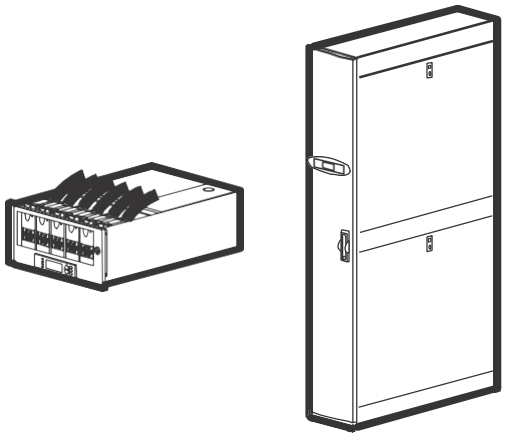
# User Guide
## Network Management Card 2 for Modular Power Distribution Units, Remote Power Panel, and Rack Distribution Panel

**PDPM138H-5U**
**PDPM138H-R**
**PDPM72F-5U**
**PDPM72F-R**
**PDPM277H**
**PDPM144F**

**990-5787B**

**Publication Date: 2/2024**



www.se.com

Schneider Electric

# Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.
This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.
The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.
This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.
Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.
Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.
**To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content there**

# Table of Contents


Introduction ..... 1
Overview ..... 1
Features ..... 1
Getting Started ..... 2
Make the connection to the unit: ..... 2
Initial setup ..... 2
Accessibility ..... 2
Network management features ..... 2
User Account Overview ..... 3
Recover from a Lost Password ..... 4
Watchdog Features ..... 6
Overview ..... 6
Network interface watchdog mechanism ..... 6
Resetting the network timer ..... 6
Automatic Logout ..... 6
Command Line Interface ..... 7
About the Command Line Interface (CLI) ..... 7
Log on to the CLI ..... 7
Remote access to the CLI ..... 7
Local access to the CLI via serial port ..... 7
Local access to the CLI via USB port ..... 8
CLI Home Screen ..... 9
Sample home screen ..... 9
Information and status fields ..... 9
Using the CLI ..... 10
Command Syntax ..... 11
Command Response Codes ..... 12
Command Editing ..... 13
Auto-Completion ..... 13
Command History ..... 13
Delimiter ..... 13
Security Lockout ..... 13
Network Management Card Command Descriptions ..... 14
? or help ..... 14
about ..... 15
alarmcount ..... 15
boot ..... 16
bye ..... 16
cd ..... 17
clrrst ..... 17
console ..... 18
date ..... 19
delete ..... 19

dir ..... 20
dns ..... 20
email ..... 21
eventlog ..... 22
exit or quit ..... 23
firewall ..... 23
format ..... 23
ftp ..... 24
help ..... 24
lang ..... 24
lastrst ..... 25
ledblink ..... 25
logzip ..... 25
netstat ..... 26
ntp ..... 26
ping ..... 27
portSpeed ..... 28
prompt ..... 28
pwd ..... 29
radius ..... 29
reboot ..... 30
resetToDef ..... 31
session ..... 31
smtp ..... 32
snmp ..... 33
snmpv3 ..... 34
snmptrap ..... 34
system ..... 35
tcpip ..... 36
tcpip6 ..... 36
user ..... 37
userdflt ..... 38
web ..... 39
whoami ..... 40
xferINI ..... 41
xferStatus ..... 41
Device Command Descriptions ..... 42
sysOutput ..... 42
modStatus ..... 43
cblStatus ..... 44
cblName ..... 45
cblLoc ..... 45
cblAlrm ..... 46
cblThrMx ..... 47
cblThrHi ..... 48
cblThrLo ..... 49
cblThrMn ..... 50
cblBrkrPos ..... 51
cblRstkWh ..... 52
getAlarm ..... 53

mfactElec ..... 53
mfactMeter ..... 54
mfactMod ..... 54
modbus ..... 55
The Web Interface ..... 56
Supported Web browsers ..... 56
Log On ..... 56
Overview ..... 56
URL address formats ..... 56
Web Interface Features ..... 57
Tabs ..... 57
Device status icons ..... 58
Quick Links ..... 58
Device Menu Tree ..... 59
The Home Page ..... 60
The Status Tab ..... 61
View the Network Status ..... 62
Current IPv4 Settings ..... 62
Current IPv6 Settings ..... 62
Domain Name System Status ..... 62
Ethernet Port Speed ..... 62
The Control Tab ..... 63
Session Management ..... 63
Reset the Network Interface ..... 64
The Configuration Tab ..... 65
Device ..... 65
Security ..... 69
Firewall ..... 73
Network Settings ..... 74
Notification ..... 83
SNMP trap receiver screen ..... 88
SNMP traps test screen ..... 88
Remote Monitoring Service ..... 89
General Options ..... 90
Logs in the Configuration Menu ..... 92
The Tests Tab ..... 93
Logs Tab ..... 94
Event, Data, and Firewall Logs ..... 94
Data log ..... 96
Firewall Logs ..... 97
Use FTP or SCP to retrieve log files ..... 98
The About Tab ..... 99
About the Device ..... 99
Device IP Configuration Wizard ..... 101
System requirements ..... 101
Installation ..... 101
Launch the Wizard ..... 101

Export Configuration Settings ..... 102
Retrieving and Exporting the .ini File ..... 102
Summary of the procedure ..... 102
Contents of the .ini file ..... 102
Detailed procedures ..... 103
The Upload Event and Error Messages ..... 104
Messages in config.ini ..... 105
Errors generated by overridden values ..... 105
Related Topics ..... 105
Firmware File Transfer Methods ..... 106
Using the Firmware Upgrade Utility ..... 106
Use FTP or SCP to upgrade one unit ..... 107
Use XMODEM to upgrade one unit ..... 108
Use a USB drive to transfer and upgrade the files ..... 108
How to upgrade multiple units ..... 109
Using the Firmware Upgrade Utility for multiple upgrades ..... 109
Verifying Upgrades and Updates ..... 110
Last Transfer Result codes ..... 110
Verify the version numbers of installed firmware. ..... 110
Troubleshooting ..... 111
Access Problems ..... 111
SNMP Issues ..... 112

# Introduction

# Overview

Network Management Cards (NMC) for the following Schneider Electric Power Distribution Units are covered in this manual:

- Modular Power Distribution Unit (PDU)
- Remote Power Panel (RPP)
- Rack Distribution Panel (RDP)

### Features

Your Schneider Electric power distribution unit provides power distribution and management of electrical power to equipment racks. In each unit, the Network Management Card (NMC) provides full management capabilities over a network using the following standards:

- Telnet
- Secure SHell (SSH)
- HyperText Transfer Protocol (HTTP)
- HTTP over Secure Sockets Layer (HTTPS)
- File Transfer Protocol (FTP)
- Simple Network Management Protocol (SNMP) versions 1 and 3
- Modbus RS-485 RTU and Modbus TCP
- TCP/IP v4 and v6
- Secure Copy (SCP)
- SMTP-based email
- RADIUS (Remote Access Dial In User Service)

The unit also provides the following features:

- Multiple login feature allows up to four users to be logged in simultaneously.
- Provides the ability to export a user configuration (.ini) file from a configured unit to one or more unconfigured units.
- Supports using a Dynamic Host Configuration Protocol (DHCP) server to provide the network (TCP/IP) values for the unit.
- Provides data and event logs.
- Enables you to configure notification through event logging (by the unit and Syslog), e-mail, and SNMP traps. You can configure notification for single events or groups of events, based on the severity level or category of events.
- Provides a selection of security protocols for authentication and encryption.

# Getting Started

### Make the connection to the unit:

A Cat-5 cable is plugged into the ethernet port on the unit. Connect the other end of the cable to the LAN.

A local computer can be connected to the Computer Interface port with a serial cable. Connect the other end of the serial cable to the local computer.

**NOTE:** Consult the Operation Manual for your equipment for information regarding the location of the Network Management Interface on your unit.

