Command Line Interface Guide

Network Management Card for Easy UPS, 1-Phase & 3-Phase

AP9544, AP9547

990-91547F-001
02/2026

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).

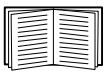
To access the Command Line Interface detailed in this CLI Guide, the NMC must have the 1-Phase or 3-Phase Easy UPS firmware installed, and the NMC must be installed in a supported UPS. For more information on UPS models compatible with your NMC, see Knowledge Base article **FA237786**.

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

NOTE: You will be prompted to enter a new password the first time you connect to the NMC with the Super User account.

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

See the UPS Network Management Card 3 **User Guide** 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. Only SSH 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”.

SSH for high-security access. If you use the high security of SSL/TLS 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.

1. Use the following example command to use SSH to access the NMC:

   ```
   ssh -c aes256-ctr apc@156.205.14.141
   ```

   NOTE: This SSH command is for OpenSSH. The command may differ depending on the SSH tool used.

2. Enter the user name and password.

   NOTE: You will be prompted to enter a new password the first time you connect to the NMC with the Super User account.

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.
   NOTE: This example works for command prompt based Telnet clients. The commands may differ for different Telnet clients.

   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.

   NOTE: You will be prompted to enter a new password the first time you connect to the NMC with the Super User account.

Local access to the command line interface

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

1. Connect the provided micro-USB cable (part number 960-0603) from a USB port on the computer to the console port at the NMC.
2. In Windows Search, type "Device Manager", or open it from the Control Panel. Select "Ports" and note the COM port number the NMC was assigned.
3. Run a terminal program (e.g. 3rd party terminal emulator programs like HyperTerminal, PuTTy, or Tera Term) and configure the COM port (noted in step 2) for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
4. Press ENTER, repeatedly if required, to display the **User Name** prompt.
5. Enter the user name and password.

   NOTE: The user name will be "apc" at first log for the Super User account. You will be prompted to enter a new password after you log in.

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 2022 All Rights Reserved Easy UPS 3-Phase APP         vx.x.x
-------------------------------------------------------------------------
Name     : Test Lab                                  Date : 02/30/2022
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+
-------------------------------------------------------------------------
IPv4                 : Enabled          IPv6               : Enabled
Ping Response        : Enabled
-------------------------------------------------------------------------
HTTP                 : Disabled         HTTPS              : Enabled
FTP                  : Disabled         Telnet             : Disabled
SSH/SCP              : Enabled          SNMPv1             : Read/Write
SNMPv3               : Disabled         Modbus TCP         : Disabled
-------------------------------------------------------------------------
Super User           : Enabled          RADIUS             : Disabled
Administrator        : Disabled         Device User        : Disabled
Read-Only User       : Disabled         Network-Only User  : Read/Write
-------------------------------------------------------------------------
Type ? for command listing
Use tcpip command for IP address(-i), subnet(-s), and gateway(-g)
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 3-Phase application firmware for a Easy UPS.

  ```
  Network Management Card AOS    vx.x.x
  Easy UPS 3-Phase 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 management interface 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 : 02/30/2022
Time : 5:58:30
```

- The **User** field reports whether you logged in through the **Super User**, **Administrator**, **Device Manager**, **Network-Only** or **Read-Only** account.
  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.

