Command Line Interface Guide

UPS Network Management Card 2

AP9630, AP9631, AP9635

990-4879B-001
10/2015

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.

Command Line Interface (CLI)

How To Log On

Overview

To access the command line interface, you can use either a local, serial connection, or a remote connection (Telnet or SSH) with a computer on the same network as the Network Management Card (NMC).

To access the Command Line Interface detailed in this CLI Guide, the NMC must have the Smart-UPS or Single Phase Symmetra firmware installed, and the NMC must be installed in a Smart-UPS or Single Phase Symmetra model UPS. For more information on UPS models compatible with your NMC, see KBase article **FA237786** on the APC support website, **www.apc.com/support**

Use case-sensitive user name and password entries to log on (by default, **apc** and **apc** for a Super User, or **device** and **apc** for a Device User). A Read-Only User cannot access the command line interface.

See the UPS Network Management Card 2 *User Guide* (for AP9630, AP9631, AP9635) for more information on these options.

If you cannot remember your user name or password, see "How to Recover from a Lost Password" in the *User Guide*.

Remote access to the command line interface

You can access the command line interface through Telnet or SSH. Telnet is enabled by default.

To enable or disable these access methods, use the Web interface. On the **Configuration** menu, select **Network** > **Console > Access**.

You can also enable or disable Telnet or SSH access through the command line interface. See "console" on page 10.

Telnet for basic access. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption.

To use Telnet to access the command line interface:

1. From a computer that has access to the network on which the NMC is installed, at a command prompt, type `telnet` and the IP address for the NMC (for example, `telnet 139.225.6.133`, when the NMC uses the default Telnet port of 23), and press ENTER.

   If the NMC uses a non-default port number (from 5000 to 32768), you must include a colon or a space, depending on your Telnet client, between the IP address (or DNS name) and the port number. (These are commands for general usage: some clients don't allow you to specify the port as an argument and some types of Linux might want extra commands).

2. Enter the user name and password (by default, **apc** and **apc** for a Super User, or **device** and **apc** for a Device User).

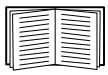
SSH for high-security access. If you use the high security of SSL for the Web interface, use SSH for access to the command line interface. SSH encrypts user names, passwords, and transmitted data. The interface, user accounts, and user access rights are the same whether you access the command line interface through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer. Enabling SSH also enables SCP (SeCure CoPy), for secure file transfer.

Dial-in access to the Command Line Interface (AP9635 only). To use a modem to dial in to the command line interface on the AP9635 NMC:

1. Connect an active telephone cable (RJ-11) to the Modem port on the front panel of the AP9635
2. On a computer connected to a modem, use modem terminal software (e.g. 3rd party terminal emulator programs like HyperTerminal or Tera Term) to dial the telephone number assigned to the cable connected to the AP9635 card.
3. When connected, the modem terminal software opens a command line terminal. When prompted, enter the user name and password (by default, **apc** and **apc** for a Super User, or **device** and **apc** for a Device User).

Configuring the AP9635 NMC modem settings.

The configuration of the AP9635 modem is available only in the Configuration INI file.



For more information on directly editing the Configuration INI file, see "*Retrieving and Exporting the .ini File - Customizing*" in the NMC User's Guide, available on the Network Management Card *Utility* CD and on the APC website, **www.apc.com**.

To configure the modem settings in the Configuration INI file:

1. Open the Configuration INI file in a text editor
2. Locate the section heading `[SystemModem]` and update the following settings:

Option	Argument	Description
ConsoleDialIn	enabled | disabled	Enable this option to allow remote modem dial-in access to the command line interface. Enabled by default.
InitString	[AT command] [& Command] [MNP Command]	The InitString option accepts standard Hayes Protocol options. It is not necessary to edit the InitString. The default is [AT&F0E0].
Country	Text string	Used to specify the country of the dial-in number of the active telephone cable connected to the NMC.
DialBack	enabled | disabled	Enable this to instruct the NMC modem to hang up and dial back a specified number when it receives a dial-in request. DialBack is disabled by default.
DialBackString	Telephone number	If DialBack is enabled, this is the telephone number to dial back when the NMC receives a dial-in request.

Local access to the command line interface

For local access, use a computer that connects to the Network Management Card through the serial port to access the command line interface:

1. Select a serial port at the computer and disable any service that uses the port.
2. Connect the provided serial cable (part number 940-0299) from the selected port on the computer to the console port at the NMC.
3. Run a terminal program (e.g.3rd party terminal emulator programs like HyperTerminal, PuTTY, or Tera Term), and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER. At the prompts, enter your user name and password.

Main Screen

Sample main screen

Following is an example of the screen displayed when you log on to the command line interface at the Network Management Card (NMC).

```
 Schneider Electric                    Network Management Card AOS  vx.x.x
(c)Copyright 2015 All Rights Reserved Symmetra APP                 vx.x.x
-------------------------------------------------------------------------------
Name      : Test Lab                                  Date : 10/30/2015
Contact   : Don Adams                                 Time : 5:58:30
Location  : Building 3                                User : Super User
Up Time   : 0 Days, 21 Hours, 21 Minutes              Stat : P+ N4+ N6+ A+

APC>
```

Information and status fields

Main screen information fields.