### Initial setup

To start using the unit:

- Install the unit using the *Installation Instructions* that were shipped with your unit.
- Apply power and connect to your network. Follow the directions in the *Installation Instructions*. Establish network settings. Three TCP/IP settings must be defined for the Network Management Card of the unit before it can operate on the network:
  – IP address of the unit's Network Management Card
  – Subnet mask
  – IP address of the default gateway

| ***NOTICE*** |
| --- |
| Do not use the loopback address as the default gateway. Doing so disables the unit. You must then log on using a serial connection and reset TCP/IP settings to their defaults. |

If a default gateway is unavailable, use the IP address of a computer (that is usually running) located on the same subnet as the unit. The unit uses the default gateway to test the network when traffic is light.

### Accessibility

Begin using the unit by way of one of the following:

1. "The Web Interface" on page 54
2. "Command Line Interface" on page 6
3. The Display Interface on the front of the unit. See the Operation Manual for instructions.

### Network management features

These applications and utilities work with a PDU, RDP, or RPP that connects to the network through its Network Management Card:

- APC StruxureWare Central™ —Provide enterprise-level power management and management of APC agents, PDUs, (RDPs, or RPPs), information controllers, and environmental monitors
- APC PowerNet™ Management Information Base (MIB) with a standard MIB browser—Perform SNMP SETs and GETs and to use SNMP traps
- APC Device IP Configuration Wizard—Configure the basic settings of one or more units over the network
- APC Security Wizard—Create the components needed for high security for the unit when using Secure Sockets Layer (SSL) and related protocols and encryption routines

## User Account Overview

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

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

All levels of access require user name and password permissions.

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

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

**NOTE:** The Super User cannot be renamed or deleted, but it can be disabled. It is recommended that the Super User account is disabled once any additional Administrator accounts are created. Make sure that there is at least one Administrator account enabled before the Super User account is disabled.

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

- Click on Add User

The User types which can be added are:

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

# Recover from a Lost Password

You can access the command line interface (CLI) via a local computer either via serial port (available on all PDU models) or USB console port (USB console port is not available on older PDU models).

1. At the local computer, do one of the following:
   – Select a serial port and disable any service that uses it. Connect the provided serial cable (part 940-0103) between the selected serial port on the local computer and the serial port on the PDU, OR
   – Connect the provided standard USB cable between the PDU USB console port and the computer USB port. A virtual serial port will be discovered on the computer.
2. Open a terminal program/emulator (such as HyperTerminal®) and configure the (virtual) serial port for:
   – Default baud rate: 9600 bps (USB serial works with any other baud rate automatically)
   – Data bits: 8
   – Parity: None
   – Stop Bits: 1
   – Flow Control: None
3. Press ENTER, repeatedly if necessary, to display the User Name prompt. If you are unable to display the User Name prompt, verify the following:
   – The serial port is not in use by another application.
   – The terminal settings are correct as specified in step 2.
   – The correct cable is being used as specified in step 1.
   – SCROLL LOCK is not turned on.
4. Press the Reset button on the back of the unit. The Status LED will flash. Press the Reset button a second time while the LED is flashing to reset the user name and password to the default temporarily.
5. Press ENTER as many times as necessary to redisplay the User Name prompt, then use the default, **apc**, user name and password. (If you take longer than 30 seconds to log on after the User Name prompt is redisplayed, you must repeat step 5 and log on again.)
6. At the Command Console, use the following commands to change the password setting for the Super User account, for which the user name is always apc, and the password is now temporarily apc:

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

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

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

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

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

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

   **NOTE:** Changing user name information is no longer supported via the Command Console. If a user's user name needs to be changed, it must be deleted and re-created.

The Super User will also have access now to log in and adjust any other user's password.

7. Type QUIT, EXIT, or BYE to log off. Remember to reconnect any serial cable you may have disconnected, and to restart any service you may have disabled. Return the local computer to its original configuration.

**NOTE:** ModbusRTU and the Command Console share a common serial port. In some instances,the baud rate may be set to different speeds for other services, i.e. Modbus (19200 bps). Enabling ModbusRTU (Serial) will disable Command Console over Serial port. USB console port will be accessible even if Modbus RTU is enabled

# Watchdog Features

## Overview

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

## Network interface watchdog mechanism

The unit implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the unit does not receive any network traffic for 9.5 minutes (either direct traffic, such as SNMP, or broadcast traffic, such as an Address Resolution Protocol [ARP] request), it assumes that there is a problem with its network interface and restarts. The network interface watchdog mechanism is only enabled on a unit that discovers an active network interface connection at start-up.

## Resetting the network timer

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

## Automatic Logout

By default, users will be automatically logged out of the unit's Web and CLI interfaces after 3 minutes of inactivity. The default logout time can be adjusted through the web interface **Configuration > Security > Local Users > Management**.

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

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

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

# Command Line Interface

# About the Command Line Interface (CLI)

You can use the CLI to view the status of and configure and manage the unit. In addition, the CLI enables you to create scripts for automated operation. You can configure all parameters of a unit (including those for which there are not specific CLI commands) by using the CLI to transfer an INI file to the unit. The CLI uses XMODEM to perform the transfer, however, you cannot read the current INI file through XMODEM.

# Log on to the CLI

To access the CLI, you can use either a local (serial) connection or a remote (Telnet or SSH) connection with a computer on the same network as your power distribution unit. By default CLI is available via Telnet on Port 23. Once the user configures the network settings, the user can access the CLI through Telnet. The user can also configure the network settings to access the CLI via SSH or disable the CLI via Telnet and SSH.

### Remote access to the CLI

You can access the CLI through Telnet and/or SSH. Telnet is enabled by default. You do not have to enable either.

**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 CLI:

1. From a computer on the same network as the unit, at a command prompt, type telnet and the System IP address for the unit (for example, telnet 139.225.6.133, when the unit uses the default Telnet port of 23), and press ENTER.

   If the unit 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.

2. Enter the user name and password.

**SSH for high-security access.** If you use the high security of SSL for the Web interface, use Secure SHell (SSH) for access to the CLI. SSH encrypts user names, passwords and transmitted data. The interface, user accounts, and user access rights are the same whether you access the CLI through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

### Local access to the CLI via serial port

Use a computer that connects to the PDU through the serial port, to access the CLI:

1. Select a serial port at the computer and disable any service that uses the port.
2. Connect the provided serial cable from the selected port on the computer to the configuration port at the unit.
3. Run a terminal program such as HyperTerminal, and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER, and at the prompts, enter your user name and password.

### Local access to the CLI via USB port

Use a computer that connects to the PDU through the USB console port to access the CLI. Note that USB console port is not available on older PDU models.

1. Connect the provided standard USB cable between the PDU USB console port and the computer USB port.
2. A virtual serial port will be discovered on the computer.
3. Open a terminal program/emulator (such as HyperTerminal®) and configure the virtual serial port for:
    a. Default baud rate: 9600 bps (USB serial works with any other baud rate automatically)
    b. Data bits: 8
    c. Parity: None
    d. Stop Bits: 1
    e. Flow Control: None

Press ENTER, and at the prompts, enter your username and password.

# CLI Home Screen

## Sample home screen

The following is an example of the screen that displays when you log on to the CLI.

```
User Name  : apc
Password   : ***

Schneider Electric                          Network Management Card AOS     v6.4.0
(c) Copyright 2015 All Rights Reserved      XRDP                            v6.4.0
-------------------------------------------------------------------------------------------------------------------
Name       : XRDP                                          Date   : 03/01/2016
Contact    : Raghav                                        Time   : 13:57:38
Location   : LAB1                                          User   : Super User
Up Time    : 0 Days 1 Hour 45 Minutes                      Stat   : P+ N4+ N6+ A+

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

  ```
  Network Management Card AOSv6.4.0
  XRDP v6.4.0
  ```

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

  ```
  Name: XRDP
  Contact: Raghav
  Location: LAB1
  ```

- The **Up Time** field reports how long the unit has been running since it was last reset or since power was applied.

  ```
  Up Time: 0 Days 1 Hour 45 Minutes
  ```

- Two fields identify the current system date and time.

  ```
  Date : 12/30/2011
  Time : 5:58:30
  ```

- The **User** field identifies the type of logged user; whether **Super User**, **Administrator** or **Device User** account.