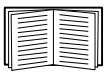
- The **Stat** field reports the NMC status. The middle status varies according to whether you are running IPv4, IPv6, or both, as indicated in the second table below.

```
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 DHCP or 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 https://www.se.com/ww/en/work/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: Super User also requires the current password when changing the password remotely. 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
E107	Serial communication with the UPS has been lost
E108	EAPoL disabled due to invalid/encrypted certificate

Command Descriptions

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

For more information, consult the Network Management Card for Easy UPS **Feature Breakdown** document.

?

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, Read-Only User, Network-Only 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, Read Only

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.
	`informational`	View the number of active informational alarms.

Example: To view all active warning alarms, type:

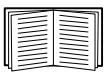
```
alarmcount -p warning
```

bacnet

Access: Super User, Administrator, Device User

Description: View and define the BACnet settings.

BACnet is not supported on the AP9544 card.



For more information on the UPS data points made available via BACnet, see the BACnet Application Maps available on www.se.com.

Option	Arguments	Description
-S	enable | disable	Select the option to enable or disable BACnet. If BACnet is disabled, the NMC cannot be accessed via BACnet. BACnet is disabled by default. **NOTE:** BACnet cannot be enabled until the Device Communication Control Password (-pw) is set.
-d	0-4194303	A unique identifier for this BACnet device, used for addressing the device.
-n	<device name>	A name for this BACnet device, which must be unique on the BACnet network. The default device name is “BACn”+ the last eight digits of the NMC MAC address. The minimum length is 1, the maximum length is 150 characters, and special characters are permitted.
-t	1000 - 30000	Specify the APDU timeout; the number of milliseconds the NMC will wait for a response to a BACnet request. The default value is 6000.
-r	0 - 10	Specify the APDU retries; the number of BACnet requests attempts that the NMC will make before aborting the request. The default value is 3.
-pw	<password>	The Device Communication Control service is used by a BACnet client to instruct a remote device (e.g. a BACnet-enabled NMC) to stop initiating, or stop responding to all APDUs (except the Device Communication Control service) for a specified duration of time. This service can be used for diagnostic purposes. Specify the Device Communication Control password to ensure that a BACnet client cannot control the BACnet communication of an NMC without first providing the password set here. The password is required to be between 8 and 20 characters, and must contain: • A number. • An uppercase character. • A lowercase character. • A special character. It is recommended to update the password when you first enable BACnet. You do not need to know the current password to update the password.
BACnet IP options:		
-o	47808, 5000-65535	Specify the UDP/IP port the NMC uses to send and receive BACnet/IP messages. **NOTE:** The address of a BACnet/IP-enabled NMC is defined as the IP address of the NMC and the local port.

Option	Arguments	Description
-fdre	enable | disable	Specify enable to register the NMC with a BACnet broadcast management device (BBMD). **NOTE:** You need to register your NMC as a foreign device with a BBMD if there is no BBMD currently on the subnet of the NMC, or if the NMC uses a different local port to the BBMD. See the NMC **User Guide** for more information on Foreign Device Registration.
-rip	IP address	The IP address or fully qualified domain name (FQDN) of the BACnet broadcast management device with which this NMC card will be registered.
-rpo	(0-65535)	The port of the BBMD with which this NMC card will be registered.
-fttl	1-65535	The number of seconds (Time To Live) that the BBMD will maintain the NMC as a registered device. If the NMC does not re-register before this time expires, the BBMD will delete it from its foreign-device table, and the NMC will no longer be able to send and receive broadcast messages via the BBMD.

Example:

```
bacnet
E000: Success
Enabled: yes
Device ID: 1013
Device name: BACnB7D7E5F2
Network Protocol: BACnet/IP
APDU timeout (ms): 6000
APDU retries: 3
IP Port: 47808 (0xBAC0)
Registration Enabled: no
Registration Status: Foreign device registration inactive
Registration BBMD: 0.0.0.0
Registration BBMD port: 47808 (0xBAC0)
Registration TTL: 7200
```

boot

Access: Super User, Administrator, Network-Only User

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.
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, Read-Only User, Network-Only User

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

Example:

```
bye

Connection Closed - Bye
```

cd

Access: Super User, Administrator, Device User, Read-Only User, Network-Only 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 ..
```

cfguio

This command is only available on the AP9544 card when connecting the AP9811 USB to Dry Contact Accessory for NMC to the USB port of the NMC card.

Access: Super User, Administrator, Device User

Description: Show or configure the parameters used by an attached AP9811 USB to Dry Contact Accessory for NMC..