- Two fields identify the American Power Conversion operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the device that connects to the network through this NMC. In the example above, the NMC uses the application firmware for a Symmetra UPS.

  ```
  Network Management Card AOS    vx.x.x
  Symmetra APP                   vx.x.x
  ```

- Three fields identify the system name, contact person, and location of the NMC.

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

- The **Up Time** field reports how long the NMC has been running since it was last turned on or reset.

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

- Two fields report when you logged in, by date and time.

  ```
  Date : 10/30/2015
  Time : 5:58:30
  ```

- The **User** field reports whether you logged in through the **Super User** or **Device Manager** account. (The **Read Only User** account cannot access the command line interface.)
  When you log on as Device Manager (equivalent to Device User in the user interface), you can access the event log, configure some UPS settings, and view the number of active alarms.

  ```
  User : Super User
  ```

Main screen status fields.

- The **Stat** field reports the NMC status. The middle status varies according to whether you are running IPv4, IPv6, or both, as indicated in the second table below.

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

P+	The operating system (AOS) is functioning properly.

IPv4 only	IPv6 only	IPv4 and IPv6*	Description
N+	N6+	N4+ N6+	The network is functioning properly.
N?	N6?	N4? N6?	A BOOTP request cycle is in progress.
N–	N6–	N4– N6–	The NMC did not connect to the network.
N!	N6!	N4! N6!	Another device is using the IP address of the NMC.

* The N4 and N6 values can be different from one another: you could, for example, have N4– N6+.

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.

If P+ is not displayed, see customer support at **http://www.apc.com/site/support/**.

How to Use the Command Line Interface

Overview

The command line interface provides options to configure the network settings and manage the UPS and its Network Management Card (NMC).

How to enter commands

At the command line interface, use commands to configure the NMC. To use a command, type the command and press ENTER. Commands and arguments are valid in lowercase, uppercase, or mixed case. Options are case-sensitive.

While using the command line interface, you can also do the following:

- Type `?` and press ENTER to view a list of available commands, based on your account type.

  To obtain information about the purpose and syntax of a specified command, type the command, a space, and `?` or the word `help`. For example, to view RADIUS configuration options, type:
  `radius ?`
  or
  `radius help`
- Press the UP arrow key to view the command that was entered most recently in the session. Use the UP and DOWN arrow keys to scroll through a list of up to ten previous commands.
- Type at least one letter of a command and press the TAB key to scroll through a list of valid commands that match the text you typed in the command line.
- Type `ups -st` to view the status of the UPS.
- Type `exit` or `quit` to close the connection to the command line interface.

Command syntax

Item	Description
-	Options are preceded by a hyphen.
< >	The definitions of options are enclosed in angle brackets. For example: `-pw <user password>`
[ ]	If a command accepts multiple options or an option accepts mutually exclusive arguments, the values may be enclosed in brackets.
|	A vertical line between items enclosed in brackets or angle brackets indicates that the items are mutually exclusive. You must use one of the items.

Syntax examples

A command that supports multiple options:

```
user -n <user name> -pw <user password>
```

Here, the `user` command accepts both the option `-n`, which specifies the user name, and the option `-pw`, which changes the password.

For example, to change a password to XYZ:

```
user -n apc -pw XYZ
```

Note that Super User also requires the current password, see the "user" section.

A command that accepts mutually exclusive arguments for an option:

```
alarmcount -p [all | warning | critical]
```

In this example, the option `-p` accepts only three arguments: `all`, `warning`, or `critical`. For example, to view the number of active critical alarms, type:

```
alarmcount -p critical
```

The command will not work if you type an argument that is not specified.

Command Response Codes

The command response codes enable scripted operations to detect error conditions reliably without having to match error message text.

The CLI reports all command operations with the following format:

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

Code	Error message
E000	Success
E001	Successfully Issued
E002	Reboot required for change to take effect
E100	Command failed
E101	Command not found
E102	Parameter Error
E103	Command Line Error
E104	User Level Denial
E105	Command Prefill
E106	Data Not Available
E107	Serial communication with the UPS has been lost

Command Descriptions

The availability of the commands and options below can vary between UPS devices.

?

Access: Super User, Administrator, Device 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.

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

about

Access: Super User, Administrator, Device User

Description: View hardware and firmware information. This information is useful in troubleshooting and enables you to determine if updated firmware is available at the website.

alarmcount

Access: Super User, Administrator, Device User

Description:

Option	Arguments	Description
-p	all	View the number of active alarms reported by the NMC. 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:
`alarmcount -p warning`

boot

Access: Super User, Administrator

Description: Define how the NMC will obtain its network settings, including the IP address, subnet mask, and default gateway. Then configure the BOOTP or DHCP server settings.

Option	Argument	Description
-b <boot mode>	dhcp | bootp | manual	Define how the TCP/IP settings will be configured when the NMC turns on, resets, or restarts.
-c	enable | disable	`dhcp` boot modes only. Enable or disable the requirement that the DHCP server provide the APC cookie.

Option	Argument	Description
		The default values for these three settings generally do not need to be changed: -v <vendor class>: 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: To use a DHCP server to obtain network settings:

1. Type `boot -b dhcp`
2. Enable the requirement that the DHCP server provide the APC cookie:
   `boot -c enable`

bye

Access: Super User, Administrator, Device User

Description: Exit from the command line interface session.This works the same as the exit or quit commands.