  ```
  User : Super User
  ```

**System and network status fields.**

- The **Stat** field reports the unit status.

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

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

| IPv4 only | IPv6 only | IPv4 and IPv6* | Description |
|---|---|---|---|
| N+ | N+ | N4+ N6+ | The network is functioning properly. |
| N? | N6? | N4? N6? | A BOOTP request cycle is in progress. |
| N– | N6– | N4– N6– | The Rack PDU failed to connect to the network. |
| N! | N6! | N4! N6! | Another device is using the Rack PDU IP address. |
| * 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. |

**NOTE:** If P+ is not displayed, contact the Schneider Electric support staff at **www.apc.com/support** even if you can still access the unit.

# Using the CLI

At the command line interface, you can 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 `exit` or `quit` to close the connection to the command line interface.

# Command Syntax

| Item | Description |
|---|---|
| - | Options are preceded by a hyphen. |
| < > | Definitions of options are enclosed in angle brackets. For example:<br>`-dp <device 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. |

**Example of a command that supports multiple options:**

```
ftp [-p <port number>] [-S <enable | disable>]
```

In this example, the `ftp` command accepts the option `-p`, which defines the port number, and the option `-S`, which enables or disables the FTP feature.

To change the FTP port number to 5010, and enable FTP:

1. Type the ftp command, the port option, and the argument `5010`:
   `ftp -p 5010`
2. After the first command succeeds, type the ftp command, the enable/disable option, and the `enable` selection:
   `ftp -S enable`

**Example of 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 fail 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 | 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 unit has been lost |

# Command Editing

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

### Auto-Completion

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

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

### Command History

Pressing the <up arrow> key presents the previously entered command onto the command line. The <up arrow> and <down arrow> keys permit the user to navigate the command history. In addition, pressing the <backspace> key deletes the last character of the command string the user is currently entering.
The command history buffer supports up to 10 previous commands.

### Delimiter

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

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

### Security Lockout

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

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

# Network Management Card Command Descriptions

### ? or help

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

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

**Parameters:** `[<command>]`

**Example 1:**

```
apc> ?

Network Management Card Commands:
-------------------------------------------------------------------------------

?           about       alarmcount  boot      bye         cd
clrrst      console     date        delete    dir         dns
email       eventlog    exit        firewall  format      ftp
help        lang        lastrst     ledblink  logzip      netstat
ntp         ping        portspeed   prompt    pwd         quit
radius      reboot      resetToDef  session   smtp        snmp
snmptrap    snmpv3      system      tcpip     tcpip6      user
userdflt    web         whoami      xferINI   xferStatus
```

**Example 2:**

```
apc> help boot
Usage: boot -- Configuration Options
   boot  [-b <dhcpBootp | dhcp | bootp | manual>] (Boot Mode)
         [-c <enable | disable>]    (Require DHCP Cookie)
         [-v <vendor class>]
         [-i <client id>]
         [-u <user class>]
```

**Error Message:** `E000, E102`

## about

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

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

**Parameters:** None

**Example:** `apc> about`

```
E000: Success
Hardware Factory
--------------------
Model Number:           XXXXXXXX
Serial Number:          XXXXXXXXXXXX
Hardware Revision:      XXXX
Manufacture Date:       3/4/2016
MAC Address:            00 00 A0 10 00 00
Management Uptime:      0 Days 1 Hour 42 Minutes
```

**Error Message:** `E000`

## alarmcount

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

**Description:** Displays alarms present in the system.

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

**Example:** To view all active warning alarms, type:

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

**Error Message:** `E000, E102`

## boot

**Access:** Super User, Administrator

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

| Option | Argument | Description |
|---|---|---|
| -b <boot mode> | dhcp \| bootp \| manual | Define how the TCP/IP settings will be configured when the unit turns on, resets, or restarts. See “IPv4 settings” on page 72 for information about each boot mode setting. |
| -c | [<enable \|disable>] (Require DHCP Cookie) | dhcp and dhcpBootp boot modes only. Enable or disable the requirement that the DHCP server provide the APC cookie. |
| -v | [<vendor class>] | Vendor Class is APC |
| -i | [<client id>] | The MAC address of the unit, Which uniquely identifies it on the network. |
| -u | [<user class>] | The name of the application firmware module. |

**Example:** Using a DHCP server to obtain network settings:

```
apc> boot
E000: Success
Boot Mode:              manual
Non-Manual Mode Shared Settings
-------------------------------------------
Vendor class:           <device class>
Client id:              XX XX XX XX XX XX
User class:             <user class>
After IP assignment:    gotoDhcpOrBootp

DHCP Settings
-----------------
Retry then stop:        4
DHCP cookie is:         enable

BOOTP Settings
--------------
Retry then fail:        never
On retry failure:       prevSettings
```

**Error Message:** E000, E102

## bye

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

**Description:** Exit the CLI

**Example:** bye

**Error Message:** None

## cd

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

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

**Parameters:** `<dicrectory name>`

**Example:**

```
apc> cd logs
E000: Success

apc> cd /
E000: Success
```

**Error Message:** `E000, E102`

## clrrst

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

**Description:** Clear reset reason.

**Example:** None

**Error Message:** None

## console

**Access:** Super User, Administrator

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

**Parameters:**

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

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

```
console -S ssh
```

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

```
apc> console -pt <5000>
Telnet:      enabled
SSH:         disabled
Telnet Port: 23
SSH Port:    22
Baud Rate:   9600
Error Message:
E000, E102
```

## date

**Access:** Super User, Administrator

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

To configure an NTP server to define the date and time for the NMC, see “Set the Date and Time” on page 88.

**Parameters:**

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

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

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

**Example 2:** To define the date as March 30, 2016, using the format configured in the preceding example, type:

```
date -d “2016-03-30”
```

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

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

**Error Message:** `E000, E100, E102`

## delete

**Access:** Super User, Administrator

**Description:** Delete a file in the file system.

**Parameters:**

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

**Example:**

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

**Error Messages:** `E000, E102`

## dir

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

**Description:** Displays the content of the working directory.

**Example:**
```
apc> dir
E000: Success
--wx-wx-wx  1 apc      apc      3145728 Mar 3  2015 aos.bin
--wx-wx-wx  1 apc      apc      3145728 Mar 4  2015 app.bin
-rw-rw-rw-  1 apc      apc        45000 Mar 6  2015 config.ini
drwxrwxrwx  1 apc      apc            0 Mar 3  2015 db/
drwxrwxrwx  1 apc      apc            0 Mar 3  2015 ssl/
drwxrwxrwx  1 apc      apc            0 Mar 3  2015 ssh/
drwxrwxrwx  1 apc      apc            0 Mar 3  2015 logs/
drwxrwxrwx  1 apc      apc            0 Mar 3  2015 sec/
drwxrwxrwx  1 apc      apc            0 Mar 3  2015 dbg/
drwxrwxrwx  1 apc      apc            0 Mar 3  2015 pdu/
```

**Error Messages:** `E000`

## dns

**Access:** Super User, Administrator

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

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

**Example:** None

**Error Message:** `E000`

## email

**Access:** Super User, Administrator, Device User

**Description:** View email

**Parameters:**

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

**Example:** None

**Error Message:** None

## eventlog

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

**Description:** View the date and time you retrieved the event log, the status of the NMC, 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. |

**Example:**

```
apc> eventlog
----- Event Log -------------------------------------------------------------------------
     Date: 03/06/2015 Time: 13:22:26
     ------------------------------------------------
     PDU : Communication Established
Date         Time      Event
     ------------------------------------------------------------------------------------
     03/06/2015 13:17:22  System: Set Time.
     03/06/2015 13:16:57  System: Configuration change. Date format
                           preference.
     03/06/2015 13:16:49  System: Set Date.
     03/06/2015 13:16:35  System: Configuration change. Date format
                           preference.
     03/06/2015 13:16:08  System: Set Date.
     03/05/2015 13:15:30  System: Set Time.
     03/05/2015 13:15:00  System: Set Time.
     03/05/2015 13:13:58  System: Set Date.
     03/05/2015 13:12:22  System: Set Date.
     03/05/2015 13:12:08  System: Set Date.
     03/05/2015 13:11:41  System: Set Date.
<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