Option	Argument	Description
`<none>`		Show all attached UIO probes and the parameters associated with those.
`-cname`	`[UIO port #] [contact #] <name>`	Input contact name.
`-cloc`	`UIO port #] [contact #] <location>`	Input contact location.
`-cnormst`	`[UIO port #] [contact #] <open | closed>`	Input contact normal state.
`-csever`	`[UIO port #] [contact #] <warning | critical>`	Input contact alarm severity.
`-cenable`	`[UIO port #] [contact #] <enable | disable>`	Enable or disable input contact alarm generation.
`-orname`	`[UIO port #] <name>`	Output relay name.
`-orloc`	`[UIO port #] <location>`	Output relay location.
`-ornormst`	`[UIO port #] <open | closed>`	Output relay normal state.
`-ordelay`	`[UIO port #] <0-65535 seconds>`	Output relay activation delay. The number of seconds an alarm condition must exist before the output relay is activated.
`-orhold`	`[UIO port #] <0-65535 seconds>`	Output relay hold time. The minimum number of seconds the output relay remains activated after the alarm occurs.

Example 1: To show all the attached UIO probes and their associated parameters, type:

```
cfguio
```

Example 2: To set the name of the input dry contact device connected to port 1, type:

```
cfguio -cname 1 "new dry contact name"
```

clrrst

Access:

Super User, Administrator

Definition: Clear the network interface reset reason. See "lastrst".

console

Access: Super User, Administrator, Network Only

Description: Define whether users can access the command line interface using Telnet, which is disabled by default, or Secure Shell (SSH), which is enabled by default, 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.
-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 |57600 | 115200	Configure the serial baud rate (9600 by default).

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

```
console -s
```

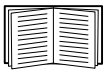
Example 2: To change the Telnet port to 5000, type:

```
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 Guide**.

Option	Argument	Description
`-d`	`<"datestring">`	Set the current date. Use the date format specified by the `date -f` command.
`-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. **NOTE:** The date format configured in the user settings in the NMC UI will override this setting at next login.
`-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 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>`

dir

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

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

Example:

```
dir
E000: Success
5165388 Dec 17  2021  apc_hw21_aos_2.1.0.6.bin
     5166412 Jan 17  2021  apc_hw21_eu3p_1.1.0.40.bin
       45000 Dec 17  5:14  config.ini
           0 Feb 23  4:31  db/
           0 Feb 23  4:31  ssl/
           0 Feb 23  4:31  ssh/
           0 Feb 23  4:31  logs/
           0 Feb 23  4:31  sec/
           0 Feb 23  4:31  fwl/
           0 Feb 23  4:31  email/
           0 Feb 23  4:31  eapol/
           0 Feb 23  4:34  fne/
```

dns

Access: Super User, Administrator, Network-Only User

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
```

eapol

Access: Super User, Administrator

Description: Configure EAPoL (802.1X Security) settings.

Option	Argument	Description
`-S`	`enable | disable`	Enable or disable EAPoL.
`-n`	`<supplicant name>`	Set the supplicant name.
`-c`	`<certificate filename>`	Set the certificate file used for authentication.
`-r`	`<restart authentication>`	Restart the EAPoL authentication process.

Example 1: To display the result of an `eapol` command:

```
apc>eapol

E000: Success
Active EAPoL Settings
---------------------
Status:enabled
Supplicant Name:NMC-Supplicant Passphrase:<hidden>
CA file Status:Valid Certificate
Private Key Status:Valid Certificate
Public Key Status:Valid Certificate

Result:Success
```

Example 2: To enable EAPoL:

```
apc>eapol -S enable
E000: Success

* Reboot required for change to take effect.
```

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 emails will be sent. This is dependent on the installed language pack.
-r [n]	<Local | recipient | custom> (Route)	Set the SMTP Server options: • **Local** (recommended): Choose this option if your SMTP server is located on your internal network, or is set up for your e-mail domain. 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>	

Option	Argument	Description
-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/TLS connections. If this is enabled, a valid root CA certificate must be loaded onto the NMC for encrypted emails to be sent.
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, using the local SMTP server:

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

eventlog

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

Description: Exit from the command line interface session.

firewall

Access: Super User, Administrator, Network-Only User

Description: Enable, disable, or configure the internal NMC firewall feature.

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.
`-Y`		Skip the firewall test prompt.

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, Network-Only User

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. **NOTE:** FTP is disabled by default, and Secure CoPy (SCP) is automatically enabled when the Super User password is set via SSH.

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, Read-Only User, 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 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 User, 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.