Example 1:

```
bye
Connection Closed - Bye
```

cd

Access: Super User, Administrator, Device User

Description: Navigate to a folder in the directory structure of the NMC.

Example 1: To change to the `ssh` folder and confirm that an SSH security certificate was uploaded to the NMC:

1. Type `cd ssh` and press ENTER.
2. Type `dir` and press ENTER to list the files stored in the SSH folder.

Example 2: To return to the previous directory folder, type:
`cd ..`

cfgshutdn

Access: Super User, Administrator, Device User

Description: Configure the shutdown parameters: this enables you to show and configure UPS Shutdown Delay, UPS Return Delay, UPS Low Battery Duration, UPS Sleep Time, UPS Minimum Battery Charge, and UPS Min Return Runtime.

These options are not available with all UPS devices.

Option	Argument	Description
-all		Show all applicable shutdown parameters for this UPS.
-sd	000 | 090 | 180 | 270 | 360 | 450 | 540 | 630	Set the shutdown delay in seconds.

Option	Argument	Description
-lo	02 | 05 | 08 | 11 | 14 | 17 | 20 | 23	Set the low battery duration in minutes.
-rd	000 | 060 | 120 | 180 | 240 | 300 | 360 | 420	Set the UPS return delay in seconds, that is, the delay time before the UPS turns on again.
-rrt	0–3600	Set the minimum return runtime in seconds, that is, the battery runtime to support the load must reach this value before the UPS turns on again.
-sl	0.0–359.9	Set the sleep time, in hours. The argument can have any number between 0.0 and 359.9.
-rsc	00 | 15 | 30 | 45 | 60 | 75 | 90	Set the minimum battery charge, as a percentage of the total capacity.

Example:

```
cfgshutdn -all
E000: Success
Low Battery Duration: 4 min
Sleep Time: 0.0 hr
```

cfgpower

Access: Super User, Administrator, Device User

Description: Configure the power parameters: this enables you to show and configure transfer points, sensitivity and output voltage.

These options are not available with all UPS devices.

Option	Argument These values can vary with different devices.	Description
-all		Show all applicable power parameters for this UPS.
-l	97–106	Set the low transfer point, in VAC.
-h	127–136	Set the high transfer point, in VAC.
-ov	100 | 120 | 110 |	Set the outlet voltage, in VAC.
-s	Normal | Reduced | Low	Set the sensitivity, using one of the three arguments.
-bu	127 | 130 | 133 | 136 | 139 | 142 | 145 | 148	Set the bypass upper voltage in VAC; when the voltage rises above this value, the device goes into bypass.
-bl	086 | 088 | 090 | 092 | 094 | 096 | 098 | 100	Set the bypass lower voltage in VAC; when the voltage drops below this value, the device goes into bypass.

Example:

```
cfgpower -all
E000: Success
Low Transfer Voltage: 106 VAC
High Transfer Voltage: 127 VAC
Sensitivity: Normal
```

clrrst

Access: Super User, Administrator

Definition: Clear the network interface reset reason. See “lastrst” on page 17.

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.

Option	Argument	Description
-s	enable | disable	Enable or disable SSH. Enabling SSH enables SCP and disables Telnet.
-t	enable | disable	Enable or disable Telnet.
-pt	<telnet port number>	Specify the Telnet port number used to communicate with the NMC (23 by default). The other range is 5000–32768.
-ps	<SSH port number>	Specify the SSH port number used to communicate with the NMC (22 by default). The other range is 5000–32768
-b	2400 | 9600 | 19200 | 38400	Configure the serial baud rate (9600 by default).

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

```
console -s
```

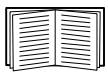
Example 2: To change the Telnet port to 5000, type:

```
console -pt 5000
```

date

Access: Super User, Administrator

Definition: Configure the date used by the NMC.



To configure an NTP server to define the date and time for the NMC, see the *User's Guide*.

Option	Argument	Description
-d	<“datestring”>	Set the current date. Use the date format specified by the `date -f` command.

Option	Argument	Description
-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 October 30, 2009, using the format configured in the preceding example, type:

```
date -d "2009-10-30"
```

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

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

delete

Access: Super User, Administrator

Description: Delete a file in the file system. (To delete the event log, see the *User's Guide*).

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

Example: To delete a file:

1. Navigate to the folder that contains the file. For example, to navigate to the `logs` folder, type:
   ```
   cd logs
   ```
2. To view the files in the `logs` folder, type:
   ```
   dir
   ```
3. Type
   ```
   delete <file name>
   ```

detbat

Access: Super User, Administrator, Device User

Description: View detailed UPS battery information.

Option	Arguments	Description
-all	<#>	Show all battery information.
-f	<#>	Pack firmware revisions.
-t	<#>	Pack temperatures.
-pe	<#>	Pack battery status.

Option	Arguments	Description
-s	<#> <#>	Pack or cartridge health.
-rd	<#> <#>	Pack or cartridge recommended replace battery dates.
-id	<#> <#> <"datestring">	Pack or cartridge battery install date in current date format.
-ce	<#> <#>	Pack or cartridge battery status.

