact Configuration

Configuration > Battery Manager > Input Contacts

View the state of the two input contacts connected to the system. Configure the name, normal state (**Open** or **Closed**), and the amount of time (in seconds) the input contact state must be abnormal before the system generates an alarm.

NOTE: For pinout information, or to connect during installation, see the Battery Manager *Installation Manual*.

Battery Manager Miscellaneous

Configuration > Battery Manager > Miscellaneous

Home Page Auto Refresh Rate	The Home page has been designed so that it can provide continuously updated data without a user needing to refresh the page. Automatic refresh of the page is disabled by default. The user can enable an auto home page refresh rate of 1 - 10 minutes.
Ohmic Test Wait Time	The amount of time (in seconds) the system waits after a discharge event begins before collecting data for the ohmic value calculation.
Number of Boosts*	The number of times the system sends a charge through a battery before moving to the next battery. This setting is available only for systems with an amp-hour (AH) rating greater than 120 AH.
* If the *Rated Battery Capacity* **(Configuration > Battery Manager > Physical)** does not surpass the minimum required value, this input is not made available to users, and the Battery Manager defaults to small battery management mode.	

System Calibration

Configuration > Calibration > System

NOTE: Schneider Electric strongly recommends that you calibrate your Battery Manager during system start up and upon battery replacement in order to ensure accurate readings and measurements and to avoid false alarms.

Ohmic Value Correction Factor	Various instruments and techniques yield different ohmic value results, as ohmic measurement instruments are not standardized. Ohmic value results vary depending on the calibrated instrument used. Use this setting to adjust the ohmic values reported by the system to correspond to the values reported by your instrument. This percent correction factor affects every individual ohmic value in a string. For example, if all of the batteries in the system report ohmic values that are 5% higher than the ohmic values the calibrated instrument reports, specify –5% in this field. All of the ohmic values reported by the Battery Manager will then be reduced by 5% to correspond to the values reported by the calibrated instrument.
Sensor Range	Sensor Range is a pull down selection of the ampere current sensor that is connected to the system. The default value of the current sensor connected to the system is a 1000 ampere sensor.
DC Zero	‘DC Zero' is entered in + or - millivolts to either add or subtract from the DC current value shown when no current is flowing through the sensor opening (as when it is not installed on a cable but plugged in to the system). Set the value for the DC current to zero by adding to or subtracting from the value for the DC current that is recorded when current is not flowing through the current sensor. For example, if the system records +2.4 amps of current with no current flow, enter –2.4 in the **DC Zero** field.
AC Ripple Zero	'AC Ripple Zero' is entered in + or - millivolts to either add to or subtract from the AC current value shown when no current is flowing through the sensor opening (as when it is not installed on a cable but plugged in to the system). Set the value for the AC ripple current to zero by adding to or subtracting from the **AC Ripple Zero** value that is recorded when current is not flowing through the current sensor. For example, if the system records +1.2 amps of current with no current flow, enter –1.2 in the **AC Ripple Zero** field.

Unit Battery Voltage Calibration

Configuration > Calibration > Unit

- **Battery Voltage Zero -** The zero factor is entered in + or - millivolts to either add to or subtract from the value shown for an open circuit individual battery input (no voltage).
- **Battery Voltage Span -** The span is in percent and corrects for the upscale voltage value (with voltage input) as compared with a known voltage standard. Calibrate the voltage indication by applying a correction factor to ensure that the system is indicating and recording accurate voltages.
    - The following formula calculates this percentage:

      ```
      Actual Voltage / Indicated Voltage = Correction Factor
      ```

    Example: A calibrated voltage meter indicates a string voltage of 434 VDC. The system indicates a voltage of 425 VDC. To calculate the correction factor, divide the voltage meter reading by the voltage the system indicates.

    434 / 425 = 1.0212

    Convert the result to a percentage (102.12%). This is the value that will be entered into the Span data entry box.

    NOTE: If the voltages are inverted (the voltage indicated by the system is higher than the voltage detected by the voltage meter) the result of the formula is a percentage of less than 100%.

Calibrating Individual Batteries

Configuration > Calibration > Battery String 1

Select **Battery String 1** (or 2 if applicable), from **Configuration > Calibration** pop up menu to view and calibrate the ohmic value corrections. The system uses the ohmic correction values to compensate for voltage drops in the cables and connections associated with each battery connected to the system.

To calculate the ohmic value correction, measure the ohmic value of the battery, then subtract the measured ohmic value from the indicated ohmic value for the circuit. Enter the difference between the ohmic values as a negative number (in milliohms), as an offset. Apply the setting to all batteries, or enter the number of a battery to which the setting will be applied.

Security

Session Management

Configuration > Security > Session Management

This option allows for various *Session Details* to be configured. Specifically, *Allow Concurrent Logins*, as well as *Remote Authentication Override* options are either enabled or disabled here. Under the Control section, see “Session Management” on page 66 for more information.

Ping Response

Configuration > Security > Ping Response

For a many reasons, it may be required to ping the Battery Manager. At this configuration screen, allowing the Battery Manager to respond to a Ping can be either enabled or disabled. If enabled, and the Battery Manager does not respond to Ping, see “Unable to Ping the Battery Manager” on page 115.

Local User Management

Configuration > Security > Local Users > Management

This page allows for the creation and management of both *Super User* and *General User* profiles on the Battery Manager. The initial view is a list of the current user profiles, separated by type. Navigate to the *User Configuration* web-page template, by clicking *Add User*, or on any *User Name*.

Any changes will take place after log off. More regarding information regarding *User Account types* can be found in “User Account Overview” on page 4“.

User Configuration

- *Access:* Determines whether or not the user account has access to log into the system.
- *User Name:* Displays the current User account name. Set the case-sensitive user name (64 byte maximum, supports up to 64 ASCII characters; Less for multi-byte languages).

  NOTE: This field cannot be changed for the Super User. This field can only be set when creating the user. To change the user name after the account has been created, the user would need to be deleted and recreated with the proper value.
- *Current Password:* To make changes to the Super User account, enter the existing password.
- *New Password:* Set the case-sensitive password (64 byte maximum supports up to 64 ASCII characters; Less for multi-byte languages). Passwords with no characters (blank passwords) are not allowed.
- *User Description:* Field used for additional notes to describe this particular user.
- *Session Timeout:* Amount of time (in minutes) the user has before they are logged out due to inactivity (3 minutes by default).
- *Serial Remote Authentication Override:* Determines whether or not this account can login serially even when the NMC authentication is set to RADIUS.

User Preferences (and Default Settings)

There are two main features for the default user settings:

1. Determine the default values to populate in each of the fields when the Super User or Administrator account creates a new user. These values can be changed before the settings are applied to the system.
2. For remote users (user accounts not stored in the system that are remotely authenticated such as RADIUS) these are the values used for those that are not provided by the authenticating server. For example, if a RADIUS server does not provide the user with a temperature preference, the value defined in this section will be used.

- *Bad Login Attempts:* Number of incorrect login attempts a user has before the system disables account. Upon reaching this limit, a message is displayed informing the user the account has been locked. The Super User or an Administrator-level account is needed to re-enable the account to allow the user to log back in.

  NOTE: A Super User account cannot be locked out, but can be manually disabled if necessary.
- *Event Log Color Coding:* Configure whether text in the event log is color-coded based on event severity.
- *Export Log Format:* Configure which format the event log should be displayed in when exported (downloaded). Tab (default) allows fields to be tab-delimited whereas CSV is comma-separated.
- *Temperature Scale:* This page allows for a temperature scale preference to be specified for a particular user. The default temperature scale is Metric (°C), and the US scale (°F) is available. This value can be changed at a later time.
- *Date Format:* Select the user interface date format from the drop-down box.
- *Language:* Select the user interface display languages from the drop-down box.
- *Strong Passwords:* Configure whether new passwords created for user accounts will require additional rules such as at least one lowercase character, one uppercase character, one number, and one symbol.
- *Password Policy:* Select the duration (in days) to which the user will be required to change their password. A value of 0 days disables this feature (by default).

Authentication & Remote Users

Configuration > Security > Remote Users > Authentication

Use this option to select how to administer remote access to the Battery Manager. For information about local authentication (not using the centralized authentication of a RADIUS server), see the *Security Handbook,* available on the *Utility* CD and at **www.apc.com**.

Schneider Electric supports the authentication and authorization functions of RADIUS (Remote Access Dial-In User Service).

- When a user accesses the Battery Manager that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user's permission level.
- RADIUS user names used with the Battery Manager are case-sensitive, and have a 64 byte maximum, supporting up to 64 ASCII characters; less for multi-byte languages. Passwords with no characters (blank passwords) are not allowed.

Select one of the following:

- **Local Authentication Only**: RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Authentication**: RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used.
- **RADIUS Only**: RADIUS is enabled. Local authentication is disabled. If **RADIUS Only** is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, you must use a serial connection to the *Command Console* and change the **Access** setting to **Local Authentication Only** or **RADIUS, then Local Authentication** to regain access. "*Serial Remote Authentication Override*" under *Local User Settings*, and "*Remote Authentication Override*" under **Security > Session Management** should be enabled.

Configuring the RADIUS Server

Configuration > Security > Remote Users > RADIUS

RADIUS	You can set up the device to use a RADIUS server to authenticate remote users. Specify up to two properly configured RADIUS servers. To add a server, click Add Server. To modify an existing server, click the server's name.
RADIUS Server	The name or IP address of the RADIUS server.
Port	The port (1812 by default) that the RADIUS server listens on. **NOTE:** You can change the port setting to any unused port from 5000 to 32768.
Secret	The secret shared by the RADIUS server and the device.
Reply Timeout	The time in seconds that the device waits for a response from the RADIUS server.
Test Settings	Enter the user name and password of any account of the device to test the newly configured settings before applying them.
Skip Test and Apply	Applies the settings without verifying that they are configured correctly.

Summary of the configuration procedure

You must configure your RADIUS server to work with the Battery Manager. For examples of the RADIUS users file with Vendor Specific Attributes (VSAs) and an example of an entry in the dictionary file on the RADIUS server, see *Security Handbook*.

1. Add the IP address of the Battery Manager to the RADIUS server client list (file).
2. Users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined. If no Service-Type attributes are configured, users will have read-only access. See your RADIUS server documentation for information about the RADIUS users file.
3. VSAs can be used instead of Service-Type attributes provided by the RADIUS server. Using VSAs needs a dictionary entry and RADIUS users file. In the dictionary file, define the names for ATTRIBUTE and VALUE, but not the numeric values. If numeric values are changed, RADIUS authentication and authorization fails. VSAs take precedence over standard RADIUS attributes.