Option	Definition
`02 NMI Reset`	The network interface was reset via the Reset button on the NMC faceplate.

Option	Definition
`09 Coldstart Reset`	The network interface was reset by removing power from the hardware.
`12 WDT Reset`	The network interface was reset via a firmware command.

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: Creates a single, compressed archive of the log files available from the NMC and UPS device. These files can be used by technical support to troubleshoot issues.

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_ZA1752123456.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
-tE	<enable | disable> (Modbus TCP status)	Enable or disable Modbus TCP.
-tP	<502, 5000 to 32768> (TCP Port Number)	Specify the Modbus TCP port number. The default port number is 502, and can be set to a value between 5000 and 32768.
-tTo		Specify the Modbus TCP communication timeout in seconds, where 0 indicates that the connection never times out.
-ka	<enable | disable>] (Keep-Alive feature)	Enable or disable Modbus Keep Alive.

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, Network-Only User

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

Example:

```
netstat
Current IP information
Family   mHome    Type     IP Address                          Status
IPv6     4        auto     FE80::2C0:B7FF:FEEA:D325/64         configured
IPv4     0        manual   10.125.43.115/22                    configured
IPv6     0        manual   ::1/128                             configured
IPv4     0        manual   127.0.0.1/32                        configured
```

ntp

Access: Super User, Administrator, Network-Only 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, Network-Only 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.

Option	Argument	Description
	<IP address or DNS name>	Type an IP address with the format *xxx.xxx.xxx.xxx*, or a DNS name.
-t	<ping until stopped>	Ping continuously until you stop it.

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, Network-Only User

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
```

NOTE: The Port Speed setting can be changed to 1000 Mbps. However, this change can only be made via the Web UI. See “Port Speed screen” in the User Guide for more information.

prompt

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

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

quit

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

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

radius

Access: Super User, Administrator, Network-Only User

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 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**.

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 or is unreachable over the network, 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.
`-m1`	`<enable | disable>`	Require Message-Auth for the primary RADIUS server.
`-m2`	`<enable | disable>`	Require Message-Auth for the 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, Network-Only User

Description: Restart the network management interface of the NMC.

This does not affect the output power of the device in which the NMC is installed.

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:

```
session
User     Interface   Address                 Logged In Time        ID
-------------------------------------------------------------------------
apc      Telnet      10.169.118.100          00:00:03              19
```

smtp

Access: Super User, Administrator, Network-Only User

Description: Configure the settings for the local e-mail server.

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.
-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/TLS connections. If this is enabled, a valid root CA certificate must be loaded onto the NMC for encrypted emails to be sent.

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, Network-Only User

Description: Enable or disable and configure SNMPv1. **NOTE:** SNMPv1 is disabled by default. The Community Name (`-c[n]`) must be set before SNMPv1 communications can be established.

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.
`-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, Network-Only User

Description: Enable or disable and configure SNMPv3. **NOTE:** SNMPv3 is disabled by default. A valid profile must be enabled with passphrases (`-a[n]`, `-c[n]`) set before SNMPv3 communications can be established.

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 (encryption) 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.
-l[n]	<Language> [language code]	Specify a language. A language pack containing the desired language must be installed, and the language codes are: • enUS - English • deDe - German • ruRu - Russian • zhCn - Chinese • jaJa - Japanese • koKo - Korean • itIt - Italian • ptBr - Portuguese • frFr - French • esEs - Spanish
-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.
-p[n]	<Port>	Specify the SNMP trap port number.
n= Trap receiver number = 1, 2, 3, 4, 5 or 6		

Example: To enable and configure an SNMPv1 trap for Receiver 1, with the 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 enUS -t1 snmpV1 -g1 enable
E000: Success
```

ssh

Access: Super User, Administrator

Description: Show, delete, and generate SSH server keys. **NOTE:** The options in the table below are available with the `ssh key` command.