**Error Message:** `E000, E100`

## exit or quit

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

**Description:** Exit from the CLI session.

**Parameters:** None

**Example:**

```
apc> exit
Bye
```

**Error Message:** None

## firewall

**Access:** Super User, Administrator

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

**Parameters:**

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

**Error Message:** None

## format

**Access:** Super User, Administrator

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

**Example:**

```
apc> format

Format FLASH file system

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

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

**Error Message:** None

## ftp

**Access:** Super User, Administrator

**Description:** Get/set the ftp configuration data,
**NOTE:** The system will reboot if any configuration is changed.

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

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

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

apc> ftp
E000: Success
Service:        Enabled
Ftp Port:       5001

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

**Error Message:** E000, E102

## help

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

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

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

```
help
```

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

```
alarmcount help
```

**Error Message:** None

## lang

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

**Description:** Language in use

**Example:** `Languages enUs - English .`

**Error Message:** None

## lastrst

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

**Description:** Last reset reason

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

**Example:**

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

**Error Message:** None

## ledblink

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

**Description:** Sets the blink rate to the LED on the unit).

**Parameters:** None

**Example:**

```
usage: ledblink -- Configuration Options ledblink <duration time in minutes>
```

**Error Message:** None

## logzip

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

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

**Parameters:**

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

**Example:**

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

**Error Message:** `E000`

## netstat

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

**Description:** Displays incoming and outgoing network connections.

**Parameters:**

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

**Example: .**

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

**Error Message:** None

## ntp

**Access:** Super User, Administrator

**Description:** Synchronizes the time to a computer client or server.

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

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

```
ntp -OM enable
```

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

```
ntp -p 150.250.6.10
```

**Error Message:** E000

## ping

**Access:** Super User, Administrator, Device User

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

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

**Example:**

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

**Error Message:** `E000, E100, E102`

## portSpeed

**Access:** Super User, Administrator

**Description:** Allows the user to get/set the network port speed.
**NOTE:** The system will reboot if any configuration is changed.

| Option | Arguments | Description |
|---|---|---|
| -s | auto \| 10H \| 10F \| 100H \| 100 F | Define the communication speed of the Ethernet port. The auto command enables the Ethernet devices to negotiate to transmit at the highest possible speed. See “Port Speed” on page 74 for more information about the port speed settings. |
| H = Half Duplex<br>F = Full Duplex | | 10 = 10 Meg Bits<br>100 = 100 Meg Bits |

**Example:**

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

apc> portspeed -s 10h
E000: Success

apc> portspeed
E000: Success
Port Speed: 10 Half_Duplex

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

**Error Message:** E000, E102

## prompt

**Access:** Super User, Administrator, Device User

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

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

**Example:**

```
apc> prompt -s long
E000: Success

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

**Error Message:** E000, E102

## pwd

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

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

**Parameters:** `pwd`

**Example:** `Usage: pwd --  Configuration Optionspwd`

**Error Message:** None

## radius

**Access:** Super User, Administrator

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

For a summary of RADIUS server configuration and a list of supported RADIUS servers, see “Summary of the Configuration Procedure” on page 70.
Additional authentication parameters for RADIUS servers are available at the Web interface of the NMC. See “Configuring the RADIUS Server” on page 70 for more information.
For detailed information about configuring your RADIUS server, see the *Security Handbook*, available at **www.apc.com**.

| Option | Argument | Description |
|---|---|---|
| `-a` | `local \| radiusLocal \| radius` | Configure RADIUS authentication:<br>`local`—RADIUS is disabled. Local authentication is enabled.<br>`radiusLocal`—RADIUS, then Local Authentication. RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used.<br>`radius`—RADIUS is enabled. Local authentication is disabled. |
| `-p1`<br>`-p2` | `<server port>` | The server port of the primary or secondary RADIUS server.<br>**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 unit supports ports 1812, 5000 to 32768. |
| `-o1`<br>`-o2` | `<server IP>` | The IP address of the primary or secondary RADIUS server. |
| `-s1`<br>`-s2` | `<server secret>` | The shared secret between the primary or secondary RADIUS server and the unit. |
| `-t1`<br>`-t2` | `<server timeout>` | The time in seconds that the unit 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.

```
apc>radius
E000: Success
Access: Local Only
Primary Server: 0.0.0.0
Primary Server Port: 1812
Primary Server Secret: <Password Hidden>
Primary Server Timeout: 5
Secondary Server: 0.0.0.0
Secondary Server Port: 1812
Secondary Server Secret: <Password Hidden>
Secondary Server Timeout: 5
```

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

```
radius -a radiusLocal
```

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

```
radius -t2 10
```

**Error Message:** `E000, E102`

## reboot

**Access:** Super User, Administrator

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

**Parameters:** None

**Example:**

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

**Error Message:** `E000, E100`

## resetToDef

**Access:** Super User, Administrator

**Description:** Reset all parameters to their default.

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

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

```
resetToDef -p keepip
Enter 'YES' to continue or <ENTER> to cancel : : <user enters 'YES'>
all User Names, Passwords.
Please wait...

Please reboot system for changes to take effect!
```

**Error Message:** E000, E100

## session

**Access:** Super User, Administrator, Device User

**Description:** Records which user is logged in, the interface, address, logged in time, and ID.

**Parameters:**

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

**Example:**

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

**Error Message:** E000

## smtp

**Access:** Super User, Administrator, Device User

**Description:** Internet standard for electronic mail.

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

**Example:**

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

**Error Message:** E000

## snmp

**Access:** Super User, Administrator

**Description:** Enable or disable SNMP 1 or SNMP 3.

| Option | Arguments | Description |
|---|---|---|
| -c | <Community> | Identify the group of units |
| -a | <read \| write \| writeplus \| disable> | Set the access level |
| -n | <IP or Domain Name> | The host's name or address |
| -S | enable \| disable | Enable or disable the respective version of SNMP, 1 or 3 |

**Example:** To enable SNMP version 1, type:

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

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

**Error Message:** None

## snmpv3

**Access:** Super User, Administrator

**Description:** Enable or disable SNMP 3

.

| Option | Arguments | Description |
|---|---|---|
| -S | enable \| disable | Enable or disable the respective version of SNMP |
| -u [n] | User Name | User Name |
| -c [n] | <Community> | Identify the group of units |
| -a [n] | <read \| write \| writeplus \| disable> | Set the access level |
| -n [n] | <IP or Domain Name> | The host's name or address |
| -ap [n] | <sha \| md5 \| none> | (Authentication Protocol)] |
| -pp [n] | <aes \| des \| none> | (Privacy Protocol)] |
| -ac [n] | <enable \| disable> | (Access) |
| -au [n] | <Nms Ip>] | [n] = Access Control # = 1,2,3, or 4) |

**Example:** To enable SNMP version 3, type:

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

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

**Error Message:** None

## snmptrap

**Access:** Super User, Administrator

**Description:** Enable or disable SNMP trap generation

**Parameters:**

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

**Error Message:** None

## system

**Access:** Super User, Administrator

**Description:** View and set the system name, the contact, the location and view up time as well as the date and time, the logged-on user, and the high-level system status P, N, A (see “CLI Home Screen” on page 7 for more information about system status).

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

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

```
system -l “Test Lab”
```

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

```
system -n “Rack 5”
```

## tcpip

**Access:** Super User, Administrator

**Description:** View and manually configure these network settings for the NMC:

| Option | Argument | Description |
|---|---|---|
| -i | <IP address> | Type the IP address of the unit, using the format *xxx.xxx.xxx.xxx* |
| -s | <subnet mask> | Type the subnet mask for the unit. |
| -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 unit will use. |
| -S | enable \| disable | Enable or disable IPv4. |

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

```
apc> tcpip
E000: Success
IP Address: 192.168.1.49
MAC Address: XX XX XX XX XX XX
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
Domain Name: example.com
Host Name: HostName
```

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

```
tcpip -i 10.179.229.50 -s 255.255.252.0 -g 10.179.228.1
```

## tcpip6

**Access:** Super User, Administrator

**Description:** Enable IPv6 and view and manually configure these network 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 unit. |
| -auto | enable \| disable | Enable the unit to automatically configure the IPv6 address. |
| -i | <IPv6 address> | Set the IPv6 address of the unit. |
| -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 unit, type `tcpip6` and press ENTER.