Configuring a RADIUS server on UNIX® with shadow passwords

If UNIX shadow password files are used (/etc/passwd) with the RADIUS dictionary files, the following two methods can be used to authenticate users:

- If all UNIX users have administrative privileges, add the following to the RADIUS “user” file. To allow only Device Users, change the Service-Type to `Device`.

```
DEFAULTAuth-Type = System
APC-Service-Type = Admin
```

- Add user names and attributes to the RADIUS “user” file, and verify password against /etc/passwd. The following example is for users `bconners` and `thawk`:

```
bconnersAuth-Type = System
APC-Service-Type = Admin
thawkAuth-Type = System
APC-Service-Type = Device
```

Supported RADIUS servers

FreeRADIUS and Microsoft IAS 2003 are supported. Other commonly available RADIUS applications may work but may not have been fully tested.

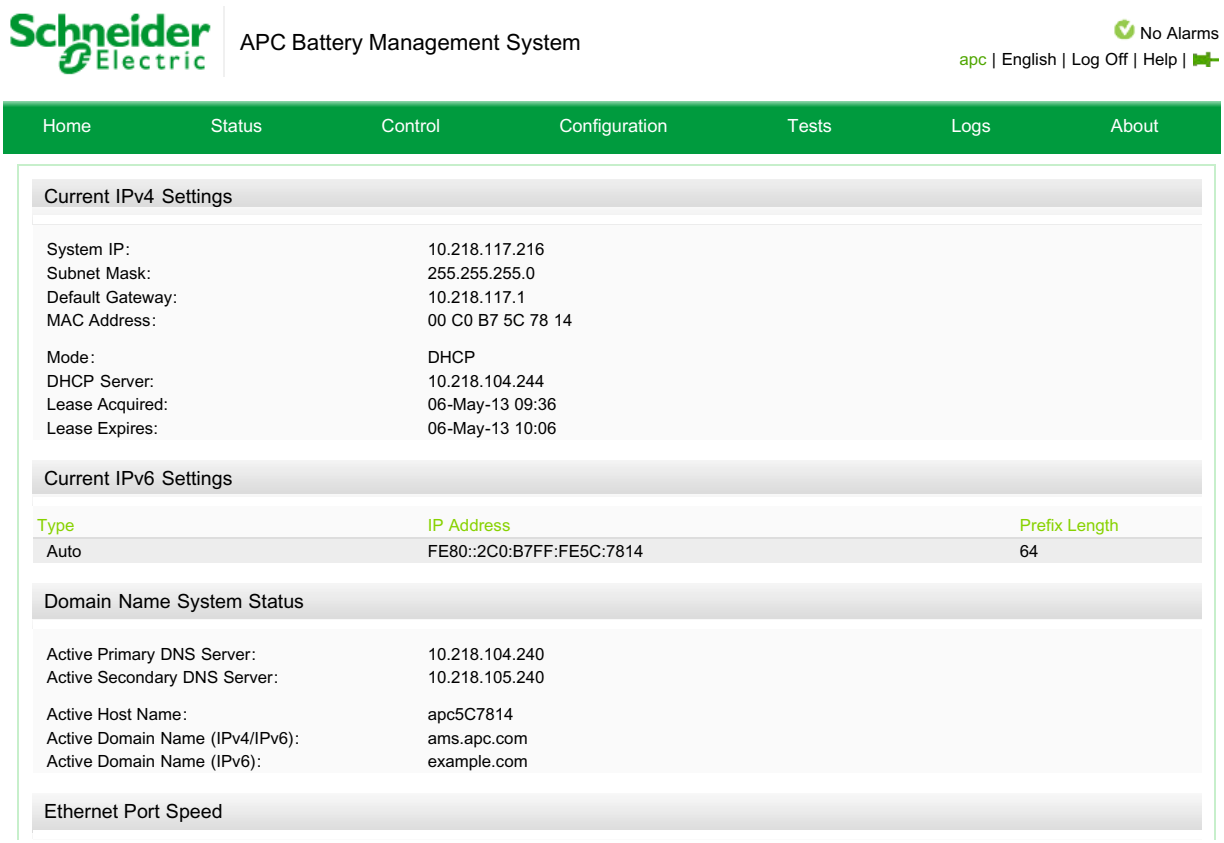
Firewall Configuration

Configuration > Security > Firewall

Configuration	Enable or disable the overall firewall functionality.
Active Policy	Select an active policy from the available firewall policies.
Active Rules	Lists the individual rules that are being enforced based on the current active policy.
Create/Edit Policy	Create a new policy or edit an existing one.
Active Policy	Load a policy file (.fwl suffix) from a source external to this device.
Test Policy	Temporarily enforce the rules of a chosen policy.

Network

Configuration > Network



- Current IPv4 Settings
    - System IP
    - Subnet Mask
    - Default Gateway
    - MAC Address
    - Mode - This field will display Manual or Automatic depending on what is selected within the IPv4 settings.
- Current IPv6 Settings - This field displays the IPv6 Settings Type, the IP Address, and the Prefix Length.
- Domain Name System Status - This field displays:
    - Active Primary DNS Server
    - Active Secondary DNS Server
    - Active Host Name
    - Active Domain Name (IPv4/IPv6)
    - Active Domain Name (IPv6)
- Ethernet Port Speed - Current Speed (i.e. 100 Full-Duplex)

TCP/IP

Configuration > Network > TCP/IP

IPv4 & IPv6

The default TCP/IP configuration setting, DHCP, assumes that a properly configured DHCP server is available to provide TCP/IP settings to the NMC.

You can also configure the setting for BOOTP. A user configuration (.ini) file can function as a BOOTP or DHCP boot file. For more information, see the TCP/IP configuration section of the Network Management Card User's Guide, available from www.apc.com.

On this page, current IPv4 settings can be viewed, and also configured. On this page, the user can enable or disable IPv4. The user can also opt to manually override the automatic settings for System IP, Subnet Mask, and Default Gateway.

BOOTP, DHCP

Setting	Description
Manual	The IPv4 settings (IP address, subnet mask, and default gateway) must be configured manually. Click **Next>>**, and enter the new values.
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Battery Manager requests network assignment from any BOOTP server: • If it receives a valid response, it starts the network services. • If it finds a BOOTP server, and receives a valid response, the device requests network assignment from any BOOTP server, and network services are initiated. • If a request to that server fails or times out, the Battery Manager stops requesting network settings until it is restarted. • By default, if no valid response is received with the new settings, and previously configured network settings exist, five attempts to connect will be made (the original and four retries), then the prior settings will be used.
DHCP	At 32-second intervals, the device requests network assignment from any DHCP server: • Optionally, the device requires the vendor specific cookie from the DHCP server in order to accept the lease and start the network services. • If it finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted.
NOTE: The default values for the other three settings on the DHCP Configuration page generally do not need to be changed: • Vendor Class: APC • Client ID: The MAC address of the device. If you change this value, the new value must be unique on the LAN. • User Class: The name of the application firmware module.	

DHCP Configuration Advanced

You can use a RFC2131/RFC2132-compliant DHCP server to configure the TCP/IP settings for the NMC.

1. The NMC sends out a DHCP request that uses the following to identify itself:
   – A Vendor Class Identifier (APC by default)
   – A Client Identifier (by default, the MAC address of the NMC)
   – A User Class Identifier (by default, the identification of the application firmware installed on the NMC)
2. A properly configured DHCP server responds with a DHCP offer that includes all the settings that the NMC needs for network communication. The DHCP offer also includes the Vendor Specific Information option (DHCP option 43). The NMC can be configured to ignore DHCP offers that do not encapsulate the APC cookie in DHCP option 43 using the following hexadecimal format. (The Card does not require this cookie by default).

   ```
   Option 43 = 01 04 31 41 50 43
      where:
   ```

   –the first byte (01) is the code

   –the second byte (04) is the length

   –the remaining bytes (31 41 50 43) are the APC cookie.

   For more detail about how a DHCP server can configure the network settings for a Network Management Card, see “DHCP Configuration” in the Network Management Card User’s Guide, available from www.apc.com.

Port Speed

Configuration > Network > Port Speed

- The Port Speed setting defines the communication speed of the TCP/IP port. For Auto-negotiation (the default), Ethernet devices negotiate to transmit at the highest possible speed, but if the supported speeds of two devices are unmatched, the slower speed is used.
- Alternatively, you can choose 10 Mbps or 100 Mbps, each with the option of half-duplex (communication in only one direction at a time) or full-duplex (communication in both directions on the same channel simultaneously).

DNS

General Configuration

Configuration > Network > DNS > Configuration

The Battery Manager and the NMC support the use of Domain Name System (DNS) Servers. Proper connection to a compatible DNS server allows for some advanced services to function properly. If a DNS name is configured, the NMC can be accessed by its assigned DNS name, instead of IP address. For the Battery Manager to send email, at a minimum, the primary DNS server must be defined.

The first section of the DNS Configuration page displays relevant DNS information:

- Active Primary DNS Server
- Active Secondary DNS Server
- Active Host Name
- Active Domain Name (IPv4/IPv6)
- Active Domain Name (IPv6)

To override the DNS Settings, the following Manual DNS Settings must be provided:

- **Primary DNS**: Provide the IP address of the primary and, optionally, of the secondary Domain Name System (DNS) server. The primary server is always tried first.
  - **NOTE:** Selection of Override Manual DNS Settings will result in configuration data from other sources (typically DHCP) taking precedence over the manual configurations.
- **System Name Synchronization**: Allow the system name to be synchronized with the host name so both fields automatically contain the same value.
- **Host Name**: Configure a host name.
- **Domain Name**: Configure the domain name. This domain name is added automatically whenever a user enters only a host name in a field that accepts domain names (except e-mail addresses). IPv4 and IPv6 can also be used.

DNS Network Test

Configuration > Network > DNS > Test

This section allows for the user to test the DNS settings that they have provided. Contained on this page is the result of the *Last Query Response.* If the query succeeded, the result is a domain name, IP address, or mail exchange. If the query fails, an error message gives the reason for the failure.

- To Test the current DNS Settings, Issue a Query
  - Specify the Query by type:
    - Host: the URL name of the server
    - FQDN: the fully qualified domain name of the server
    - IP: the IP address of the server
    - MX: the mail exchange used by the server
  - Query Question: The value to be used for the selected query type: the URL, the IP address, the fully qualified domain name (for example, myserver.mydomain.com), or the mail exchange address.

Network Configuration for Web Access

Configuration > Network > Web > Access

Option	Description
Access	This section of the web interface allows the user to enable/disable access to the web interface. In most cases, in order to activate the changes to any of these selections, a user must first log off from the Battery Manager. A computer with telnet access must be used to re-enable web access. • **Enable HTTP:** Sets Hypertext Transfer Protocol (HTTP) as the means of access to the web interface. Access through HTTP is by user name and password; neither is encrypted, and data is not encrypted during transmission. • **Enable HTTPS:** Sets Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) as the means of access to the web interface. HTTPS encrypts user names, passwords, and data during transmission, and uses digital certificates for authentication. • **HTTP Port:** The port (80 by default) that HTTP uses to communicate. • **HTTPS Port:** The port (443 by default) that HTTPS uses to communicate. • **Require Authentication Cookie:** If enabled, a session cookie will be used for authentication tracking within the browser. **NOTE:** The cookie will be removed upon session end. • **Limited Status Access:** Select whether or not to display a read-only, public web page with basic device status. This feature is disabled by default and can be set via the 'Use as default page' option to show as the default landing page when a user accesses the device with just the IP/hostname (no specific page listed).