Example: `detbat -all`

```
E000: Success
Firmware Revision (IP): BMC 12.5
Temperature (IP): 26.00C
Pack Status (IP): No Errors
Health (IP, C1): Battery Life OK
Predicted Replacement Date (IP, C1): 07/02/2019
Installation Date (IP, C1): 02/12/2015
Status (IP, C1): OK
```

detstatus

Access: Super User, Administrator, Device User

Description: View the detailed status of the UPS. See also the -st option in “ups” on page 27.

Option	Arguments	Description
-all		Show all applicable status information for this UPS.
-rt		Runtime remaining, in hours and minutes.
-ss		UPS status summary: on line, on battery, etc.
-soc		UPS battery charge, as a percentage of the total capacity.
-om		Output measurements: voltage, frequency, watts percentage, VA percentage, current.
-im		Input measurements: voltage and frequency.
-bat		Battery voltage
-tmp		Internal temperature of the UPS
-dg		Diagnostic test results: self-test result and date, calibration result and date.

Example:

```
detstatus -rt
E000: Success
Runtime Remaining: 9 hr 22 min 30 sec
```

dir

Access: Super User, Administrator, Device User

Description: View the files and folders stored on the NMC.

dns

Access: Super User, Administrator

Description: Configure and display the manual Domain Name System (DNS) settings.

Option	Argument	Description
-OM	enable | disable	Override the manual DNS.
-y	enable | disable	Synchronizes the system and the hostname. This is the same as using "system -s".
-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 hostname.

Example:

```
dns -OM
E000: Success
Override Manual DNS Settings:   enabled
```

email

Access: Super User, Administrator, Network Only User

Description: Use the following commands to configure parameters for email, used by the NMC to send event notification.

Option	Argument	Description
-g[n]	<enable | disable>	Enables (default) or disables sending email to the recipient.
-t[n]	<To Address>	The e-mail address of the recipient.
-o[n]	<long | short> (Format)	The long format contains name, location, contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.
-l[n]	<Language Code>	The language in which the e-mails will be sent. This is dependent on the installed language pack.

Option	Argument	Description
-r [n]	<Local | recipient | custom> (Route)	Set the SMTP Server options: • **Local** (recommended): This setting uses the locally configured SMTP server. Choose this setting to limit delays and network outages. If you choose this setting, you must also enable forwarding at the SMTP server of the device, and set up a special external e-mail account to receive the forwarded e-mail. **Note:** Check with your SMTP server administrator before making these changes. • **Recipient**: This setting sends email directly to the recipient's SMTP server, which is determined by an MX record lookup of the domain of the To: Address. The device tries only once to send the e-mail. A network outage or a busy remote SMTP server can cause a time-out and cause the e-mail to be lost. This setting requires no additional administrative tasks on the SMTP server. • **Custom**: This setting allows each email recipient to have its own server settings. These settings are independent of the settings given by option -s[n].
-f[n]	<From Address>	The sender email address used by the NMC in the **From:** field of the email sent.
-s[n]	<SMTP Server>	The IPv4/IPv6 address or DNS name of the local SMTP server. Use this when option -r[n] is set to Local.
-p[n]	<Port>	The SMTP port number, with a default of 25. Alternative ports: 465, 587, 2525, 5000 to 32768.
-a[n]	<enable | disable> (Authentication)	Enable if the SMTP server requires authentication.
-u[n]	<User Name>	If your mail server requires authentication, type your user name and password here.
-w[n]	<Password>	
-e[n]	<none | ifsupported | always | implicit> (Encryption)	• **None**: 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 the advertisement is given. • **Always**: The SMTP server requires the STARTTLS command to be sent on connection to it. • **Implicit**: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.
-c[n]	<enable | disable > (Required 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 onto the NMC for encrypted e-mails to be sent.
-i[n]	<Certificate File Name>	This field is dependent on the root CA certificates installed on the NMC and whether or not a root CA certificate is required. The file must have an extension of .crt or .cer.
n=	Email Recipient Number (1,2,3, or 4)	Specifies the recipient of the e-mail, identified by the recipient number.

Example: To enable email to be sent to email recipient 1 with email address recipient1@apc.com, from address sender@apc.com, using the local SMTP server:

```
email -g1 enable -r1 local -t1 recipient1@apc.com -f1 sender@apc.com
E000: Success
```

energyWise

Access: Super User, Administrator, Device User

Description: These options facilitate the use of a Cisco EnergyWise switch to monitor and control your UPS and its devices. This includes turning off the UPS and individual Switched Outlets (if your UPS has them).

Option	Argument	Definition
-e	enable | disable	Enable or disable EnergyWise.
-p	<Port>	Specify a port number, between 1- 65535.
-d	<Domain>	Specify a domain
-m	enable | disable	Enable or disable secure mode.
-s	<Shared Secret>	Specify the shared secret.
-v		Specify the toolkit version.
-n [outlet group #]	<Name>	For an outlet group, specify the name, the role, any keywords. Specify 0 for the outlet group number for a Parent.
-r [outlet group #]	<Role>	
-k [outlet group #]	<Keywords>	
-i [outlet group #]	<1-100>	Indicate the importance for this outlet #. Specify 0 for the outlet # for a Parent.

Example:

To enable secure-mode EnergyWise, type:

```
energyWise -m enable
```

eventlog

Access: Super User, Administrator, Device User

Description: View the date and time you retrieved the event log, the status of the UPS, and the status of sensors connected to the NMC. 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.