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

```
tcpip6 -i 2001:0:0:0:0:FFD3:0:57ab  -g <Valid IPv6 gateway>
```

## user

**Access:** Super User, Administrator

**Description:** Configure the user name, password, and inactivity timeout for each account types. You can't edit a user name, you must delete it and then create a new user. For information on the permissions granted to each account type, see "User Account Overview" on page 3.

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

**Example 1:** To change the Administrator user name to XYZ, type:

```
user -n XYZ
```

**Example 2:** To change the log off time to 10 minutes, type:

```
user -st 10
```

## userdflt

**Access:** Super User, Administrator

**Description:** Complimentary function to “user” establishing default user preferences.

There are two main features for the default user settings:

Determine the default values to populate in each of the fields when the Super User or Administrator-level account creates a new user. These values can be changed before the settings are applied to the system.

For remote users (user accounts not stored in the system that are remotely authenticated such as RADIUS) these are the values used for those that are not provided by the authenticating server. For example, if a RADIUS server does not provide the user with a temperature preference, the value defined in this section will be used.

**Parameters:**

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

**Error Message:** None

## web

**Access:** Super User, Administrator

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

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

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

**Parameters:**

| Option | Argument | Definition |
|---|---|---|
| -h | enable \| disable | Enable or disable access to the user interface for HTTP. |
| -s | enable \| disable | Enable or disable access to the user interface for HTTPS.<br><br>When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate. |
| -mp | SSL3.0 \| TLS1.0 \| TLS1.1 \| TLS1.2 | Specify the minimum HTTPS protocol to use. |
| -ph | <http port #> | Specify the TCP/IP port used by HTTP to communicate with the unit (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 unit (443 by default). The other available range is 5000–32768. |

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

```
web -S disable
```

**Example:**

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

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

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

**Error Message:** E000, E102

### whoami

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

**Description:** Provides login information on the current user.

**Parameters:** None

**Example:**

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

**Error Message:** `E000`

## xferINI

**Access:** Super User, Administrator

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

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

**Parameters:** None

**Example:**

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

**Error Message:** None

## xferStatus

**Access:** Super User, Administrator

**Description:** View the result of the last file transfer. See "Verifying Upgrades and Updates" on page 108 for descriptions of the transfer result codes.

**Parameters:** None

**Example:**

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

**Error Message:** E000

# Device Command Descriptions

### sysOutput

**Access:** Super User, Administrator, Device User

**Description:** Output measurements include each phase-to-phase voltage, each phase-to-neutral voltage, load and power supported by each phase, total power and the frequency.

**Parameters:** `none`

**Example:.**

```
apc> sysOutput
E000: Success

                     L1-2      L2-3      L3-1     Units
   Output Voltage    410       411       410      V

                     L1        L2        L3       Units
   Output Voltage    238       237       237      V
   Output Current    0.0       0.8       0.0      A

                     L1        L2        L3       Total     Units
   Output Power      0.0       0.0       0.0      0.04      kW
   ------------------------------------------------------------

   Frequency <Out>   50.0 Hz
```

**Error Message:** `E102`

## modStatus

**Access:** Super User, Administrator, Device User

**Description:** Display the module number, status, each breaker rating, load name, each breaker current and module power. To specify module, choose from the following options.

| Argument | Definition |
|---|---|
| <all> | Display the status of all Modules. |
| <module#> | Display the status of a selected Module. |

**Example 1:**

```
apc> modStatus 2
E000: Success
   Selected Module : 2
   Module Status   : Normal
                        L1        L2        L3
   Breaker Rating      20 A      20 A      20 A
   Breaker Position    Closed    Closed    Closed
   Breaker Current     0.0 A     0.0 A     0.0 A
   Percentage Current  0.0%      0.0%      0.0%
   Associated Cable    Cable 1   Cable 2   Cable 3
   Power               0.00 kW   0.00 kW   0.00 kW
```

**Example 2:**

```
apc> modStatus 1
E000: Success
   Selected Module : 1
   Module Not Installed
```

**Error Message:** E102

## cblStatus

**Access:** Super User, Administrator, Device User

**Description:** Display cable parameters of name, location, alarm status, total power, energy usage, usage reset date, alarm generation enable and threshold configurations on the module and cable selected

| Argument | Definition |
|---|---|
| <module#><cbl#> | View by module number and cable number.<br>module# = module of interest<br>cbl# = cable of interest (normally 1\|2\|3) |

**Example:** To view the status of a module cable, type:

```
apc> cblStatus 2 1
E000: Success

   Module 18 Cable 1

   Cable Name                  : Circuit 18a
   Location                    : Ckt Location 18a
   Alarm Status                : Normal
   Total Power                 : 0.00 kW
   Energy Usage                : 0.0 kW
   Last kWh Reset              : 04/08/2016

                      L1       L2       L3
   Breaker Rating     20 A     20 A     20 A
   Breaker Position   Closed   Closed   Closed
   Breaker Current    0.0 A    0.0 A    0.0 A
   Breaker Alarm      Disable  Disable  Disable

   Alarm Generation            : Disable
   Max <Critical> Threshold    : 90%
   Max Current Alarm           : Disable
   High <Warning> Threshold    : 80%
   High Current Alarm          : Disable
   Low <Warning> Threshold     : 20%
   Low Current Alarm           : Disable
   Min <Critical> Threshold    : 10%
   Min Current Alarm           : Disable
```

**Error Message:** E102

## cblName

**Access:** Super User, Administrator, Device User

**Description:** Configures the name of the cable selected module # and cable #.

| Argument | Definition |
|---|---|
| <module#><cbl#><br><name string> | Select the module# and cable#.<br>(Input String is a maximum of 20 characters and should be a valid string. Quotes are required if the string contains a space.) |

**Example:** To configure the name of a module cable, type:

```
apc> cblName 2 1 LoadNo-1
E000: Success

   Module 2 Cable 1
   Cable Name                    : LoadNo-1
   Location                      : Ckt Location 2a
   Alarm Status                  : Normal
   Breaker Rating                : 20 A
   Breaker Position              : Closed
   Breaker Current               : 0.0 A
   Total Power                   : 0.00 kW
   Energy Usage                  : 0.0 kWh
   Last kWh Reset                : 03/18/2016
```

**Error Message:** E102

## cblLoc

**Access:** Super User, Administrator, Device User

**Description:** Configure the cable location on a selected module.

| Argument | Definition |
|---|---|
| <module#><cbl#><br><location string> | Configures the location of the cable selected.<br>(Input String is a maximum of 20 characters and should be a valid string. Quotes are required if the string contains a space.) |

**Example:**

```
apc> cblLoc 2 1 RackNo-1
E000: Success

   Module 2 Cable 1

   Cable Name                          : LoadNo-1
   Location                            : RackNo-1
   Alarm Status                        : Normal
   Breaker Rating                      : 20 A
   Breaker Current                     : 0.0 A
   Total Power                         : 0.00 kW
   Energy Usage                        : 0.0 kWh
   Last kWh Reset                      : 03/18/2016
```

**Error Message:** E102

## cblAlrm

**Access:** Super User, Administrator, Device User

**Description:** Configure cable alarm enabled/disabled status.

| Argument | Definition |
|---|---|
| <all><enable\|disable> | Enables or disables the alarm generation of all cables. |
| <module#><cbl#><enable\|disable> | Enable or disable alarm generation by cable selected cbl# on a selected module# through the command.<br>module# = module of interest<br>cbl# = cable of interest (normally 1\|2\|3) |

**Example:**

```
apc> cblAlrm 2 1 enable
E000: Success

   Module 2 Cable 1

   Alarm Generation              : Enable
   Breaker Position Alarm<L1>    : Enable
   Max <Critical> Threshold      : 91%
   Max Current Alarm             : Enable
   High <Warning> Threshold      : 81%
   High Current Alarm            : Enable
   Low <Warning> Threshold       : 21%
   Low Current Alarm             : Enable
   Min <Critical> Threshold      : 11%
   Min Current Alarm             : Enable
```

**Error Message:** E102

## cblThrMx

**Access:** Super User, Administrator, Device User

**Description:** Configures cable maximum load alarm threshold and enabled/disabled status.Valid threshold values are 0-100% for ThrMx, ThrHi, ThrLo, and ThrMn.