	NOTE: For either port, any unused port from 5000 to 32768 can be used for additional security. Users must then use a colon (:) in the address field of the browser to specify the port number.
	
	For port number 5000 and IP address 152.214.12.114:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

SSL Certificate	This page allows the user to view the status of an installed SSL Certificate, as well as Add, Replace, or Remove a security certificate. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL,** restarting the device creates a default certificate, a process which delays access to the interface for up to one minute. You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on. In a default certificate, the Organizational Unit field displays “Internally Generated Certificate,” and the Common Name field reports the serial number of the device. **Status**: • **Not installed**: A certificate is not installed, or was installed by FTP or SCP to an incorrect location. • **Generating**: A certificate is being generated because no valid certificate was found. • **Loading**: A certificate is being activated on the Battery Manager. • **Valid certificate**: A valid certificate was installed or was generated by the Battery Manager. Click on this link to view the certificate’s contents. • **Add or Replace Certificate File**: Enter or browse to the certificate file created with the Security Wizard. • **Remove**: Delete the current certificate.
	NOTE: See “Creating and Installing Digital Certificates” to choose a method for using digital certificates created by the Security Wizard or generated by the Battery Manager.

Console

Configuration > Network > Console

Option	Description
Access	This section of the web interface allows the user to configure access to the *Command Console*. • **Disable:** Disables access to the Command Console. • **Enable Telnet:** *Telnet* transmits user names, passwords, and data without encryption. • **Enable SSH:** Secure SHell (*SSH*) version 2 transmits user names, passwords and data in encrypted form. • Telnet Port: The TCP/IP port (23 by default) that *Telnet* uses to communicate. • SSH Port: The TCP/IP port (22 by default) that *SSH* uses to communicate.
NOTE: To enhance security, the port setting can be changed to any unused port from 5000 to 32768. Users must then specify the non-default port to gain access. *Telnet* clients require users to append either a space and the port number or a colon and the port number to the command line to access the command line interface. For **SSH**, see your *SSH* client documentation to specify a non-default port in the command line that starts *SSH*.	
SSH Host Key	This page allows the user to view the status of an installed *SSH* Host Key, as well as Add, Replace, or Remove a Host Key. • Status: Indicates whether the current *SSH* Host Key is valid. • Add or Replace Host Key: To use a host key you created with the Security Wizard, load the host key before you enable *SSH*. Browse to or enter the path name of the host key file created with the Security Wizard, and click Apply. If the host key has been removed or if no host key was loaded, and you enable *SSH*, the device restarts, and it generates a host key. Allowing the device to generate its own host key could make the *SSH* server unavailable for use for as long as 1 minute. Host Key Fingerprint: A fingerprint helps authenticate a server. If the Security Wizard is used to generate the host key, it also generates the fingerprint, which is displayed here when *SSH* is enabled and the host key is in use. When you first connect to the device using *SSH*, compare the fingerprint presented by the *SSH* client to the fingerprint that the Security Wizard generated to ensure that they match. (Almost all *SSH* clients display the fingerprint.) Remove: Remove the current host key.

NOTE: To use *SSH*, you must have an *SSH* client installed. Most Linux and other UNIX® platforms include an *SSH* client, but Microsoft Windows operating systems do not. Clients are available from various vendors.

Network Configuration SNMP

General Configuration SNMPv1

Configuration > Network > SNMPv1

All user names, passwords, and community names for Simple Network Management Protocol (*SNMP*) are transferred over the network as plain text. If your network requires encryption, disable SNMPv1 access or set the access for each community to Read. (Read access can receive status information and use SNMP traps.)

StruxureWare is Schneider Electric's platform of integrated software applications and suites that help maximize business performance while making the best of enterprise resources. To manage the Battery Manager on the public network of a StruxureWare system, you must have SNMP enabled in the Battery Manager interface. Read access will allow StruxureWare to receive traps from a Battery Manager, but Write access is required while you use the interface of the Battery Manager to set StruxureWare as a trap receiver.

For detailed information on enhancing the security of your system, see the *Security Handbook*, available on **www.schneider-electric.com**.

Option	Description
Access	Enable SNMPv1 Access: Enables SNMP version 1 as a method of communication with this device.
Access Control	You can configure up to four access control entries to specify which NMS can have access to the Battery Manager. • If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network. • If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device. **Community Name:** The name that a NMS must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are "public," "private," "public2," and "private2." **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows: • 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment. • 149.225.**255.255**: Access only by an NMS on the 149.225 segment. • 149.**255.255.255**: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. **Access Type:** The actions an NMS can perform through the community. • Read: GETS only, at any time. • Write: GETs and SETs at any time. **NOTE:** In the multi-user system, this now allows SETs while users are logged in which operates in the same manner as Write+. • Write+: GETS and SETS at any time. • Disable: No GETS or SETS at any time.

General Configuration SNMPv3

Configuration > Network > SNMPv3

For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users.

Access	SNMPv3 Access: Enables SNMPv3 as a method of communication with this device.
User Profiles	By default, lists the settings of four user profiles, configured with the user names “apc snmp profile1” through “apc snmp profile 4,” and no authentication and no privacy (no encryption of data). To edit the following settings for a user profile, click a user name in the list. **User Name:** The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters. **Authentication Passphrase:** A phrase up to 32 bytes, ASCII English characters; that verifies the NMS communicating with this device through SNMPv3, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time. **Privacy Passphrase:** A phrase up 32 bytes, ASCII English characters, that ensures the privacy of the data (by means of encryption) that a NMS is sending to this device or receiving from this device through SNMPv3. **Authentication Protocol:** The Schneider Electric implementation of SNMPv3 supports SHA or MD5 authentication. Authentication will not occur unless SHA or MD5 is selected here. **Privacy Protocol:** The Schneider Electric implementation of SNMPv3 supports AES or DES as the protocol for encrypting and decrypting data. Privacy of transmitted data requires that AES or DES is selected here. **NOTE:** You cannot select the privacy protocol if no authentication protocol is selected.

Access Control	You can configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles. To edit the access control settings for a user profile, click its user name. • If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device. • If you configure multiple access entries for one profile, the limit of four entries requires that one or more of the other user profiles must have no access control entry. If no access control entry is listed for a user profile, no NMS that uses that profile has any access to this device. **Access:** Mark the **"**Enable**"** check box to activate the access control specified by the parameters in this access control entry. **User Name:** From the drop-down list, select the user profile to which this access control entry will apply. **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by the NMS. • A host name or a specific IP address (such as 149.225.12.1) allows access by only the NMS at that location. An IP address mask that contain 255 restricts access as follows: • 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment. • 149.225.**255.255**: Access only by an NMS on the 149.225 segment. • 149.**255.255.255**: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

Enabling Modbus

Enabling Modbus allows a Building Management System to monitor the Battery Manager. The AP9922 supports Modbus serial (RTU) and Modbus TCP.

Modbus - Serial (RTU) Access

Configuration > Network > Modbus > Serial

To use Modbus RTU serial protocol, set the baud rate for Modbus access (9600 or 19200 bps), and define the Target Unique ID. The Target Unique ID is a unique identifier from 1 to 247, and needs to be unique on the Modbus bus.

Modbus - TCP Access

Configuration > Network > Modbus > TCP

To use Modbus TCP, a user can also enable Modbus TCP to view the device through your building management service's interface. The port is the Modbus TCP port number.

You must log off for the changes to take effect. See the Battery Management System *Installation* manual for Modbus installation information, including DIP switch configuration settings and serial Modbus connection.

FTP Server

Configuration > Network > FTP Server

The File Transfer Protocol (**FTP**) Server can be enabled or disabled from the primary FTP Server Access page. FTP transfers files without encryption. For higher security, disable the FTP server, and transfer files with Secure CoPy (SCP). Selecting Secure SHell (*SSH*) enables SCP automatically.

By default, the FTP server communicates with the Battery Manager through TCP/IP port 21. Both the specified port and the port one number lower than the specified port are used.

For enhanced security, the **port** being used can be changed. The appended port name must be preceded by a space or colon depending on the FTP client used. Allowed non-default port numbers are 5001 through 32768. Users must then use a colon (:) to specify the non-default port number.

For port 5001 and IP address 152.214.12.114:

```
ftp 152.214.12.114:5001
```

NOTE: At any time that you want a device to be accessible for management by StruxureWare, FTP Server must be enabled.

For detailed information on enhancing and managing the security of your system, see the Security Handbook, available from www.apc.com.

Notification

Configuration > Notification

You can configure Event Actions to occur in response to an event, or group of events. To configure multiple events simultaneously by severity level or category, use the “by group” option under Event Actions. For a summary of the configured event notifications, select the appropriate category or subcategory.

These actions notify users of the event in any of several ways:

- Active, automatic notification. The specified users or monitoring devices are contacted directly.
- Indirect notification in the event log. If no direct notification is configured, users must check the log to determine which events have occurred.

To configure an individual event, click the event name, and select the appropriate notification parameters.

Select the types of notification to be used for:

- Event Log: Record the event in the event log.
- Syslog: Notify Syslog servers to record the event in the Syslog system log.
- E-mail: Notify the defined e-mail recipient.
- Trap: Notify the configured trap receivers with an SNMP trap.

Battery String Event Handling

The number of string/battery related events of each kind has been limited to 20 events per string, due to the potential number of battery string events which can be generated.

If one of the signaled events clears and more alarm conditions exist, which have not been signaled, another event will be signaled as a previous one clears. See “Battery String Event Handling” on page 96 for more information.

Event Actions

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

- Active, automatic notification. The specified users or monitoring devices are contacted directly.
  - E-mail notification
  - SNMP traps
  - Remote Monitoring Service
  - Syslog notification
- Indirect notification
  - Event log. If no direct notification is configured, users must check the log to determine which events have occurred
  - You can also log system performance data to use for device monitoring. For more information on how to configure and use data logging, See “Logs” on page 95.
  - Queries (SNMP GETs)
  - For more information, see “Network Configuration SNMP” on page 83. SNMP enables an NMS to perform informational queries. For SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without the risk of allowing remote configuration changes.

Configure event actions

By default, logging an event is selected for all events. To define event actions for an individual event:

1. To find an event, click on a column heading to see the lists under the Device Events or System Events categories. Or you can click on a sub-category under these headings, like Security or Temperature.
2. Click on the event name to view or change the current configuration, such as recipients to be notified by e-mail, or Network Management Systems (NMSs) to be notified by SNMP traps. If no Syslog server is configured, items related to Syslog configuration are not displayed.