Option	Arguments	Description
`-s`		Display the current SSH server key in use.
`-f`		Display the current SSH server key's fingerprint.
`-d`		Delete the current SSH server key in use.
`-i`	`<File Name>.pk15`	Import the SSH server key from a PKCS #15 file.
`-ecdsa`	`256`	Generate an Elliptic Curve Digital Signature Algorithm (ECDSA) SSH server key with the specified size in bits.
`-rsa`	`1024 | 2048 | 4096`	Generate a Rivest–Shamir–Adleman (RSA) SSH server key with the specified size in bits.

Example 1: To display the current SSH server key, type:

```
ssh key -s
E000: Success.
```

Example 2: To import the SSH server key from a .p15 file generated by the NMC Security Wizard CLI Utility, type:

```
ssh key -i nmc.p15
E000: Success.
```

ssl

Access: Super User, Administrator, Network-Only User

Description: Configure and manage the NMC's public key and Web UI certificate, and create a Certificate Signing Request (CSR).

NOTE: There are three sets of options for this command, indicated below (`key`, `csr`, and `cert`).

Configure public keys (`key`):

Option	Arguments	Description
`-s`		Display the current public key in use.
`-d`		Delete the current public key in use.
`-i`	`<File Name>.p15`	Import the public key from a PKCS #15 file.
`-ecdsa`	`256 | 384 | 521`	Generate an Elliptic Curve Digital Signature Algorithm (ECDSA) public key with the specified size in bits.
`-rsa`	`1024 | 2048 | 4096`	Generate a Rivest–Shamir–Adleman (RSA) public key with the specified size in bits.

Example 1: To generate a new ECDSA-521 public key, type:

```
ssl key -ecdsa 521
```

```
E000: Success.
```

Example 2: To import the public key from a .p15 file generated by the NMC Security Wizard CLI Utility, type:

```
ssl key -i nmc.p15
E000: Success.
```

Configure Certificate Signing Request (`csr`):

Option	Arguments	Description
`-s`	`<File Name>`	Display the current Certificate Signing Request (CSR).
`-q`	`<File Name>`	Create a Certificate Signing Request (CSR) from active configuration.
`-CN`	`<Common Name>`	Create a custom Certificate Signing Request (CSR). The Common Name is the fully qualified domain name (FQDN) of the NMC. For example, its IP address or *.nmc.local.
Custom Certificate Signing Request (CSR) options. **NOTE:** The below options are only available for `-CN`.		
`-O`	`<Organization>`	The name of your organization.
`-OU`	`<Organizational Unit>`	The division of your organization handling the certificate.
`-C`	`<Country>`	The two-letter country code of where your organization is located.
`-san`	`<Common Name | IP Address>`	The Common Name or IP address of the NMC.

NOTE: Created Certificate Signing Requests will be stored in the NMC's ssl directory. See **dir**.

Example 3: To create a quick Certificate Signing Request (CSR) from active configuration, type:

```
ssl csr -q
E000: Success
```

Example 4: To create a minimal Certificate Signing Request (CSR), type:

```
ssl csr -CN 190.0.2.0 -C US
E000: Success
```

Example 5: To create a custom Certificate Signing Request (CSR), type:

```
ssl csr -CN apcXXXXXX.nmc.local -C US -san *.nmc.local -san 190.0.2.0

E000: Success
```

Configure the Web UI's certificate (`cert`):

Option	Arguments	Description
`-s`	`<File Name>`	Display the specified certificate. **NOTE:** Executing this option without an argument will display the current certificate in use.

Option	Arguments	Description
-f	<File Name>	Display the specified certificate's fingerprint. **NOTE:** Executing this option without an argument will display the current certificate's fingerprint.
-i	<File Name>	Import a certificate.

Example 6: To display the active certificate, type:

```
ssl cert -s
```

Example 7: To display nmc.crt located in the ssl directory, type:

```
ssl cert -s ssl/nmc.crt
```

Example 8: To import other.crt, type:

```
ssl cert -i other.crt
```

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 Data Center Expert, or EcoStruxure IT Expert and the NMC's SNMP agent.
-c	<system contact>	
-l	<system location>	
-m	<system-message>	Show a custom message or banner 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, Network-Only User

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

Option	Argument	Description
`-S`	`enable | disable`	Enable or disable TCP/IP v4.
`-i`	`<IPv4 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, Network-Only User

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 TCP/IP v6.
`-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

This command is only available on the AP9544 card when connecting the AP9811 USB to Dry Contact Accessory for NMC to the USB port of the NMC card.