| Argument | Definition |
|---|---|
| <all><enable \| disable> | Enable or disable max load alarm on all cables. |
| <module#><cbl#><enable \| disable> | Enable or disable max load alarm on cable selected by module and cable. |
| <all><thresh> | Configure the maximum load alarm threshold on all existing cables. |
| <module#><cbl#>thresh> | Configure maximum load alarm threshold on cables selected by module# and cbl#. |

**Example 1:** To enable a module cable maximum alarm threshold, type:

```
apc> cblThrMx 2 1 enable
E000: Success
   Module 2 Cable 1
   Alarm Generation                    : Enable
   Breaker Position Alarm<L1>          : Enable
   Max <Critical> Threshold            : 91%
   Max Current Alarm                   : Enable
   High <Warning> Threshold            : 81%
   High Current Alarm                  : Enable
   Low <Warning> Threshold             : 21%
   Low Current Alarm                   : Enable
   Min <Critical> Threshold            : 11%
   Min Current Alarm                   : Enable
```

**Example 2:** To configure a module cable maximum alarm threshold, type:

```
apc> cblThrMx 2 1 90
E000: Success
   Module 2 Cable 1
   Alarm Generation                    : Enable
   Breaker Position Alarm<L1>          : Enable
   Max <Critical> Threshold            : 90%
   Max Current Alarm                   : Enable
   High <Warning> Threshold            : 81%
   High Current Alarm                  : Enable
   Low <Warning> Threshold             : 21%
   Low Current Alarm                   : Enable
   Min <Critical> Threshold            : 11%
   Min Current Alarm                   : Enable
```

**Error Message:** `E102`

## cblThrHi

**Access:** Super User, Administrator, Device User

**Description:** Configure or enable/disable the cable high load alarm threshold and warning alarm. Valid threshold values are 0-100% for ThrMx, ThrHi, ThrLo, and ThrMn..

| Argument | Definition |
|---|---|
| `<all><enable \| disable>` | Enable or disable high load alarm on all cables. |
| `<module#><cbl#><enable \| disable>` | Enable or disable high load alarm on cable selected by module and cable. |
| `<all><thresh>` | Configure the high load alarm threshold on all existing cables. |
| `<module#><cbl#>thresh>` | Configure high load alarm threshold on cables selected by module# and cbl#. |

all = all cables
module# = module of interest
cbl# = cable of interest (normally 1|2|3)
thresh = % rated load

**Example:** To enable a module cable high load alarm threshold, type:

```
apc> cblThrHi 2 1 enable
E000: Success

   Module 2 Cable 1

   Alarm Generation               : Enable
   Breaker Position Alarm<L1>     : Enable
   Max <Critical> Threshold       : 90%
   Max Current Alarm              : Enable
   High <Warning> Threshold       : 81%
   High Current Alarm             : Enable
   Low <Warning> Threshold        : 21%
   Low Current Alarm              : Enable
   Min <Critical> Threshold       : 11%
   Min Current Alarm              : Enable
```

**Error Message:** `E102`

## cblThrLo

**Access:** Super User, Administrator, Device User

**Description:** Configure the cable low load alarm threshold and enabled/disabled status. Valid threshold values are 0-100% for ThrMx, ThrHi, ThrLo, and ThrMn.

| Argument | Definition |
|---|---|
| `<all><enable \| disable>` | Enable or disable low load alarm on all cables. |
| `<module#><cbl#><enable \| disable>` | Enable or disable low load alarm on cable selected by module and cable. |
| `<all><thresh>` | Configure the low load alarm threshold on all existing cables. |
| `<module#><cbl#>thresh>` | Configure low load alarm threshold on cables selected by module# and cbl#. |

all = all cables
module# = module of interest
cbl# = cable of interest (normally 1|2|3)
thresh = % rated load

**Example:** To enable the status of a module cable low load alarm threshold, type:

```
apc> cblThrLo 2 1 enable
E000: Success

   Module 2 Cable 1

   Alarm Generation               : Enable
   Breaker Position Alarm<L1>     : Enable
   Max <Critical> Threshold       : 90%
   Max Current Alarm              : Enable
   High <Warning> Threshold       : 81%
   High Current Alarm             : Enable
   Low <Warning> Threshold        : 21%
   Low Current Alarm              : Enable
   Min <Critical> Threshold       : 11%
   Min Current Alarm              : Enable
```

**Error Message:** `E102`

## cblThrMn

**Access:** Super User, Administrator, Device User

**Description:** Configure the minimum load alarm threshold and enabled/disabled status on the cable(s). Valid threshold values are 0-100% for ThrMx, ThrHi, ThrLo, and ThrMn.

| Argument | Definition |
|---|---|
| `<all><enable \| disable>` | Enable or disable minimum load alarm on all cables. |
| `<module#><cbl#><enable \| disable>` | Enable or disable minimum load alarm on cable selected by module and cable. |
| `<all><thresh>` | Configure the minimum load alarm threshold on all existing cables. |
| `<module#><cbl#>thresh>` | Configure minimum load alarm threshold on cables selected by module# and cbl#. |

all = all cables
module# = module of interest
cbl# = cable of interest (normally 1|2|3)
thresh = % rated load

**Example:** To enable the status of a module cable minimum load alarm threshold, type:

```
apc> cblThrMn 2 1 enable
E000: Success

   Module 2 Cable 1

   Alarm Generation               : Enable
   Breaker Position Alarm<L1>     : Enable
   Max <Critical> Threshold       : 90%
   Max Current Alarm              : Enable
   High <Warning> Threshold       : 81%
   High Current Alarm             : Enable
   Low <Warning> Threshold        : 21%
   Low Current Alarm              : Enable
   Min <Critical> Threshold       : 11%
   Min Current Alarm              : Enable
```

**Error Message:** `E102`

## cblBrkrPos

**Access:** Super User, Administrator, Device User

**Description:** Configure the cable breaker position alarm enabled/disabled status.

| Argument | Definition |
|---|---|
| `<all><enable \| disable>` | Enable or disable the breaker position alarm of all existing cables. |
| `<module#><cbl#><enable \| disable>` | Enable or disable the breaker position alarm by target cable selected through the command.<br>**NOTE:** If the selected cable has more than one breaker, then the command will prompt for selecting the breaker. |

all = all cables
module# = module of interest
cbl# = cable of interest (normally 1|2|3)

**Example:** To enable the status of a cable breaker position, type:

```
apc> cblBrkrPos 2 1 enable
E000: Success

   Module 2 Cable 1

   Alarm Generation               : Enable
   Breaker Position Alarm<L1>     : Enable
   Max <Critical> Threshold       : 90%
   Max Current Alarm              : Enable
   High <Warning> Threshold       : 81%
   High Current Alarm             : Enable
   Low <Warning> Threshold        : 21%
   Low Current Alarm              : Enable
   Min <Critical> Threshold       : 11%
   Min Current Alarm              : Enable
```

**Error Message:** `E102`

## cblRstkWh

**Access:** Super User, Administrator, Device User

**Description:** Reset the usage and usage date on the cable selected by module number and cable number.

| Argument | Definition |
|---|---|
| <module#><cbl#> | Reset usage and usage date on the target cable selected through the command.<br>module# = module of interest<br>cbl# = cable of interest (normally 1\|2\|3) |

**Example:** To view the usage and date of a cable, type:

```
apc> cblBrkrPos 2 1
E000: Success

   Module 2 Cable 1

   Cable Name                  : LoadNo-1
   Location                    : RackNo-1
   Alarm Status                : Critical
   Breaker Rating              : 20 A
   Breaker Position            : Closed
   Breaker Current             : 0.0 A
   Total Power                 : 0.00 kW
   Energy Usage                : 0.0 kW
   Last kWh Reset              : 03/10/2016
```

**Error Message:** E102

## getAlarm

**Access:** Super User, Administrator, Device User

**Description:** Displays the active alarms in the system.

| Argument | Definition |
|---|---|
| <all \| critical \| warning> | <all> Display all active (critical + warning) alarms in the system.<br><critical> Display all active critical alarms in the system.<br><warning> Display all active warning alarms in the system. |

**Example:**

```
apc> getAlarm all
E000: Success

8 Critical Alarms Present:
-----------------------------------

   MDS: Module Breaker Open Alarm Mod[8].L1 Circuit 8a
   MDS: Module Breaker Open Alarm Mod[7].L1 Circuit 7a
   MDS: Module Breaker Open Alarm Mod[19].L1 Circuit 19a
   MDS: Module Breaker Open Alarm Mod[8].L2 Circuit 8a
   MDS: Module Breaker Open Alarm Mod[19].L2 Circuit 19a
   MDS: Module Breaker Open Alarm Mod[8].L3 Circuit 8a
   MDS: Module Breaker Open Alarm Mod[7].L3 Circuit 7c
   MDS: Module Breaker Open Alarm Mod[19].L3 Circuit 19a

No Warning Alarms Present
```

**Error Message:** `E102`

## mfactElec

**Access:** Super User, Administrator, Device User

**Description:** Displays nominal line-to-neutral voltage and maximum panel current.

**Example:**

```
apc> mfactElec
E000: Success


   Nominal Voltage          : 230 V/4-Wire
   Maximum Current Rating   : 400 A
```

**Error Message:** `E102`

## mfactMeter

**Access:** Super User, Administrator, Device User

**Description:** Displays model number, serial number, date of manufacture and firmware revision for each metering device in the PDU.