NOTE: When viewing details of an event configuration, you can enable or disable event logging or Syslog, or disable notification for specific e-mail recipients or trap receivers, but you cannot add or remove recipients or receivers. To add or remove recipients or receivers, see the following:

- “Servers” on page 94
- “E-mail Recipients” on page 91
- “SNMP Trap Receivers” on page 92

Configure event actions by group

1. Select how to group events for configuration:
   – Select Events by Severity, and then select one or more severity levels. You cannot change the severity of an event.
   – Select Events by Category, and then select all events in one or more pre-defined categories.
2. Click **Next** to move to the next screen to do the following:
   a. Select event actions for the group of events.
      • To select any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
      • If you selected **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** on the next screen.
3. Click **Next** to move to the next screen to do the following:
   a. If you selected **Logging** on the previous screen, select **Enable Notifications** or **Disable Notification**.
   b. If you selected **Email Recipients** on previous screen, select therecipients to configure.
   c. If you selected **Trap Receivers** on previous screen, select the trap receiver to configure.
4. Click **Next** to move to the next screen to do the following:
   a. If you are configuring **Logging** settings, view the pending actions and click **Apply** to accept the changes or click **Cancel** to revert to the previous settings.
   b. If you are configuring **Email Recipients** or **Trap Receivers,** select **Enable Notifications** or **Disable Notification** and set the notification timing settings (see “Notification parameters” on page 89 for more information on these settings).
5. Click **Next** to move to the next screen to do the following:
   a. View the pending actions and click **Apply** to accept the changes or click **Cancel** to revert to the previous settings.

Notification parameters Configuration fields define e-mail parameters for notifications of events.

They are usually accessed by clicking the receiver or recipient name.

Field	Description
Delay *n* time before sending	If the event persists for the specified time, the notification is sent. If the condition clears before the time expires, no notification is sent.
Repeat at an interval of *n*	The notification is sent repeatedly at the specified interval (the default is every 2 minutes until the condition clears).
Up to *n* times	During an active event, the notification repeats for this number of times.
or	
Until condition clears	The notification is sent repeatedly until the condition clears or is resolved.

NOTE: For events that have an associated clearing event, you can also set these parameters.

E-mail Notifications

Configuration > Notification > E-mail

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

- The IP addresses of the primary and, optionally, the secondary DNS servers.
- The IP address or DNS name for the SMTP Server and From Address.
- The e-mail addresses for a maximum of four recipients.
- You can use the To Address setting of the recipients option to send e-mail to a text-based screen.

E-mail Server Settings

Configuration > Notification > E-mail > Server

This screen configures the Outgoing Mail server settings, as well as several Advanced email settings. Further, this page displays current primary and secondary DNS server addresses.

- **Outgoing Mail Configuration**
  - **From Address:**
    - user@[IP_address] (if an IP address is specified as Local SMTP Server
    - user@domain (if DNS is configured and the DNS name is specified as Local SMTP Server) in the e-mail messages.
      NOTE: The local SMTP server may require that you use a valid user account on the server for this setting. See the server documentation.
  - **SMTP Server:** The IPv4/ IPv6 address or DNS name of the local SMTP server.

    NOTE: This definition is required only when the SMTP server is set to *Local*.
  - **Port:** The SMTP default port is 25. Alternative ports: 465, 587, 5000 to 32768.
  - **Authentication:** Enable this if the SMTP server requires authentication. This performs a simple authentication, not SSL.
    - User Name, Password: If your mail server requires authentication, enter your user name and password here.
- **Advanced**
  - Use SSL/TLS: Select when encryption is used.

    •**Never:** The SMTP server does not require nor support encryption.

    •**If Supported:** The SMTP server advertises support for STARTTLS, but doesn't require the connection to be encrypted. The STARTTLS command is sent after advertisement is given.

    •**Always:** The SMTP server requires the STARTTLS command to be sent on connection to it.

    •**Implicitly:** The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.
    - **Require CA Root Certificate:** This should only be enabled if the security policy of your organization does not allow for implicit trust of SSL connections. If this is enabled, a valid root CA certificate must be loaded for encrypted e-mails to be sent.
    - **File Name:** This field is dependent on the root CA certificates installed, and whether or not a root CA certificate is required.

E-mail Recipients

Configuration > Notification > E-mail > Recipients

Specify up to four e-mail recipients. Click on "*Add Recipient*" or the email address(if already configured) to configure the settings. *'Active E-mail Server Settings'* will display the current configuration.

E-mail Recipient

- **Generation:** Checkbox in which Enable is checked by default.
- **To Address:** The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's mobile gateway account (for example, `myacct100@skytel.com`). The mobile gateway will generate the page. To bypass the DNS lookup of the IP address of the mail server, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.
- **Language:** The language which the e-mail notification will be sent in. This is dependent on the installed language pack (if applicable).
- **Server**
  - **Local:** This is through the site-local SMTP server. This recommended setting ensures that the e-mail is sent using the site-local SMTP server. Choosing this setting limits delays and network outages and retries sending e-mail for many hours. When choosing the Local setting you must also enable forwarding at the SMTP server of your device and set up a special external e-mail account to receive the forwarded e-mail. Check with your SMTP server administrator before making these changes.
  - **Recipient:** This is the SMTP server of the recipient. The Battery Manager performs an MX record look-up on the recipients e-mail address and uses that as its SMTP server. The e-mail is only sent once so it could easily be lost.
  - **Custom:** This setting enables each e-mail recipient to have its own server settings. These settings are independent of the settings given under "SMTP Server" above. If your mail server requires authentication, type your user name and password.

Custom E-mail Server Settings

- See "Outgoing Mail Configuration" on page 90.

Email SSL Certificates

Configuration > Notification > E-mail > SSL Certificates

Load a mail SSL certificate for greater security. The file must have an extension of `.crt` or `.cer`. Up to five files can be loaded at any given time. An invalid certificate will display "n/a" for all fields except **File Name**. Certificates can be deleted using this screen. Any e-mail recipients using the certificate should be manually modified to remove reference to this certificate.

Test Email

Configuration > Notification > E-mail > Test

Send a test message to a configured recipient.

SNMP Traps Notifications

Configuration > Notification > SNMP Traps

SNMP Trap Receivers

Configuration > Notification > SNMP Traps > Trap Receivers

With Simple Network Management Protocol (SNMP) traps, you can automatically get notifications for significant events. They are a useful tool for monitoring devices on your network. The trap receivers are displayed by **NMS IP/Host Name**, where NMS stands for Network Management System. You can configure up to six trap receivers.

If you delete a trap receiver, all notification settings configured under “Configuring event actions” for the deleted trap receiver are set to their default values.

To configure a new trap receiver, click *‘Add Trap Receiver.’* To edit (or delete) one, click its IP address/ host name.

- **Trap Generation:** Enable (the default) or disable trap generation for this trap receiver.
- **NMS IP/Host Name:** The IPv4/ IPv6 address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.
- **Language:** Select a language from the drop-down list. This can differ from the UI and from other trap receivers.
- Select either the **SNMPv1** or **SNMPv3** radio button to specify the trap type. For an NMS to receive both types of traps, you must separately configure two trap receivers for that NMS, one for each trap type.
  - **SNMPv1**
    - **Community Name:** The name (“public” by default) used as an identifier when SNMPv1 traps are sent to this trap receiver.
    - **Authenticate Traps:** When this option is enabled (the default), the NMS identified by the NMS IP/Host Name setting will receive authentication traps (traps generated by invalid attempts to log on to this device).
  - **SNMPv3**
    - **User Name:** Select the identifier of the user profile for this trap receiver.

SNMP Traps Test Screen

Configuration > Notification > SNMP Traps > Test

- **Last Test Result:** The result of the most recent SNMP trap test. A successful SNMP trap test verifies only that a trap was sent; it does not verify that the trap was received by the selected trap receiver. A trap test succeeds if all of the following are true:
  - The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
  - The trap receiver itself is enabled.
  - If a host name is selected for the **To** address, that host name can be mapped to a valid IP address. Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver is configured, a link to the **Trap Receiver** configuration screen is displayed.

Remote Monitoring

Configuration > Notification > Remote Monitoring

The Schneider Electric Remote Monitoring Service (RMS) is an optional service providing maximum protection to your systems. RMS is a professional service that monitors your power systems and surrounding environment from a remote operation center, 24 hours a day, 7 days a week.

Through the RMS Web site, you can instantaneously modify the response to your device events. Information concerning your equipment and system events can also be retrieved at any time from any place where you can log on to the Internet.

If you wish to purchase this option or find out more information, please contact your hardware vendor or visit the RMS website. Enabling the Remote Monitoring Service is made available after a successful registration has been completed.

Registration

To activate Schneider Electric RMS for the Battery Manager, select Remote Monitoring, choose between **Register Company and Device** and **Register Device Only**, complete the form, and click **Send APC RMS Registration**.

Use the **Reset Remote Monitoring Service Registration** check box to discontinue the service, whether permanently or temporarily (for example, if you are moving a Battery Manager).

Syslog

Configuration > Logs > Syslogs

Servers

Configuration > Logs > Syslogs > Servers

Implementation of Syslog supports the sending of notifications to specific servers. The Syslog servers record events that occur, at network devices, in a log that provides a centralized record of events. Describing the Syslog in great detail is outside of the scope of this manual. See **RFC3164** online for more information about Syslog.

The Battery Manager can be configured to send a notification of events to up to four Syslog servers. To add a server, click Add Server. To modify an existing server, click the server's name. The Battery Manager uses the default port 514 to send Syslog messages.

NOTE: To disable Syslog messages, See “Configure event actions” on page 88. In addition, Syslog messages can be disabled if the "Message Generation" option is not selected in *Syslog Settings*.

Language: Choose a language for any Syslog messages.

Protocol: Choose between UDP and TCP.

Settings

Configuration > Logs > Syslogs > Settings

Messages from this device will be categorized by Facility Code, and the associated facility categorization allows Syslog messages from different devices to be placed in separate logs.

These messages can be categorized in the drop-down list by an available Syslog priority. The local severity options are Critical, Warning, and Informational. In addition, Syslog supports Severity Mapping. Various system events can be prioritized and highlighted through the generation of a severity map.

Test

Configuration > Logs > Syslogs > Test

Last Test Result	Result of Last Test Performed
Server	The message will be sent to all configured servers.
Severity	Select a severity level (Syslog priority) for the test message.
Test Message	Format the message to consist of the event type (APC, System, or Device, for example) followed by a colon, a space, and the event text (50 character max).

Tests

LED Blink

Tests > Networks > LED Blink

Initiate flashing of the device's Status and Link LEDs on the Ethernet Port to assist the user in locating the physical device.

Logs

Event Log

Logs > Events > Log

Event Log Filtering: By default, the event Log displays the most recent events first. To see the data log listed together on a Web page, click the *Launch Log in New Window* button. The log entries can always be cleared, by clicking **Clear Log**.

NOTE: JavaScript must be enabled in your browser to do this.

Event Log: The Event Log lists the most recent events, including the date and time each event occurred, in reverse chronological order.

System events are logged for most activities. These include, but are not limited to:

- Abnormal internal system events.