Access: Super User, Administrator, Device User

Description: View the status of any connected UIO probes.

Option	Argument	Description
`-rc`	`<UIO port #> <open | close >`	Relay control.
`-st`	`<UIO port #> | <UIO port #>, <UIO port #> | <UIO port #>- <UIO port #>`	View the status of the dry contact devices connected. To view the status of a specific dry contact device, type their UIO port numbers.
`-disc`	`<UIO port #>, <UIO port #> | <UIO port #>- <UIO port #>`	Identify the dry contact devices connected, if any, to the UIO port(s). 9811 = Dry Contact Accessory for NMC (AP9811)

Example 1: To open the output relay on the second UIO port, type:

```
uio -rc 2 open
```

Example 2: To view the status of the device connected to UIO port 2, type:

```
uio -rc 2 open
```

ups

Some **ups** options are dependent 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 Guide for information on how these options relate to that screen.

The ups command options for specific UPS devices:

These commands are only available on supported 3-Phase UPS devices. Some options may only be available based on the individual UPS model. Please refer to Knowledge Base article **FA237786** for a list of UPS devices the Network Management Cards are compatible with.

Option	Argument	Description
`-im`	`<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.
`-bym`	`<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.
`-om`	`<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.
`-bat`		Display the battery status of the UPS
`-abt`		Displays information about the UPS.
`-al`	`c | w | i`	Display all existing alarms. Specifying “c”, “w”, or “i” limits the display to either Critical (c), Warning (w), or Informational (i) alarms.
`-amb`		Display the ambient temperature of the UPS.
`-maint`		Display the maintenance parameters of the UPS.

Example 1: To view maintenance parameters, type:

```
ups -main
```

These commands are only available on supported 1-Phase Easy UPS On-Line devices. Some options may only be available based on the individual UPS model. Please refer to Knowledge Base article FA237786 for a list of UPS devices the Network Management Cards are compatible with.

Option	Description
-im	Display the input measurements for the UPS: input voltage, input fault voltage, and frequency.
-om	Display the output measurements for the UPS: output voltage, output current, real power, and apparent power rating.
-bat	Display the battery measurements of the UPS: battery voltage and battery temperature.
-al	Display all existing critical, warning, and informational alarms.
-abt	Displays information about the UPS.

Example 2: To view input measurements, type:

```
ups -im

E000: Success

UPS Input Measurement(s)

------------------------

Voltage:       245.7 VAC

Frequency:     59.99 Hz

Fault Voltage: 200.0 VAC
```

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 User, Network-Only User), see the User Guide.

Option	Argument	Description
-n	<user>	Indicate the user.
-cp	<current password>	For a Super User, you must specify the current password. **NOTE:** The -cp option is only required when changing the Super User's password remotely.
-pw	<user password>	Specify these options for a user. **NOTE:** Description must be enclosed in quotation marks.
-pe	<user permission>	
-d	<user description>	
-e	enable | disable	Enable or disable access for the particular user account.
-te	enable | disable	Enable touch screen access.

Option	Argument	Description
-tp	<touch screen access pin>	This option is only available on certain devices.
-tr	enable | disable	Enable the touch screen remote authorization override. This option is only available on certain devices. 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.
-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. For a list of available languages and corresponding language codes, type `lang` at the command prompt.
-del	<user name>	Delete a user.
-l		Display the current user list.

Example: 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.