Key	Description
D	Delete the event log. Follow the prompts to confirm or deny the deletion. Deleted events cannot be retrieved.

exit

Access: Super User, Administrator, Device User

Description: Exit from the command line interface session.

firewall

Access: Super User, Administrator

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

Option	Argument	Definition
-S	<enable | disable>	Enable or disable the firewall.
-f	<file name to activate>	Name of the firewall policy file to activate.
-t	<file name to test>	Name of the firewall to test, and duration time in minutes.
-fe		Shows a list of active file errors.
-te		Shows a list of test file errors.
-c		Cancel a firewall test.
-r		Shows a list of active firewall rules.
-l		Shows a firewall activity log.

Example: To enable firewall policy file example.fwl, enter the following:

```
firewall -f example.fwl
E000: Success
```

format

Access: Super User, Administrator

Description: Reformat the file system of the NMC and erase all security certificates, encryption keys, configuration settings, and the event and data logs. Be careful with this command.

To reset the NMC to its default configuration, use the `resetToDef` command instead.

ftp

Access: Super User, Administrator

Description: Enable or disable access to the FTP server. Optionally, change the port setting to the number of any unused port from 5001 to 32768 for added security.

Option	Argument	Definition
-p	<port number>	Define the TCP/IP port that the FTP server uses to communicate with the NMC (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:

```
ftp -p 5001
```

help

Access: Super User, Administrator, Device 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 someone logged on as a Device User, type:

```
help
```

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

```
alarmcount help
```

lang

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

Description: Language in Use

Example:

```
lang
Languages
enUS - English
```

lastrst

Access: Super User, Administrator

Description: Last network interface reset reason. Use the output of this command to troubleshoot network interface issues with the guidance of technical support.

Example: `lastrst`

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

ledblink

Access: Super User, Administrator

Description: Sets the status LED of the NMC to blink for the specified amount of time. Use this command to help visually locate the NMC.

Parameters: Time in minutes

Example: `ledblink 2`

```
E000: Success
```

logzip

Access: Super User, Administrator

Description: Places large logs into a zip file before sending to a configured email recipient, or before exporting from the NMC.

Option	Argument	Definition
-m	<email recipient> (email recipient number (1-4)	The identifying number of the email recipient to which the zip file will be sent. Enter the number of one of the four possible email recipients configured.

Example: `logzip -m 1`

```
Generating files
Compressing files into /dbg/debug_ZA150.tar
Emailing log files to email recipient - 1
E000: Success
```

modbus

Access: Super User, Administrator, Device User

Description: View and configure the Modbus parameters.

Option	Argument	Definition
-a	<enable | disable> (Modbus status)	Enable or disable Modbus Serial. [1]
-br	<9600 | 19200> (baud rate)	Set the baud rate in bits per second. [1]
-pr	event | odd | none	Set the parity bit. [1]
-s	<1-F7> (slave address in hex)	Set the hexidecimal Modbus slave address. [1]
-rDef		Reset the Modbus configuration to defaults.
-tE	<enable | disable> (Modbus TCP status)	Enable or disable Modbus TCP.[2]

Option	Argument	Definition
-tP		Specify the Modbus TCP port number. The default port number is 502, and can be set to a value between 5000 and 32768[2].
[1]Modbus Serial is supported on the AP9635 card only. [2]Modbus TCP is supported on the AP9630, AP9631 and AP9635 cards.		

Example: `modbus`

```
E000: Success
Slave Address = 0x1
Status = ENABLED
Baud Rate = 9600
Parity = none
TCP Status = ENABLED
TCP Port Number = 502
```

netstat

Access: Super User, Administrator, Device User

Description: View the status of the network and all active IPv4 and IPv6 addresses.

ntp

Access: Super User, Administrator, Device User

Description: View and configure the Network Time Protocol parameters.

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.
-e	enable | disable	Enables or disables the use of NTP.
-u	<update now>	Immediately updates the NMC time from the NTP 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
```

ping

Access: Super User, Administrator, Device User

Description. Determine whether the device with the IP address or DNS name you specify is connected to the network. Four inquiries are sent to the address.

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: To determine whether a device with an IP address of 150.250.6.10 is connected to the network, type:

```
ping 150.250.6.10
```

portspeed

Access: Super User, Administrator

Description:

Option	Arguments	Description
-s	auto | 10H | 10F | 100H | 100F	Define the communication speed of the Ethernet port. The `auto` command enables the Ethernet devices to negotiate to transmit at the highest possible speed.

Example: To configure the TCP/IP port to communicate using 100 Mbps with half-duplex communication (communication in only one direction at a time), type:

```
portspeed -s 100H
```

prompt

Access: Super User, Administrator, Device User

Description: Configure the command line interface prompt to include or exclude the account type of the currently logged-in user. Any user can change this setting; all user accounts will be updated to use the new setting.

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: To include the account type of the currently logged-in user in the command prompt, type:

```
prompt -s long
```

pwd

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

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

quit

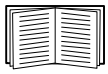
Access: Super User, Administrator, Device User

Description: Exit from the command line interface session (this works the same as the exit and bye commands).

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.



For a summary of RADIUS server configuration and a list of supported RADIUS servers, see the *User's Guide*.

Additional authentication parameters for RADIUS servers are available at the user interface of the NMC.

For detailed information about configuring your RADIUS server, see the *Security Handbook*, available on the Network Management Card *Utility* CD and at the website, **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 does not 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 NMC supports ports 1812, 5000 to 32768.
-s1 -s2	<server secret>	The shared secret between the primary or secondary RADIUS server and the NMC.
-t1 -t2	<server timeout>	The time in seconds that the NMC waits for a response from the primary or secondary RADIUS server.

Example 1:

To view the existing RADIUS settings for the NMC, 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
```

reboot

Access: Super User, Administrator

Description: Restart the network management interface of the NMC.

resetToDef

Access: Super User, Administrator

Description: Reset all configurable parameters to their defaults.