To view the details on what events will be logged, see the “by event” category, under Event Actions, on the Notification menu, of the Configuration drop down menu.

- To change the color of log text:
  - Event log color coding is configurable on a per-user basis. To configure color coding for a specific user, select **Configuration > Security > Local Users > Management**, then select the user to configure.
  - On the *User Configuration* page, under the *User Preferences* section, mark the Event Log Color Coding check box to enable color-coding of event log text.
    - Red text indicates a critical alarm event
    - Orange text indicates a warning alarm event
    - Blue text indicates an informational event
    - Green text indicates a clearing event

Battery String Event Handling

The number of string/battery related events of each kind has been limited to 20 events per string, due to the potential number of battery string events which can be generated.

If one of the signaled events clears and more alarm conditions exist - which have not been signaled, another event will be signaled as a previous one clears.

These events include "Cell shorted", "Open fuse or connection", "Capacity is low", "Ohmic value is high", "Thermal runaway potential exists", "Dryout/sulfation present."

On the web interface, the Home page and the Status/Alarm page will show all existing alarms:

Log Retrieval - General

The Log Retrieval process can be useful for many reasons, and is a useful option to utilize. Creating a log is resource intensive. Depending on your system's configuration, generating and downloading a data log may require several minutes to complete. The computer that you are using, and/or the web browser may appear unresponsive during this time.

Event Log Filtering

Event Log Filtering: By default, the event Log displays the most recent events first. To see the data log listed together on a Web page, click the *Launch Log in New Window* button. The log entries can always be cleared, by clicking **Clear Log**.

NOTE: JavaScript must be enabled in your browser to do this.

To display the entire event log, or to change the number of days or weeks for which event log information is displayed, select “Last,” choose an option from the drop-down box, and click Apply.

To display events logged during a specific time range, select “From”, specify the beginning and ending dates and times for which to display events, then click Apply.

NOTE: Enter the time using the 24-hour clock format.

View or Delete the Event Log

To delete all events recorded in the log, click **Clear Log** on the Web page that displays the log. Deleted events cannot be retrieved. To disable the logging of events based on their assigned severity level or their event category see Configuring Event Actions by Group.

Retrieval of Event Log Using Web Interface

To open or save the log in a text file, click on the floppy disk icon on the right side, contained on the same line as the Event Log heading.

Reverse Lookup

When a network-related event occurs, reverse lookup logs both the IP address and (if a domain name entry exists) the domain name for the networked device associated with the event in the event log. Reverse lookup is disabled by default.

Enable this feature unless you have no DNS server configured or have poor network performance because of heavy network traffic.

If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change less frequently than IP addresses in systems using Bootp or DHCP device configuration, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events.

Event Log Size

Logs > Events > Size

The size of the even log can be specified at this interface screen. The size is defined by events. The minimum number of events is 25, and the maximum number of events is 1500. Resizing the Event Log will also delete all current log entries. Before continuing, offloading the Event Log via FTP or SCP is suggested.

Data Log

The file will contain reports of the date and time that data is logged. Under the abbreviated column headings the data is recorded.

The following events are logged:

- Battery Voltages and Ohmic values
- String Current
- Ambient / Pilot Temperature
- Charge / Discharge Mode
- Each entry is listed by the date and time the data was recorded.

Retrieve Data Log File Using Web Interface

Logs > Events > Log

To open or save the log in a text file, click on the floppy disk icon on the right side, contained on the same line as the ***Data Log*** heading.

NOTE: See “Log Retrieval - General” on page 96.

Retrieve Data Log File using FTP or SCP

An *Administrator* or *Device User* can use **FTP** or **SCP** (if enabled) to retrieve an **event log** file (*event.txt*) or **data log** file (*data.txt*).

- The file reports all events or data recorded since the log was last deleted or truncated after reaching maximum size.

NOTE: The file received includes information not available to the user through the web interface. Using SCP to retrieve the log file allows for the use of encryption-based security protocols; retrieval by FTP is unencrypted. See “Log Retrieval - General” on page 96.

FTP Retrieval of event.txt or data.txt

Some FTP clients require a colon instead of a space between the IP address and the port number.

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

1. At a command prompt, type `ftp` and the Battery Manager’s IP address, and press ENTER.

   ```
   ftp>open ip_address port_number
   ```

   NOTE: For enhanced security, using a non-default port value is encouraged. See “FTP Server” on page 86 for more information. The default Port setting for the FTP Server is 21; if changed, use the current value.

2. Enter the User Name and Password for either *Super User, Administrator, Device User or Read-Only*.

   NOTE: Credentials are case-sensitive.

3. Use the **get** command to retrieve the text of a log to your local drive.

   ```
   ftp>get event.txt
   ```
   or
   ```
   ftp>get data.txt
   ```

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

FTP Delete

The contents of either log can be cleared via FTP. You will not be asked to confirm the deletion. If you clear the data log, the event log records a deleted-log event. The new *event.txt* file records the event.

After logging in, use the **del** command:

```
ftp>del event.txt
```
or
```
ftp>del data.txt
```

Retrieval of event.txt or data.txt by SCP

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

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

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

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

Graphing the Data Log

Logs > Data > Graphing

Data log graphing provides a graphical display of logged data. Graphing large amounts of data may cause performance problems on the computer and Web browser you are using. Reducing the number of data points or data lines being graphed may improve performance.

NOTE: As an alternative to the built-in graphing functionality, FTP or SCP can be used to retrieve the data.txt file which can be imported into a spreadsheet, or other graphic software. See “Log Retrieval” in the Data: Log section for further FTP and SCP instructions.

Parameter	Description
Graph Data	To graph multiple data items, select the column heading in order to specify the data to be graphed.
Graph Time	To graph all records, or to change the number of hours, days, or weeks for which data log information is graphed, select Last. Select an option from the drop-down menu, then click Apply. To graph data logged during a specific time range, select From. Specify the beginning and ending dates and times for which to graph data, then click Apply. **NOTE:** Enter the time using the 24-hour clock format.

Click *Apply* to view the graph, or click *Cancel* to discard the changes. Click *Launch Graph* in New Window to display the graph in a new browser window that provides a full-screen view.

Graph Usability

At the lowest magnification, all data is displayed and you cannot move left or right. At the higher magnification levels, left/right movement is allowed. The blue bar between the left and right arrows changes size to indicate how many of the total data records are being displayed and the relative location of the displayed data records. The blue bar is not a scroll bar; however, you may click on any part of the gray line or blue bar to re-center the graph.

If the data items have the same unit of measurement, the units are displayed on the left side of the graph. If the data items do not have the same units, the units are displayed in the legend with their corresponding data item.

Graph Data Lines

Graph data lines provide a visual representation of the stored data records. Move the mouse pointer over any horizontal line to view the date and time as well as the Y-axis value for that data record. Click on any point in the graph to center and magnify that point on the screen.

Data Log Collection Interval

Logs > Data > Interval

The Log Interval shows how often data is recorded for the *Charge Mode Log* and *Discharge Mode Log*. You can change these values. Based on the interval and the data log size specified, the system calculates and displays the length of time that data is kept. Decrease the interval time to record data more frequently but to keep the record for a shorter time. Increase the interval time to record data less frequently but to keep the record for a longer time.

When Batteries are sitting on float, the system is in *Charge Mode*. In this mode, information is collected by default at 10 minute intervals.

When the device is in *Discharge Mode*, the UPS is providing power and the batteries are discharging, a secondary interval of data collection initializes. During *Discharge Mode*, data is logged at 1 minute intervals. To save the data log periodically to a server, use the rotation option.

Configuring Data Log Rotation

Logs > Data > Rotation

Since there is a limited amount of solid state storage in the Battery Manager, users may opt to periodically back up the data log to an FTP server to avoid loss of data due to automatic deletion of old information.

Data Log rotation causes the data log to be saved periodically to a user provided FTP server. The file name and location must be specified, and new information is appended onto the specified file on the FTP server. If desired, the data log repository can also be password protected.

Parameter	Description
Last Upload Result	Indicates whether the last upload of the data file to the FTP server succeeded or failed, or displays “None Available.”
Data Log Rotation	Enable it by selecting the check box.
FTP Server	IP address or host name of the server.
User Name	The user name required to send data to the stored log file. This user must also have read and write access to the stored log file and the directory (folder) in which it is stored.
Password	FTP Server Password required to send data to the stored log.
File Path	The path to the stored log file on the FTP server. You must specify a path that already exists on the FTP Server.
Filename	The file name to which the log is saved.
NOTE: Data is appended to the file, with no overwriting.	
Unique Filename	If this option is selected, the log is saved to daily log files named by including the date as part of the filename. The file name is in the format MMDDYYYY_filename.txt where filename is user configurable and MMDDYYYY represents the NMC date.
NOTE: Data is appended to the file if the data records are from the same day, with no overwriting. User should verify that the file size does not become too large for available disc space.	
Parameters	Define the following: • The interval at which the data log will be uploaded to the server. • If an upload fails, how frequently it will be retried. • The maximum number of times the upload will be retried before being skipped.
Upload Now	To initiate the first upload immediately, click Upload Now!

Data Log Size

Logs > Data > Size

Specify the maximum size (number of entries) of the data log. When you resize the data log, all existing log entries are deleted. It is recommended that a user retrieve the existing entries using the web, FTP or SCP before you resize the log.

After the data log reaches the maximum size, the oldest entries are deleted from the log as new entries are logged.

Firewall Log

Logs > Firewall

This page contains a log of active Firewall Policies. Log entries contain information about the traffic and the rules action (allowed, discarded). When logged here, these events are not logged in the main Event Log. The firewall log is cleared when the Battery Manager reboots.

General Options

Configuration > General > Identification

Define the values for:

- *Host Name Synchronization:* Allows the *Name* to be synchronized with the *System Name*, so both fields automatically contain the same value.

  A *Host Name* does not allow spaces. Therefore, if *Host Name Synchronization* is enabled, spaces are not allowed for *Name*. An attempt to enter a space in the *Host Name* field will be rejected as an invalid entry. If *Host Name Synchronization* is turned off, spaces are allowed.
- *Name* (the device name)
  - The *Name* assigned to the device is used by the *sysName OID* in the NMC's SNMP agent, by Remote Monitoring Service, and by StruxureWare Data Center.
- *Contact* (the person responsible for the device)
  - The *Contact* is the person responsible for the maintenance of the device. This value is used by the *sysContact OID* in the SNMP agent and by StruxureWare Data Center.
- *Location* (the physical location).
  - The *Physical Location* of the device is used by the *sysLocation OID* in the SNMP agent, by Remote Monitoring Service, and by StruxureWare Data Center.
- *System Message*
  - When defined, a custom message will appear on the log on screen for all users.

Services Used By	Name	Contact	Physical Location
sysName OID in the NMC's SNMP agent	●	●	●
Remote Monitoring Service	●		●
StruxureWare Data Center	●	●	●

NOTE: For more information about MIB-2 OIDs, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide,* on **www.schneider-electric.com**.