Option	Argument	Definition
-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. Description must be enclosed in quotation marks.
-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 | 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 (e.g. enUS)>	Specify a user language. For a list of available languages and corresponding language codes, type `lang` at the command prompt.
-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, Network-Only User

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. HTTP is disabled by default.
`-s`	`enable | disable`	Enable or disable access to the user interface for HTTPS. HTTPS is disabled by default. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate using SSL/TLS.
`-mp`	`<minimum protocol>`	Specify the minimum protocol used by the web interface: SSL v3.0, TLS v1.1, or TLS v1.2.
`-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.
`-lsp`	`enable | disable`	Enable or disable access to the Limited Status page in the Web UI.
`-lsd`	`enable | disable`	Enable or disable the Limited Status page being used as the default page when accessing the device's IP or hostname in a web browser.
`-cs`	`<0 | 1 | 2 | 3 | 4>`	Select the level of security of TLS v1.2 cipher suites between 0 - 4, where 4 is the highest level of security, and 0 is the lowest level of security. The default value is 4. **NOTE:** The `-cs` option is only applied when `-mp` is set to TLS v1.2. When a value between 0 - 4 is entered, the CLI responds with a list of the currently allowed SSL cipher suites.

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

```
web -s disable
```

whoami

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

Description: Provides login information on the current user

Example:

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

wifi

Access: Super User, Administrator

Description: Enable or disable wi-fi and configure the Wi-Fi network's settings.

This command requires the optional APC USB Wi-Fi Device (AP9834) to be inserted in a USB port of an AP9544/AP9547 card.

IMPORTANT: It is recommended that you do not download a config.ini file from a wired device and upload the entire file to a Wi-Fi-enabled device. It is also not recommended to download a config.ini file from a Wi-Fi-enabled device and push the entire file to a wired device unless the entire `[NetworkWiFi]` section is removed or commented out using semi-colons (for example `;WiFi=enabled`).

The `[NetworkWiFi]` section contains device settings specific to Wi-Fi use. These settings should not be uploaded to a wired device.

Option	Argument	Definition
`-S`	`enable | disable`	Enable or disable Wi-Fi. Disabled by default. **NOTE:** Enabling/ disabling Wi-Fi will disable/enable the wired LAN connection.
`-n`	`<network name (SSID)>`	Specify the network name (SSID) of the Wi-Fi network. The maximum length is 32 characters.
`-t`	`WPA | WPA2-AES |WPA2-Mixed | WPA2-TKIP | WPA2-Enterprise`	Specify the security type (authentication and encryption) of the Wi-Fi network.
`-p`	`<wifi password>`	Specify a password for the Wi-Fi network. The maximum length is 64 characters. **NOTE:** This is required for WPA, WPA2-AES, and WPA2-Mixed security types.
`-eu`	`<WPA2-Enterprise user name>`	The user name for WPA2-Enterprise authentication. The maximum length is 32 characters.
`-ep`	`<WPA2-Enterprise password>`	The password for WPA2-Enterprise authentication. The maximum length is 32 characters.
`-eo`	`<WPA2-Enterprise outer identity>`	Specify the WPA-2-Enterprise outer identity. This is an optional unencrypted identification used by the WPA-2-Enterprise server. For example: user@example.com or anonymous. The maximum length is 32 characters.
`-fw`	`<path/ filename>`	Specify the firmware file to upgrade the APC USB Wi-Fi Device's firmware. This must be an .ism file located on a USB drive inserted into the USB port of the NMC. **NOTE:** The Wi-Fi network will be unavailable during the firmware upgrade.

Example 1: To enable Wi-Fi and configure the Wi-Fi network's settings, type:

```
wifi -S enable -n NETGEAR06 -t WPA2-AES -p apc123
```

Example 2: To upgrade the APC USB Wi-Fi Device's firmware, type:

```
wifi -fw apc_uw01_wni_1-26-7.ism
```

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

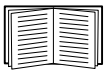
Access: Super User, Administrator

Description: View the result of the last file transfer.

Example: `xferStatus`

```
E000: Success

Result of last file transfer: OK
```



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

Copyright Notices

Cryptlib Cryptology Library

Cryptlib copyright © Digital Data Security New Zealand Ltd 1998.

Berkeley Database

Copyright © 1991, 1993 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Lua

Copyright © 1994–2021 Lua.org, PUC-Rio.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions ofthe Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Worldwide Customer Support

Access to customer support terms may vary by product. 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.se.com** (Corporate Headquarters)
    Connect to localized Schneider Electric Web sites for specific countries, each of which provides customer support information.
  - **www.se.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.se.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.

990-91547F-001 **02/2026**