**Parameters:** None

**Example:**

```
apc> mfactMeter
E000: Success


    Metering Segment 1
    ------------------------
    Serial Number         : 0524950609505658
    Firmware Revision     : 01.07
    Model Number          : 0P2495
    Manufacture Date      : 12112008
    Hardware Revision     : 1050G-E9
```

**Error Message:** `E102`

## mfactMod

**Access:** Super User, Administrator, Device User

**Description:** Displays factory details for power distribution modules.

| Argument | Definition |
|---|---|
| `<all \| module#>` | <all> display model number, serial number, date of manufacture, and number of attached cables for each module in the PDU.<br><module#> display above information plus cable information breaker rating, length, connector style and available voltage, for any cables attached to the module.<br>all = all modules<br>module# = module of interest |

**Example:**

```
apc> mfactMod 2
E000: Success


   Model Number                : PDM1320IEC-3P-1
   Serial Number               : 5F1038P00115
   Manufacture Date            : 09/20/2016
   Whips Count                 : 3
                        L1             L2             L3
   Breaker Rating       20 A           20 A           20A
                        Cable1         Cable2         Cable3
   Length               2.6m <8.5ft>   3.8m <12.5ft>  5.0m <16.4ft>
   Connector Style      2.6m <8.5ft>   IEC309-3W      IEC309-3W
   Available Voltage    230 V          230 V          230 V
```

**Error Message:** `E102`

### modbus

**Access:** Super User, Administrator

**Description.** View and configure modbus parameters.

| Option | Argument | Definition |
|---|---|---|
| -a | <enable \| disable> (Modbus status) | Enable or disable Modbus Serial.[1] |
| -br | | Displays the current baud rate. |
| | <9600 \| 19200> (baud rate) | Set the baud rate in bits per second.[1] |
| -s | <1 - F7> (slave address in hex) | Set the hexidecimal Modbus slave address. [1] |
| -rDef | | Reset the Modbus configuration to default. |
| -tE | <enable \| disable> (Modbus status) | Enable or disable Modbus TCP. [2] |
| -tP | | Specify the Modbus TCP port number. [2] |
| [1] Modbus Serial only<br>[2] Modbus TCP only | | |

**Example:**

```
apc> modbus
E000: Success
Slave Address = 0x1
Status = ENABLED
Baud Rate = 9600
TCP Status = DISABLED
TCP Port Number = 502
```

**Error Message:** E102

Note: Modbus RTU is disabled by default. Modbus RTU is disabled when "Reset to Defaults" action is performed.

# The Web Interface

# Supported Web browsers

Use Microsoft® Internet Explorer (IE) 7.x and higher (Windows operating systems) or Mozilla Firefox 3.0.6 or higher (all operating systems) to access the NMC through its Web interface. Other commonly available browsers may work but have not been fully tested by APC. The unit cannot work with a proxy server. Before using a Web browser to access its Web interface, do one of the following:

- Configure the Web browser to disable the use of a proxy server for the unit.
- Configure the proxy server so that it does not proxy the specific IP address of the unit.

# Log On

## Overview

Use the DNS name or System IP address of the unit for the URL address of the Web interface. Use your case-sensitive user name and password to log on.

The default user name differs by account type:

- **apc** for the Super User
- **device** for a Device User
- **readonly** for a Read-Only User

The Super User or an Administrator created by the Super User should define the user names, passwords, and other account characteristics for the lower tier users.

If you are using HTTPS (SSL/TSL) as your access protocol, your logon credentials are compared with information in a server certificate. If the certificate was created with the APC Security Wizard, and an IP address was specified as the common name in the certificate, you must use an IP address to log on to the unit. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

## URL address formats

Type the DNS name or IP address of the unit in the URL address field of the Web browser and press ENTER. When you specify a non-default Web server port in Internet Explorer, you must include http:// or https:// in the URL.

**Common browser error messages at log-on.**

| Error Message | Browser | Cause of the Error |
|---|---|---|
| “This page cannot be displayed.” | Internet Explorer | Web access is disabled, or the URL was not correct |
| “Unable to connect.” | Firefox | |

**URL format examples.**

- For a DNS name of Web1:
  - `http://Web1` if HTTP is your access mode
  - `https://Web1` if HTTPS (HTTP with SSL) is your access mode
- For a System IP address of 139.225.6.133 and the default Web server port (80):
  - `http://139.225.6.133` if HTTP is your access mode
  - `https//139.225.6.133` if HTTPS (HTTP with SSL) is your access mode
- For a System IP address of 139.225.6.133 and a non-default Web server port (5000):
  - `http://139.225.6.133:5000` if HTTP is your access mode
  - `https://139.225.6.133:5000` if HTTPS (HTTP with SSL) is your access mode

For a System IPv6 address of 2001:db8:1::2c0:b7ff:fe00:1100 and a non-default Web server port (5000):
`http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` if HTTP is your access mode

# Web Interface Features

Read the following to familiarize yourself with basic Web interface features for your unit.

## Tabs

In addition to the **Home** page, the following tabs are displayed. Click on a tab to display the options:

- **Home:** Appears when you log on (This is the default tab when you log on. To change the login page to a different page, click on the green pushpin at the top right side of the browser window while on the desired page). View active alarms, the load status of the unit, and the most recent device events. For more information, see “The Home Page” on page 58.
- **Status:** Gives the user the status of the **Device** and **Network**. The **Device** tab covers the status of modules, system output, and an overview. **Network** tab covers just the network. See “The Status Tab” on page 59 for more information.
- **Control:** The **Control** tab covers **Security** and **Network**. Much more information is covered under each of these tabs and will be described in “The Control Tab” on page 61.
- **Configuration**: The **Configuration** tab covers **Device**, **Security**, **Network**, **Notification**, **General** and **Logs**. Much more information is covered under each of these tabs and will be described in the “The Configuration Tab” on page 63.
- **Tests:** The **Tests** tab covers **Network**. The **Network** tab covers LED Blink.
- **Logs:** The **Logs** section covers: **Event**, **Data**, and **Firewall**. The **Event** and **Data** tabs cover more information which will be further discussed later in the “Logs Tab” on page 92.
- **About:** The **About** section covers **Device**, **Network** and **Support**, which will be further discussed later in “The About Tab” on page 97.

### Device status icons

One or more icons and accompanying text indicate the current operating status of the unit.

**Critical**: A critical alarm exists, which requires immediate action.

**Warning**: An alarm condition requires attention and could jeopardize data or equipment if its cause is not addressed.

**No Alarms Present:** The unit is operating normally.

At the upper right corner of every page, the web interface displays the same icons currently displayed on the **Home** page to report the status of the unit:

- The **No Alarms** icon if no alarms exist.
- One or both of the other icons (**Critical** and **Warning**) if any alarms exist, and after each icon, the number of active alarms of that severity.

### Quick Links

At the lower left on each page, there are three configurable links. You can also click on the Configuration tab, from the menu, click on General and select Quick Links from the menu that opens.