Set the Date and Time

Configuration > General > Date/Time > Mode

This section allows the user to set the time and date used by the Battery Manager. On this page, *Current Settings* displays the current date and time, as well as other related settings. You can change the current settings manually or from a Network Time Protocol (NTP) Server.

Manual Mode:

- Enter the date and time for the Battery Manager.
- Mark the check-box Apply Local Computer Time to match the date and time settings of the computer you are using.
- Synchronize with NTP Server: Have an NTP Server define the date and time for the Battery Manager.

Primary NTP Server	Enter the IP address or domain name of the primary NTP server.
Secondary NTP Server (Optional)	Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.
Time Zone	Select a time zone. The number of hours preceding each time zone in the list is the offset from Coordinated Universal Time (UTC), formerly Greenwich Mean Time.
Update Interval	Define how often, in hours, the Battery Manager accesses the NTP Server for an automatic update. *Minimum*: 1; *Maximum*: 8760 (1 year).
Update Using NTP Now	Initiate an immediate update of date and time from the NTP Server.
NOTE: Selection of Override Manual NTP Settings will result in configuration data from other sources (typically DHCP) taking precedence over the manual configurations set here.	

Daylight Saving

Configuration > General > Date/Time > Daylight Savings

Enable either traditional United States Daylight Saving Time (DST) or enable and configure a customized daylight saving time to match how Daylight Saving Time is implemented in your local area. DST is disabled by default.

When customizing Daylight Saving Time (DST):

- If the local DST always starts or ends on the fourth occurrence of a specific weekday of a month (e.g, the fourth Sunday), choose **Fourth/Last**. If a fifth Sunday occurs in that month in a subsequent year, the time setting still changes on the fourth Sunday.
- If the local DST always starts or ends on the last occurrence of a specific weekday of a month, whether it is the fourth or the fifth occurrence, choose **Fifth/Last**.

Using a Configuration File (.ini)

Configuration > General > User Config File

See “Retrieval of the .ini File Using Web Interface” on page 106. for more information.

Configuring Links

Configuration > General > Quick Links

Quick Links displayed at the bottom left corner of the web interface pages are user-definable. They provide quick access to useful Web sites, servers, devices, etc. To edit the URL of a link, select the **Configuration** tab, **General** from the drop down menu bar, and **Quick Links**.

Within each link, the option to *Reset to Defaults* is also presented.

By default, the links access the following web pages:

- **Link 1:** Website homepage
- **Link 2:** Demonstrations of Schneider Electric web-enabled products
- **Link 3:** Information on Schneider Electric Remote Monitoring Services

To reconfigure any of the following, click the link name in the **Display** column:

The Name that fully identifies the target or purpose of the link is required (up to 40 characters), as well as the URL address (up to 100 characters).

About the Battery Manager

Network

About > Network

The hardware and software information conveyed at this page is useful to Customer Support to help troubleshoot problems with the Battery Manager. This page allows the user to view many device parameters.

Model number, serial number, hardware revision, manufacture date, MAC address, as well as current APC OS (AOS), Application Module (APP), as well as APC Boot Monitor (Bootmon) information is provided.

Unit

About > Unit

Displays information about the individual Battery Manager units.

Support

About > Support

At this page, a user can access various support websites and consolidate various data into a single zipped file for troubleshooting purposes and customer support. The data includes the event and data logs, the configuration file (see “Retrieving and Exporting the .ini File”), as well as complex debugging information.

Creating the support file is a two step process. First, click *Generate Logs,* to gather and compress the data. This process can take several minutes. During the preparation of this data, progress can be judged by observing the progress bar.

Once complete, click *Download* to have the compressed file transferred to your computer. At this point, the file is ready to be sent to Customer Support.

Available Data Includes:

- *Support Resources:* Contact e-mail addresses, websites, and phone numbers for additional sales, customer service, or technical support questions.
- *Technical Support Debug Information Download:* This feature captures an assortment of debug data into a single file and then allows the user to download that file to a local computer which is intended for technical support use.
- *Generate Logs:* A new internal debug archive containing various files for subsequent download and review by technical support is generated.
- *Download:* Initiates a download of the currently stored debug archive.

  NOTE: Make sure you have previously clicked the “Generate Logs**”** button if no file is downloaded.

For problems that are not described here, or if the problem still persists, contact **Worldwide Customer Support**, www.apc.com/support.

Device IP Configuration Wizard

Capabilities, Requirements, and Installation

How to use the Wizard to configure TCP/IP settings

The Device IP Configuration Wizard can discover Battery Managers that do not have an IP address assigned. Once discovered, you can configure the IP address settings for the cards. You can also search for devices already on the network by entering an IP range to define the search. The Utility scans the IP addresses in the defined range and discovers Battery Managers that already have a DHCP-assigned IP address.

NOTE: For detailed information on the Utility, see the Knowledge Base on the support page of the www.apc.com website and search for FA156064 (the ID of the relevant article).

NOTE: To use the DHCP Option 12, see Knowledge Base ID FA156110.

System requirements

The Device IP Configuration Wizard runs on Microsoft® Windows® 2000, Windows Server® 2003, Windows Server® 2012, and on 32- and 64-bit versions of Windows XP, Windows Vista, Windows 2008, Windows 7, and Windows 8 operating systems. The Device IP Configuration Wizard supports cards that have firmware version 3.0.x or higher and is for IPv4 only.

Installation

To install the Device IP Configuration Wizard from a downloaded executable file

1. Go to http://www.apc.com/tools/download.
2. Download the Device IP Configuration Wizard.
3. Run the downloaded executable file.

When installed, the Device IP Configuration Wizard is available through the Windows Start menu options.

Configuration File (.ini) Settings

Retrieving and Exporting the .ini File

Summary of the Procedure

Configuring new devices, whether replacement devices, or when setting up essentially similar systems can be greatly simplified by re-using the configuration settings from an existing device with desired settings. An Administrator can retrieve the .ini file of a Battery Manager and then export it to one or more Battery Managers. Using a .ini file can also be useful for backup purposes, in case of a future device failure. The config.ini file can be retrieved in several ways.

1. Configure a Battery Manager to have the settings you want to export.
2. Retrieve the .ini file from that Battery Manager.
3. Customize the file to change at least the TCP/IP settings.
   NOTE: Retain the original customized file for future use. Each receiving Battery Manager network card uses the file to reconfigure its own settings, and then deletes it. **The file that you retain is the only record of your comments.**
4. Use a file transfer protocol supported by the Battery Manager to transfer a copy to one or more other Battery Managers. For a transfer to multiple Battery Managers, use an FTP or SCP script or the .ini file utility.

Contents of the .ini file

The config.ini file you retrieve from a Battery Manager contains the following:

- *section headings* and *keywords* (only those supported for the device from which you retrieve the file)*:* Section headings are category names enclosed in brackets ([ ]). Keywords, under each section heading, are labels describing specific Battery Manager settings. Each keyword is followed by an equals sign and a value (either the default or a configured value).
- The `Override` keyword: With its default value, this keyword prevents the exporting of one or more keywords and their device-specific values, e.g., in the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the Battery Manager) blocks the exporting of values for the `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.

Retrieval of the .ini File Using Web Interface

Configuration > General > User Config File

At the User Configuration File page of the web interface, the current config.ini file can be downloaded, or, a new config.ini file can be uploaded.

Retain the original customized file for future use. **The file that you retain is the only record of your comments.** Comments are ignored by the NMC upon file import.

Status	Reports the progress of the upload. The upload succeeds even if the file contains errors, but a system event reports the errors in the event log.
Upload	Browse to the customized file and upload it so that the current Battery Manager can use it to set its own configuration.
Download	Prompts the user to download the config.ini file.

Retrieval of the .ini File Using FTP

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

1. If possible, use the interface of the Battery Manager to configure it with the settings to export. Directly editing the .ini file risks introducing errors.
2. To use FTP to retrieve config.ini from the configured Battery Manager:
   a. Open a connection to the Battery Manager, using its IP Address:

      ```
      ftp> open ip_address
      ```

   b. Log on using the Super User/Administrator user name and password.
   c. Retrieve the config.ini file containing the Battery Manager's settings:

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

NOTE: By default, the file is written to the folder from which you launched FTP. See *Release Notes: ini File Utility, version 2.0,* available at www.apc.com/support in the Knowledge Base.

Customizing

Using a text editor, customizable features and meta data of the file include:

- Comments
  – Start each comment line with a semicolon (`;`)
- Section Headings, Keywords, and Pre-defined values
  – Not case-sensitive (defined string values are case-sensitive).

Enclose in quotation marks any values that contain leading or trailing spaces, or happen to have already been in quotation marks.

- Adjacent quotation marks indicate no value.

  ```
  LinkURL1=""
  ```

- Indicates that the URL is intentionally undefined.
- To export:
  – Scheduled Events: Configure the values directly in the .ini file
  – System Time: Export the `[SystemDate/Time]` section as a separate .ini file. Alternatively, access the Network Time Protocol server, and configure `enabled` for `NTPEnable`:

    ```
    NTPEnable=enabled
    ```

Copy the customized file to another file name in the same folder:

– The file name can have up to 64 characters and must have the .ini suffix.
– Retain the original customized file for future use. **The file that you retain is the only record of your comments.**

Transferring the File to a Single Battery Manager

- Select the Configuration tab, General on the top menu bar, and User Config File on the dropdown menu. Enter the full path of the file, or use Browse.
- Use any file transfer protocol supported by Battery Managers, i.e., FTP, FTP Client, SCP, or TFTP. The following example uses FTP:
  - From the folder containing the copy of the customized .ini file, use FTP to log in to the Battery Manager to which you are exporting the .ini file:

```
ftp> open ip_address
Export the copy of the customized .ini file to the root
directory of the receiving Battery Manager:
ftp> put filename.ini
```

Exporting the File to Multiple Battery Managers

- You can export the file to multiple devices by using FTP or SCP with a script. The script would incorporate and repeat the steps used in exporting a single Configuration file
- Batch processing files, and the APC .ini file utility are also available from **www.apc.com/tools/download**.
- To create the batch file and use the utility, see *Release Notes: ini File Utility, version 2.0, a*vailable at www.apc.com/support in the Knowledge Base.

The Upload Event and Error Messages

After the Battery Manager updates its settings using the .ini file, the user will see:

```
Configuration file upload complete, with number valid values
```

If a keyword, section name or value is invalid, the upload by the receiving Battery Manager succeeds, and additional event text states the error.

Event text	Description
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number.*	If a section name is invalid, all keyword/ value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number*.	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, an incomplete upload occurs. Reduce the size of the file, or divide it into two files, and try uploading again.

Errors Generated by Overridden Values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values. See “Contents of the .ini file” on page 106 for information about which values are overridden.

Because the overridden values are device-specific, ignore these messages as they are not applicable to or relevant for other Battery Managers. To prevent these error messages, you can delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Related Topics

On Windows operating systems, instead of transferring .ini files, you can use the Device IP Configuration Wizard to update the basic TCP/IP settings of Battery Managers and configure other settings through their user interface. See “Device IP Configuration Wizard” on page 105 for more information.