Option	Arguments	Description
-p	all | keepip	Caution: This resets all configurable parameters to their defaults. Reset all configuration changes, including event actions, device settings, and, optionally, TCP/IP configuration settings. Choose keepip to retain the settings that determine how the NMC obtains its TCP/IP configuration values, which by default is DHCP.

Certain non-configurable parameters are not reset using resetToDef, and can only be erased from the NMC by formatting the file system using the **format** command.

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

```
resetToDef -p keepip
```

session

Access: Super User, Administrator

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

Option	Arguments	Description
-d	<session ID> (Delete)	Delete the session for the current user with the specified session ID.
-m	<enable | disable> (Multi-User Enable)	Enable to allow two or more users to log on at the same time. Disable to allow only one user to log in at a time.
-a	<enable | disable> (Remote Authentication Override)	The NMC supports RADIUS storage of passwords on a server. Enable Remote Authentication Override to allow a local user to log on using a username and password for the NMC that is stored locally on the NMC.

Example:

```
User        Interface         Address      Logged In Time    ID
-------------------------------------------------------------------------
apc         Serial                         00:00:05          1
```

smtp

Access: Super User, Administrator

Description: Internet standard protocol for electronic mail.

Option	Arguments	Description
-f	<From Address>	The address from which e-mail will be sent by the NMC.
-s	<SMTP Server>	The IPv4/IPv6 address or DNS name of the local SMTP server.

Option	Arguments	Description
-p	<Port>	The SMTP port number, default is 25. Port options are 25, 465,587,2525, 5000 to 32768
-a	<enable | disable>	Enable this if your SMTP server requires authentication.
-u	<User Name>	If the SMTP server requires authentication, type the user name and password here.
-w	<Password>	
-e	<none | ifavail | always | implicit>	Encryption options: • **none**: The SMTP server does not require/support encryption • **ifavail**: The SMTP server advertises support for STARTTLS but does not require the connection to be encrypted. • **always**: The SMTP server requires the STARTTLS command to be sent upon connection to the server. • **implicit**: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.
-c	<enable | disable>	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 onto the NMC for encrypted e-mails to be sent.
-i	<Certificate File Name>	This field is dependent on the root CA certificates installed on the NMC and whether or not a root CA certificate is required.

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>
```

snmp

Access: Super User, Administrator

Description: Enable or disable and configure SNMPv1.

In the table below, n is the access control number: 1,2,3, or 4.

Option	Arguments	Description
-S	enable | disable	Enable or disable SNMPv1.
-c[n]	Community	Specify a community name or string.

Option	Arguments	Description
-a[n]	read | write | writeplus | disable	Indicate the usage rights.
-n[n]	IP or Domain Name	Specify the IPv4/IPv6 address or the domain name of the Network Management Station.

Example: To enable SNMP version 1, type:

```
snmp -S enable
```

snmpv3

Access: Super User, Administrator

Description: Enable or disable and configure SNMPv3.

In the table below, n is the access control number: 1,2,3, or 4.

Option	Arguments	Description
-S	enable | disable	Enable or disable SNMPv3.
-u[n]	<User Name>	Specify a user name, an authentication phrase and encryption phrase.
-a[n]	<Authentication Phrase>	
-c[n]	<Crypt Phrase>	
-ap[n]	sha | md5 | none	Indicate the type of authentication protocol.
-pp[n]	aes | des | none	Indicate the privacy protocol.
-ac[n]	enable | disable	Enable or disable access.
-au[n]	<User Profile Name>	Give access to a specified user profile.
-n[n]	<IP or hostname for NMS>	Specify the IPv4/IPv6 address or the hostname for the Network Management Station.

Example: To give access level 2 to user “JMurphy”, type:

```
snmpv3 -au2 "JMurphy"
```

snmptrap

Access: Super User, Administrator, Network Only User

Description: Enable or disable SNMP trap generation.

Option	Arguments	Description
-c[n]	<Community>	Specify a community name or string.
-r[n]	<Receiver NMS IP>	The IPv4/IPv6 address or host name of the trap receiver.

Option	Arguments	Description
-l[n]	<Language> [language code]	Specify a language. A language pack containing the desired language must be installed, and the language codes are: • en - English (default) • de - German • ru - Russian • zh - Chinese • ja - Japanese
-t[n]	<Trap Type> [snmpV1 | snmpV3]	Specify SNMPv1 or SNMPv3.
-g[n]	<Generation> [enable | disable]	Enable or disable trap generation for this trap receiver. Enabled by default.
-a[n]	<Auth Traps> [enable | disable]	Enable or disable authentication of traps for this trap receiver, SNMPv1 only.
-u[n]	<profile1 | profile2 | profile3 | profile4> (User Name)	Select the identifier of the user profile for this trap receiver, SNMPv3 only.
n= Trap receiver number = 1, 2, 3, 4, 5 or 6		

Example: To enable and configure an SNMPv1 trap for Receiver 1, with the default Community Name of public, receiver 1 IP address of `10.169.118.100, using the default English language, enter the following command:`