File Transfers

Upgrading Firmware

Keeping firmware versions current and consistent across your network allows for implementation of the latest features, performance improvements, as well as bug fixes. Regular upgrades also ensures that all Battery Managers support the same features, in the same manner. Obtain the free, latest firmware version from **www.apc.com/tools/download**

Firmware consists of:

- Boot Monitor Module *(bootmon)*
- APC Operating System *(AOS)*
- Application Module *(APP Module)*

The naming convention used for the *APP Module* and *AOS* indicate the context, the firmware version, type, and version number. This information is also useful for troubleshooting and enables you to determine if updated firmware is available at www.apc.com.

The *APP Module* name differs according to the device type. The *AOS* module is always named `aos`, and the *boot monitor module* is always named `bootmon`.

Version numbers of the firmware modules may differ, but compatible modules are released together. Never combine *APP Module* and *AOS modules* from different releases.

NOTE: If the *bootmon* must be updated, a *bootmon* module is included in the firmware release. Otherwise, the *bootmon* module that is installed on the card is compatible with the firmware update.

Firmware Module Files

A firmware version has three modules, and they *must* be upgraded (placed on the NMC) in this order:

	Module	Description
1	boot monitor (bootmon)	Roughly equivalent to the BIOS of a PC
2	APC Operating System (*AOS*)	Can be thought of as the NMC operating system
3	Application Module	Specific to the device, e.g. the Battery Manager

(Each module contains one or more Cyclical Redundancy Checks (CRCs) to protect its data from corruption).

NOTE: When you transfer individual firmware modules, *Bootmon* must precede AOS, if *bootmon* update is required. The *AOS* module must be transferred to the Battery Manager before you transfer the APP Module.

The *bootmon*, the *AOS*, and the *App Module* file names share the same basic format:

- `apc_hardware-version_type_firmware-version.bin`
- `apc`: Indicates the context.
- `hardware-version: hw0n` where n identifies the hardware version on which you can use this file.
- `type`: Identifies which module.
- `version`: The version number of the file.
- `bin`: Indicates that this is a binary file

Firmware File Transfer Methods

Use one of these three methods:

- **Battery Manager Firmware Upgrade Utility on Windows**. On a Windows operating system, use the **Firmware Upgrade Utility** downloaded from **www.apc.com**.
- **Use FTP or SCP**. Use **FTP or SCP** to transfer the individual AOS and App Module firmware.To upgrade multiple Battery Manager's using an FTP client or using SCP, write a script which automatically performs the procedure.
- **Export configuration settings**. You can create batch files and use a utility to retrieve configuration settings from multiple Battery Managers and export them to other Battery Managers.
- **Use XMODEM through a serial connection.** Use **XMODEM** through a serial connection to transfer the individual firmware modules from your computer to the Battery Manager. This method is also one which works with a Battery Manager NOT on your network.

Using the Firmware Upgrade Utility on Windows Systems

On any supported Windows operating system, the *Firmware Upgrade Utility* automates the transferring of the firmware modules, *in the correct module order*. The utility only works with an Battery Manager that has an IPv4 or IPv6 address.

Unzip the downloaded firmware upgrade file and double-click the .exe file. Then enter the IP address, the user name, and the password in the dialog fields and click **Upgrade Now**. You can use the **Ping** button to test your entered details. See also "Using the Firmware Upgrade Utility for Multiple Upgrades on Windows" .

Using the Utility for Manual Upgrades, Primarily on Linux.

On non-Windows operating systems, the Firmware Upgrade Utility extracts the individual firmware modules, but does not upgrade the Battery Manager. See “Firmware File Transfer Methods” for the different upgrade methods after extraction.

To extract the firmware files:

1. After obtaining the files from the downloaded firmware upgrade file, run the *Firmware Upgrade Utility* (the .exe file).
2. At the prompts, click *Next*>, and then specify the directory location to which the files will be extracted.
3. When the *Extraction Complete* message displays, close the dialog box.

FTP to Upgrade Battery Manager

To use FTP to upgrade an Battery Manager over the network:

- The Battery Manager must be on the network, with its system IP, subnet mask, and default gateway configured.
- The FTP server must be enabled at the Battery Manager, see “FTP Server” .

NOTE: To transfer the files, perform these steps (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two):

1. The firmware module files must be extracted, see “To extract the firmware files:”
2. At a computer on the network, open a command prompt window. Go to the directory that contains the firmware files, and list the files:

   ```
   C:\>cd apc
   C:\apc>dir
   For file information, See “Firmware Module Files” on page 110.
   ```

3. Open an FTP client session:

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

4. Type `open` with the **IP address** of the Battery Manager, and press ENTER. If the **port** setting for the FTP Server has changed from its default of **21**, you must use the non-default value in the FTP command.

   - For Windows FTP clients, separate a non-default port number from the IP address by a space. For example (showing a space before 21000):

     ```
     ftp> open 150.250.6.10 21000
     ```

   - Some FTP clients require a colon instead before the port number.

5. Log in using an account with the correct level of user access to perform file transfers (apc is the default user name and password).
6. Upgrade the *AOS*. (Always upgrade the *AOS* before the *App Module*).

   ```
   ftp> bin
   ftp> put apc_hw05_aos_nnn.bin (where nnn is the firmware version
   number)
   ```

7. When FTP confirms the transfer, type `quit` to close the session.
8. After 20 seconds, repeat step 3 through step 7, using the *App Module* file name at step 6.

SCP to Upgrade Battery Manager

To use Secure CoPy (SCP) to upgrade firmware for the Battery Manager, follow these steps (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two though):

1. Locate the firmware modules, see See “Firmware Module Files” on page 110..
2. Use an SCP command line to transfer the AOS firmware module to the Battery Manager. The following example uses *nnn* to represent the version number of the AOS module:

   `scp apc_hw05_aos_`*`nnn`*`.bin apc@158.205.6.185:apc_hw05_aos_`*`nnn`*`.bin`
3. Use a similar SCP command line, with the name of the *App Module*, to transfer the *App Module* firmware to the Battery Manager. (Always upgrade the *AOS* before the *App Module*).

XMODEM to Upgrade Battery Manager

To use XMODEM to upgrade one Battery Manager that is not on the network, you must extract the firmware files with the Firmware Upgrade Utility (see “To extract the firmware files:”).

To transfer the files (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two though):

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect the provided serial configuration cable (part number 940-0103) to the selected port and to the serial port at the Battery Manager.
3. Run a terminal program such as HyperTerminal, and configure the selected port for 57600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press the **Reset** button on the Battery Manager, then immediately press the **Enter** key twice, or until the Boot Monitor prompt displays: `BM>`
5. Type `XMODEM`, then press ENTER.
6. From the terminal program’s menu, select XMODEM, then select the binary AOS firmware file to transfer using XMODEM.
   After the XMODEM transfer is complete, the Boot Monitor prompt returns:

   `(Always upgrade the `*`AOS`*` before the `*`App Module`*`).`
7. To install the *App Module*, repeat step 5 and step 6. In step 6, use the *App Module* file name.
8. Type `reset` or press the **Reset** button to restart the Battery Manager NMC.

Using the Firmware Upgrade Utility for Multiple Upgrades on Windows

After downloading the Upgrade Utility from the Firmware downloads page on the **www.apc.com** website, double click on the .exe file to run the utility and follow these steps to upgrade your Battery Manager NMC firmware:

1. In the utility dialog, type in an IP address, a user name, and a password, and choose the **Ping** button if you need to verify the IP address.
2. Choose the **Device List** button to open the `iplist.txt` file. Here you should type all UPS devices to upgrade with the necessary information: IP, user name, and password.

   Example:

   ```
   SystemIP=192.168.0.1

   SystemUserName=apc

   SystemPassword=apc

   AllowDowngrade=0
   ```

   NOTE: You can use an existing iplist.txt file if it already exists. *AllowDowngrade=1* is also a valid value, in reference to the above example.
3. Select the **Upgrade From Device List** check box to use the `iplist.txt` file.
4. Choose the **Upgrade Now** button to start the firmware version upgrade(s).
5. Make sure to save the file after editing is complete. Choose **View Log** to verify any upgrade.

Verifying Upgrades

Verify the success of the transfer

To verify whether a firmware upgrade succeeded, you can use the `xferStatus` command in the command line interface to view the last transfer result.

Alternatively, you can use an SNMP GET to the *mfiletransferStatusLastTransferResult* OID.

Last Transfer Result codes

Possible transfer errors include the TFTP or FTP server not being found, or the server refusing access, the server not finding or not recognizing the transfer file, or a corrupt transfer file.

Verify the Version Numbers of Installed Firmware

About > Network

Use the Web UI to verify the versions of the upgraded firmware modules. You could also use an SNMP GET to the MIB-2 sysDescr OID. In the command line interface, use the about command.

Troubleshooting

Battery Management System Access Problems

For problems that are not described here, or if the problem still persists, contact **Worldwide Customer Support**.

Problem	Solution
Unable to Ping the Battery Manager	The Battery Manager supports the ability to disable IPv4 Ping Response for security reasons. This setting is located in the web UI under **Configuration > Security > Ping Response** or can be located in config.ini. Check this setting or verify other access methods such as HTTPS, FTP, Telnet, or SSH. If the Battery Manager's Status LED is green, try to ping another node on the same network segment as the Battery Manager. If that fails, it is not a problem with the Battery Manager. If the Status LED is not green, or if the ping test succeeds, perform the following checks: Verify all network connections. Verify the IP addresses of the Battery Manager and the NMS. If the NMS is on a different physical network (or subnetwork) from the Battery Manager, verify the IP address of the default gateway (or router). Verify the number of subnet bits for the Battery Manager's subnet mask.
Cannot Allocate the Communications port through a Terminal Program	Before you can use a terminal program to configure the Battery Manager, you must shut down any application, service, or program using the communications port.
Cannot Access the Command Console through a Serial Connection	Make sure that the correct serial cable (APC part number 940-0103) is connected to the serial port. Make sure that the baud rate is configured correctly. Try 9600 or 19200. Make sure the DIP switch settings are correct. To access the Command Console through a serial connection, the DIP switch #7 must be set to the OFF position.
Cannot access the Command Console remotely	Make sure you are using the correct access method, *Telnet* or Secure SHell (*SSH*). An Administrator can enable these access methods. By default, Telnet is enabled. SSH and Telnet can be enabled/disabled independently. For *SSH*, the Battery Manager may be creating a host key. The Battery Manager takes several minutes to create the host key, and *SSH* is inaccessible during that time.