```
snmptrap -c1 public -r1 10.169.118.100 -l1 en -t1 snmpV1 -g1 enable
E000: Success
```

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 “Main screen status fields”).

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: If you define a value with more than one word, you must enclose the value in quotation marks. These values are also used by StruxureWare Data Center Expert and the NMC’s SNMP agent.
-c	<system contact>	
-l	<system location>	
-m	<system-message>	Show a custom message on the logon page of the web UI or the CLI.
-s	enable | disable	Synchronize the system and the hostname. This is the same as using “dns -y”.

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

```
system -l "Test Lab"
```

Example 2: To set the system name as `Don Adams`, type:

```
system -n "Don Adams"
```

tcpip

Access: Super User, Administrator

Description: View and manually configure these IPv4 TCP/IP settings for the NMC:

Option	Argument	Description
-S	enable | disable	Enable or disable TCP/IP.
-i	<IP address>	Type the IP address of the NMC, using the format *xxx.xxx.xxx.xxx*
-s	<subnet mask>	Type the subnet mask for the NMC.
-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 NMC will use.

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

Example 2: To manually configure an IP address of `150.250.6.10` for the NMC, type:
`tcpip -i 150.250.6.10`

tcpip6

Access: Super User, Administrator

Description: Enable IPv6 and view and manually configure these IPv6 TCP/IP settings for the NMC:

Option	Argument	Description
-S	enable | disable	Enable or disable IPv6.
-man	enable | disable	Enable manual addressing for the IPv6 address of the NMC.
-auto	enable | disable	Enable the NMC to automatically configure the IPv6 address.
-i	<IPv6 address>	Set the IPv6 address of the NMC.
-g	<IPv6 gateway>	Set the IPv6 address of the default gateway.
-d6	router | statefull | stateless | 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 NMC, type `tcpip6` and press ENTER.

Example 2: To manually configure an IPv6 address of 2001:0:0:0:0:FFD3:0:57ab for the NMC, type:
`tcpip -i 2001:0:0:0:0:FFD3:0:57ab`

uio

Access: Super User, Administrator, Device User

Description: This command is available for an AP9631 or AP9635 Network Management Card 2 with a connected Dry Contact I/O Accessory (AP9810).

Option	Argument	Description
-rc <UIO port #>	open | close	Change the state of a connected output, and specify the UIO (universal input/ output) port number.
-st	<UIO port #> | <UIO port #>, <UIO port #> | <UIO port #>–<UIO port #>	View the status of the sensors connected to the Dry Contact I/O Accessory. To view the status of a specific sensor or several sensors, type their UIO port numbers.
-disc	<UIO port #> | <UIO port #>, <UIO port #> | <UIO port #>–<UIO port #>	Identify new input contact or output relay connections.

Example 1: To open the output, type:

```
uio -rc 2 open
```

Example 2: To view the status of the devices connected to a Dry Contact I/O Accessory that is installed in universal input/ output port 2, type:

```
uio -st 2
```

ups

Some **ups** options are dependant on the UPS model. Not all configurations may support all options of the **ups** command.

Access: Super User, Administrator, Device User

Description: Control the UPS and view status information. See the *User's Guide* for information on how these options relate to that screen.

Option	Arguments	Description
-c	off | graceoff | on | reboot | gracereboot | sleep | gracesleep	Configure UPS actions.
-r	start | stop	Initiate or end a runtime calibration. A calibration recalculates remaining runtime and requires the following: • Because a calibration temporarily depletes the UPS batteries, you can perform a calibration only if battery capacity is at 100%. • The load must be at least 15% to guarantee that a calibration will be accepted.
-s	start	Initiate a UPS self-test.
-b	enter | exit	Control the use of bypass mode. This command is model-specific and may not apply to your UPS.

Option	Arguments	Description
-o#	Off | DelayOff | On | DelayOn | Reboot | DelayReboot| Shutdown | DelayShutdown | Cancel	Control any of three outlet groups at a Smart-UPS XLM. Specify the outlet group with #. When the state of the outlet group is **on**, the option accepts three arguments: • `Off` — Turn off the group immediately. • `DelayOff` — Turn off the group after the number of seconds configured as **Power Off Delay**. • `Reboot` — Turn off the group immediately, then turn it on after the number of seconds configured as **Reboot Duration** and **Power On Delay**. • `DelayReboot` — Turn the outlet group off after the number of seconds configured as **Power Off Delay**, then turn it on after the number of seconds configured as **Reboot Duration** and **Power On Delay**. • `Shutdown` — If the UPS is online, this reboots the outlet group. If the UPS is on battery, this shuts down the group and waits for AC utility power before turning on the group again. • `DelayShutdown` — Shut down the outlet group after the number of seconds configured as **Power Off Delay**. • `Cancel` — Cancel your previous commands, e.g. turning off. When the state of the outlet group is **off**, the option accepts two arguments: • `On` — Turn on the group immediately. • `DelayOn` — Turn on the group after the number of seconds configured as **Power On Delay**. The **Power On Delay**, **Power Off Delay**, and **Reboot Duration** must be configured at the user interface.
-os#		View the status (on, off, or rebooting) of all the outlet groups. To view the status of a specific outlet group, specify its number. For example, type `ups-os1` to view the status of outlet group 1. But: a) When you use this option on a UPS with a Main Outlet Group: 1 identifies the Main Outlet Group, 2 identifies Switched Outlet Group 1, 3 identifies Switched Group 2, etc. b) On a UPS with NO main outlet group: 1 identifies Switched Outlet Group 1, etc.
-st		View the status of the UPS.
-a	start	Test the UPS audible alarm.

The ups command options for MGE Galaxy-specific UPS devices:

These commands are only available on the MGE Galaxy 300 and MGE Galaxy 7000 UPS. Some options may only be available based on the individual UPS model.

Option	Argument	Description
-input	<phase#> | all	Display the input measurements for the chosen phase of the UPS. Typing "all" displays the information for all phases of the UPS.
	voltage | current | frequency | all	Specify the input measurement for the `ups` command. **Example:** `ups -input 2 frequency` Displays the frequency for phase 2 of the UPS.
-bypass	<phase#> | all	Display the input measurements for the chosen phase of the bypass main. Typing "`all`" displays all phases of the bypass main.
	voltage | current | frequency | all	Specify the input measurement for the `ups` command. **Example:** `ups -bypass 2 current` Displays the current for phase 2 of the bypass main.
-output	<phase#> | all	Display the output measurements for the chosen phase of the UPS. Typing "all" displays the information for all phases of the UPS.
	voltage | current | load | power | percload | pf | frequency | all	Specify the output measurement for the ups command. **Example:** `ups -output 2 percload` Displays the percentage of load for phase 2 of the UPS.
-batt		Display the battery status of the UPS
-about		Displays information about the UPS.
-al	c | w	Display all existing alarms. Specifying "c" or "w" limits the display to either Critical (c) or Warning (w) alarms.

Example 1: To initiate a runtime calibration, type:

```
ups -r start
```

Example 2: To immediately turn off outlet group 2 at a Smart-UPS XLM, type:

```
ups -o2 off
```

upsabout

All UPS information listed by the **upsabout** command might not be available for all UPS devices.

Access. Super User, Administrator, Device User.

Description: Displays information about the UPS including:

Model, SKU, Serial Number, UPS Firmware Revision, Manufacture Date, Apparent Power Rating, Real Power Rating, Internal Battery SKU and External Battery SKU.

upsfwupdate

This command might not be available for all UPS devices.

Access. Super User, Administrator, Device User.

Description: Initiate an update of the UPS firmware. The firmware update file must have been previously sent using FTP to the NMC and stored in the /upsfw/ directory.

Option	Argument	Description
-status		Check the status of a firmware update that is already initiated.
-lastresult		View the result of the last attempted firmware update.

Example: `upsfwupdate -status`

```
E000: Success
Status: 3k/257k (1%)
```

user

Access: Super User, Administrator

Description: Configure the user name and password for each account type, and configure the inactivity timeout. (You can't edit a user name, you must delete and then create a new user).

For information on the permissions granted to each account type (Super User, Administrator, Device User, Read-Only, Network-only), see the *User's Guide*.

Option	Argument	Description
-n	<user>	Indicate the user.
-cp	<current password>	For a Super User, you must specify the current password.
-pw	<user password>	Specify these options for a user.
-pe	<user permission>	
-d	<user description>	
-e	enable | disable	Enable overall access.
-te	enable | disable	Enable touch screen access.
-tp	<touch screen access pin>	Not yet available.
-tr	enable | disable	Enable the touch screen remote authorization override. If you enable this override, the NMC will allow a local user to log on using the password for the NMC that is stored locally on the NMC.
-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.

Option	Argument	Description
-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 1: To change the log off time to 10 minutes for user “JMurphy”, type:

```
user -n “JMurphy” -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.

Option	Argument	Definition
-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.

Option	Argument	Definition
-lf	<tab | csv> (Export Log Format)	Specify the log export format, tab or CSV.
-ts	<us | metric> (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 | yyyymm-dd> (Date Format)	Specify the user's preferred date format.
-lg	<language code (enUs, etc)>	Specify the user's preferred language.
-sp	<enable | disable>	Enable/disable strong password.
-pp	<interval in days>	Required password change interval.

Example. To set the default user's session timeout to 60 minutes:

```
userdflt -st 60
E000: Success
```

web

Access: Super User, Administrator

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

For additional security, you can change the port setting for HTTP and HTTPS to any unused port from 5000 – 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:

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

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 NMC (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 NMC (443 by default). The other available range is 5000–32768.

Example: To prevent all access to the user interface for HTTPS, type:

```
web -s disable
```

whoami

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

Description: Provides login information on the current user

Example:

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

xferINI

Access: Super User, Administrator. This command only works through serial/local console CLI.

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 NMC, you must reset the baud rate to the default to re-establish communication with the NMC.

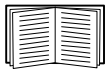
xferStatus

Access: Super User, Administrator

Description: View the result of the last file transfer.

Example: `xferStatus`

```
E000: Success
Result of last file transfer: OK
```



See the *User's Guide* for descriptions of the transfer result codes.

APC Worldwide Customer Support

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

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

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