Problem	Solution
Cannot access the Web Interface	Verify that HTTP or HTTPS access is enabled. Check your browser's proxy settings. Make sure you are specifying the correct URL — one that is consistent with the security system used by the Battery Manager. SSL requires https, not http, at the beginning of the URL. Verify that you can ping the Battery Manager. Verify that you are using a supported Web browser. If available, try a different web browser. See "Supported Web Browsers" on page 61. If the Battery Manager has just restarted and SSL security is being set up, the Battery Manager may be generating a server certificate. The Battery Manager may take up to several minutes to create this certificate, and the SSL server is not available during that time.

SNMP Issues

Problem	Solution
Unable to perform a GET	Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3). Use the Command Console or web interface to ensure that the NMS has access. See "Network Configuration SNMP" on page 83.
Unable to perform a SET	Verify the read/write (SET) community name(SNMPv1) or the user profile configuration (SNMPv3). Use the Command Console or the web interface to ensure that the NMS has write (SET) access (SNMPv1) or is granted access to the target IP address through the access control list (SNMPv3). See "Network Configuration SNMP" on page 83.
Unable to receive traps at the NMS	Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the designated NMS as a trap receiver. For SNMP v1, query the mconfigTrapReceiverTable APC MIB OID 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 either is not correct, use SETs to the mconfigTrapReceiverTable OIDs, or use the Command Console or web interface to correct the trap receiver definition. For SNMPv3, check the user profile configuration for the NMS, and run a trap test. See "Network Configuration SNMP" on page 83, "SNMP Trap Receivers" on page 92," and "Event Actions" on page 88.
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.

Alarms

Environment Alarms

Environmental alarms activate the Environment LED of the Battery Manager.

Critical Alarms		
Alarm	Possible Cause	Corrective Action
High Ambient Temperature	The air temperature in the battery string environment is above the configured threshold. Default high threshold: 95.0°F (35°C)	Check temperature control and ventilation systems in the room, and check for overheated batteries (usually caused by overcharging). **NOTE:** Lead-Acid batteries provide optimum output and longevity at 77°F. An uncorrected high temperature can significantly shorten the life of the battery string.

Warning Alarms		
Alarm	Possible Cause	Corrective Action
Low Ambient Temperature	The air temperature in the battery string environment is below the configured threshold. Default low threshold: 50.0°F (10°C)	Check temperature control and ventilation systems in the room. **NOTE:** Lead-Acid batteries provide optimum output and longevity at 77°F.
Input Contacts	Activation of input contacts triggers an alarm.	Check the status of the external monitoring device that sent the input signal.

Charger Alarms

The **Charger** LED activates when the voltage (VDC) of a battery string enters the alarm state, or when a discharge event occurs.

Alarm	Possible Cause	Corrective Action
High String Voltage	The voltage of a battery string is above the configured threshold. Default high threshold: 2.4 V per cell for lead-acid batteries The string charger may be defective or improperly adjusted. If uncorrected, this condition can cause permanent damage to the batteries.	See “Cell Min Voltage Limit” on page 68 for configuration information. Adjust the DC string-charging voltage to the voltage specified by the battery manufacturer.
Low String Voltage	The voltage of a battery string is below the configured threshold. Default low threshold: 2.15 V per cell for lead-acid batteries	Check for open fuses or connections in the Battery Manager wiring. (An open fuse or connection activates the Management Controller LED.) See “Cell Min Voltage Limit” on page 68 for configuration information.
	If the Management Controller LED is not active, and all battery voltages are present and balanced, the string charger may be defective or improperly adjusted. If uncorrected, this condition can cause permanent damage to the batteries.	Adjust the DC string-charging voltage to the voltage specified by the battery manufacturer.
System On Battery	The charger is not receiving power. The batteries are providing power to the load. **NOTE:** Any negative current flow of over 10 A and 2 seconds causes the Discharge Alarm. However, to initiate a Discharge Test, the Battery Manager requires a sustained 10-A discharge for more than 5 seconds.	Investigate the loss of power to the charger and restore it as soon as possible.
High Ripple Current	The detected ripple current exceeds the alarm threshold. Default high ripple current: 5%	Investigate the source of high AC current in the charger output. A high ripple current may indicate electronic issues with the rectifier, or harmonic and other distortions. To prevent premature battery failure, immediately correct any ripple current greater than 5% of battery ampacity.

Critical Battery Alarms

Alarm	Possible Cause	Corrective Action
Battery Low Capacity	The voltage of individual batteries listed in the alarm text dropped below the configured threshold during the last discharge. Default minimum threshold: 15% **NOTE:** Recorded voltage below the minimum threshold indicates that the battery will not provide adequate system backup, in relation to other batteries in the same string.	Identify the listed batteries immediately so that system backup time is not reduced. Check for external causes of this alarm, such as a loose connection or corrosion on a battery post. If the battery has no external problems, perform a follow-up reading with a battery tester. If a specific battery causes repeated alarms, the battery is failing. Replace the battery.
Charge Current Deviation	When the Battery Manager applied a test current, the batteries listed in the alarm message showed a higher than acceptable percentage of deviation from the benchmarked values. (Benchmark values are set at installation, after a system reset, or after any discharge.) **NOTE:** The charge test detects changes within a battery and its intercell connectors.	Identify the listed batteries immediately so that system backup time is not reduced. Check for external causes of this alarm, such as a loose connection or corrosion on a battery post. If the battery has no external problems, perform a follow-up reading with a battery tester. If a specific battery causes repeated alarms (especially if the alarms have increasing deviation percentages), the battery is failing.
Battery Cell Shorted	The voltage of the indicated battery is below normal, usually by more than the voltage of one cell. The alarm value is calculated using the following formula: ((#Cells/Batt)-1) x (Vstring) (#Cells/Batt) x (#Batt/String) **Example**: A normally float-charged 12-V VRLA battery measures 13.5 V at 2.25 Volts per Cell (VPC). If the voltage falls below 11.25 V (2.25 VPC x 5 cells), but is still above 0.5 V, the battery activates the **Battery Cell Shorted** alarm.	Check the voltage reading of the indicated battery. If the alarm is accurate, replace the battery immediately.

Alarm	Possible Cause	Corrective Action
Battery Low Chemistry Voltage	The voltage of a battery is below the threshold for the battery type.	Identify the listed batteries immediately so that system backup time is not reduced. Check for external causes of this alarm, such as a loose connection or corrosion on a battery post. If the battery has no external problems, perform a follow-up reading with a battery tester. If a specific battery causes repeated alarms (especially if the voltage continues to decrease), the battery is failing. Replace the battery.
Battery High Chemistry Voltage	The voltage of a battery is above the threshold for the battery type.	If a specific battery causes repeated alarms (especially if the voltage continues to increase), the battery is failing. Replace the battery.
Battery Thermal Runaway	The response current is higher than the configured value. Default: 20% higher than the benchmark, or greater than 95°F A thermal runaway occurs when oxygen and hydrogen fail to recombine at the positive plates in the cells of a VRLA battery. Without recombination, the battery cannot maintain the electrolyte level and the cell voltage decreases, causing the charge current to increase.	This alarm indicates that there is potential for a thermal runaway. It does not indicate that a thermal runaway is occurring. Inspect the battery. Closely monitor the battery to ensure that thermal runaway does not occur. If random batteries occasionally generate **Battery Thermal Runaway** alarms, the **Charge Current Deviation From Benchmark** setting may be too close to the normal deviation range of the battery string. To reconfigure this value, see See “Charge Current Deviation From Benchmark” on page 68. If a specific battery causes repeated alarms (especially if the alarms have increasing deviation percentages), the battery is failing. Replace the battery.

Warning Alarms

Alarm	Possible Cause	Corrective Action
Battery Dryout	The response current is lower than the benchmark. Default: 30% lower than the benchmark **NOTE:** This alarm indicates that there is potential for battery dryout. It does not indicate that there is a failed battery in the string.	Inspect the battery. Closely monitor the battery to ensure that battery Dryout does not occur. If random batteries occasionally generate Battery Dryout alarms, the Charge Current Deviation From Benchmark setting may be too close to the normal deviation range of the battery string. To reconfigure this value, see “Charge Current Deviation From Benchmark” If a specific battery causes repeated alarms (especially if the alarms have increasing deviation percentages), the battery is failing. Replace the battery.
Battery High User Defined Voltage	The voltage of a battery is above the configured threshold.	If a specific battery causes repeated alarms (especially if the alarms have increasing deviation percentages), the battery is failing. Replace the battery.
Battery Low User Defined Voltage	The voltage of a battery is below the configured threshold.	Identify the listed batteries immediately so that system backup time is not reduced. Check for external causes of this alarm, such as a loose connection or corrosion on a battery post. If the battery has no external problems, perform a follow-up reading with a battery tester. If a specific battery causes repeated alarms (especially if the alarms have increasing deviation percentages), the battery is failing. Replace the battery.

Management Controller Alarms

Alarm	Possible Cause	Corrective Action
Missing or Defective Sensors	Not all sensors are present and functional. **NOTE:** The system must have at least one current sensor, one ambient temperature sensor, and one pilot battery temperature sensor to operate reliably. Systems with two strings must have two current sensors.	Connect or replace the sensor indicated in the event log.
Monitor Stuck	A relay in a unit is stuck.	Reset the Battery Manager using the On/Off button on the front panel of the unit. If the problem persists, contact Customer Support.
Monitor Suspend (lead-acid batteries only)	The batteries are reporting low voltage levels. **NOTE:** When the Battery Manager detects this alarm, it inhibits relay scanning to decrease current draw and prevent damage to the batteries.	Check that the Battery Manager is receiving power. Check that the charger is functioning correctly.
Unit Communication	One or more units are not reporting to the master unit, or other communication among units failed.	Check that the cables on the expansion ports are in place. If the system has never been operated, check that the DIP switches are set correctly on each unit. If the problem persists, contact Customer Support.
Open Fuse or Open Connection	One or more connections between the Management Controller and the batteries are open. **NOTE:** If the fuse at the end of a battery string opens, only the first or last battery is affected. If an intermediate fuse opens, the two concurrent battery voltage readings are 0 V.	Replace the fuse, wire connection, or battery in the location indicated in the event log.
High Pilot Temperature	The surface temperature of one battery in the string is above the configured threshold. The battery may be overcharged. Default high threshold: 95°F (35°C)	Check the current flow for higher-than-normal float charge. A current flow that is higher than the float charge could indicate a shorted cell, a runaway charger, or the beginning of a thermal runaway. Replace failed batteries.

Worldwide Customer Support

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

- Visit the Schneider Electric Web site to access documents in the Schneider Electric Knowledge Base and to submit customer support requests.
  - **www.schneider-electric.com** (Corporate Headquarters)
    Connect to localized Schneider Electric Web sites for specific countries, each of which provides customer support information.
  - **www.schneider-electric.com/support/**
    Global support searching Schneider Electric Knowledge Base and using e-support.
- Contact the Schneider Electric Customer Support Center by telephone or e-mail.
  - Local, country-specific centers: go to **www.schneider-electric.com > Support > Operations around the world** for contact information.

For information on how to obtain local customer support, contact the representative or other distributors from whom you purchased your product.

Customer support and warranty information is available at **www.apc.com**.