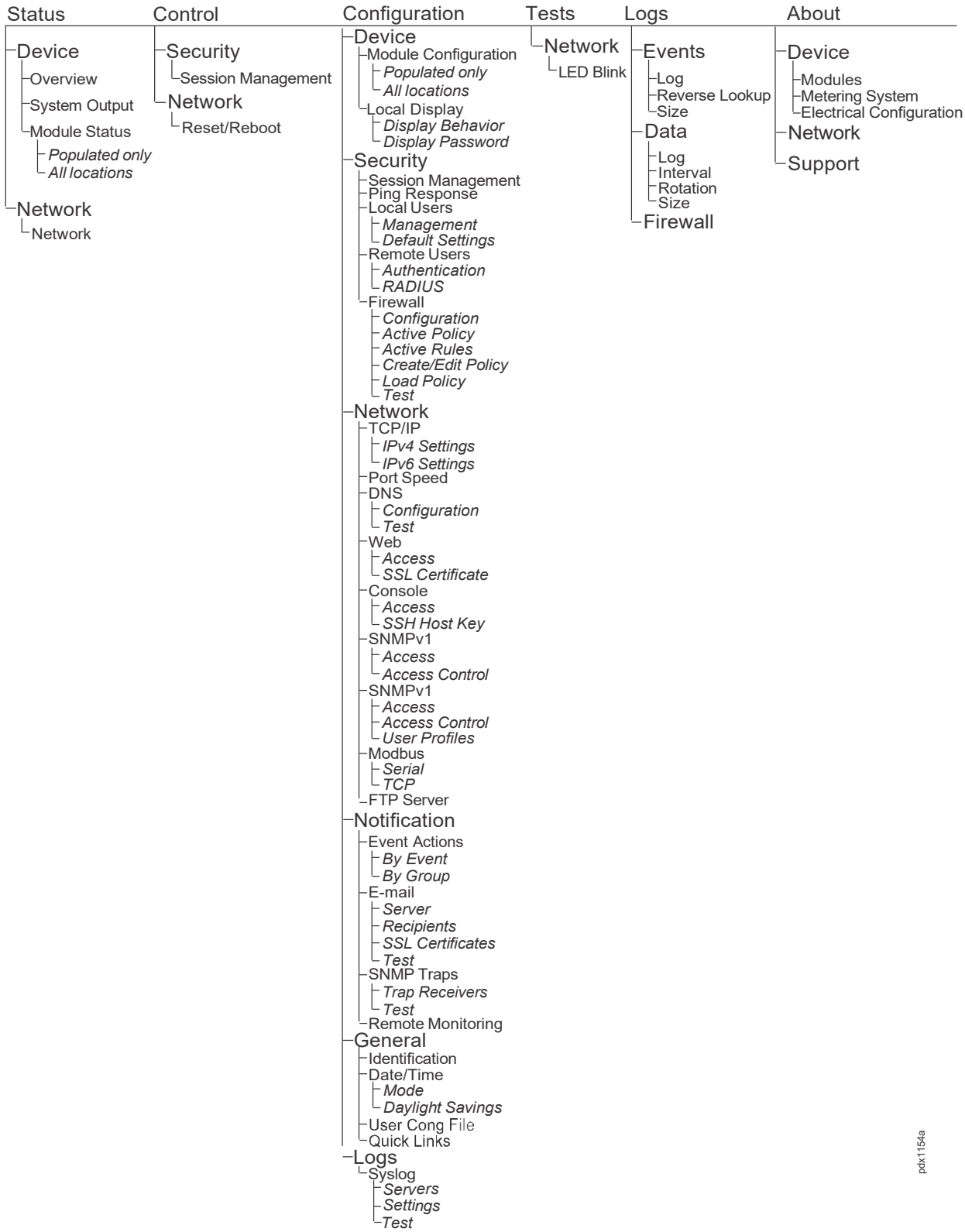
- **Link 1**: The home page of the APC Web site
- **Link 2**: **Testdrive Demo** provides demonstrations of APC Web-enabled products.
- **Link 3**: Information on APC Remote Monitoring Services.

Located in the upper right hand corner of each page:

- User name (click to change user preferences)
- Language (if available, click to change language preference)
- Log Off (click to log the current user off of the web interface)
- Help (click to view help contents)

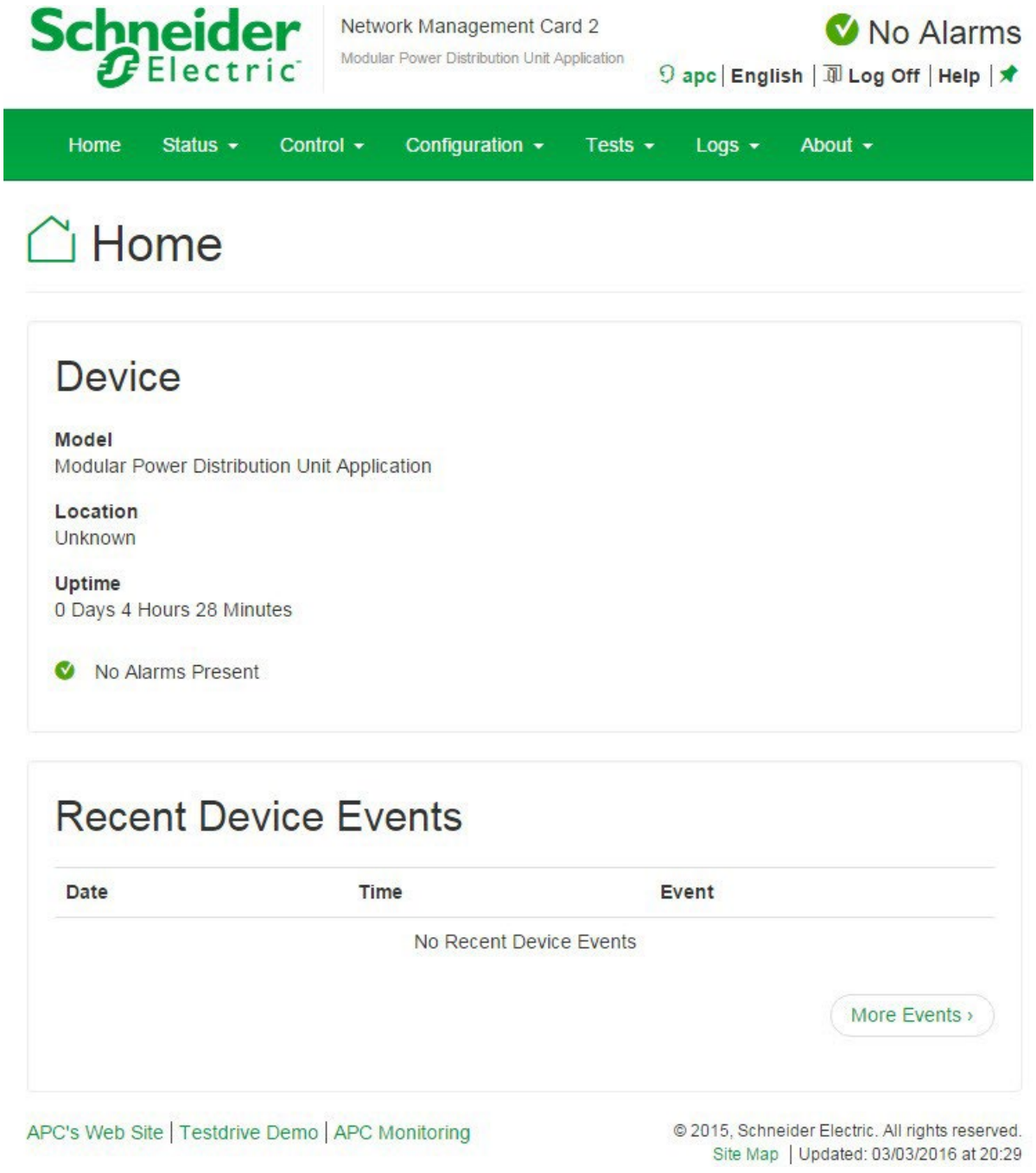
(click to set the current web page to be the log in home page)
Example:
**Log In Home:** To make any screen the “home” screen (i.e., the screen that displays first when you log on), go to that screen, and click the icon in the top right corner.
Click to revert to displaying the Home screen when you log on.

# Device Menu Tree



# The Home Page

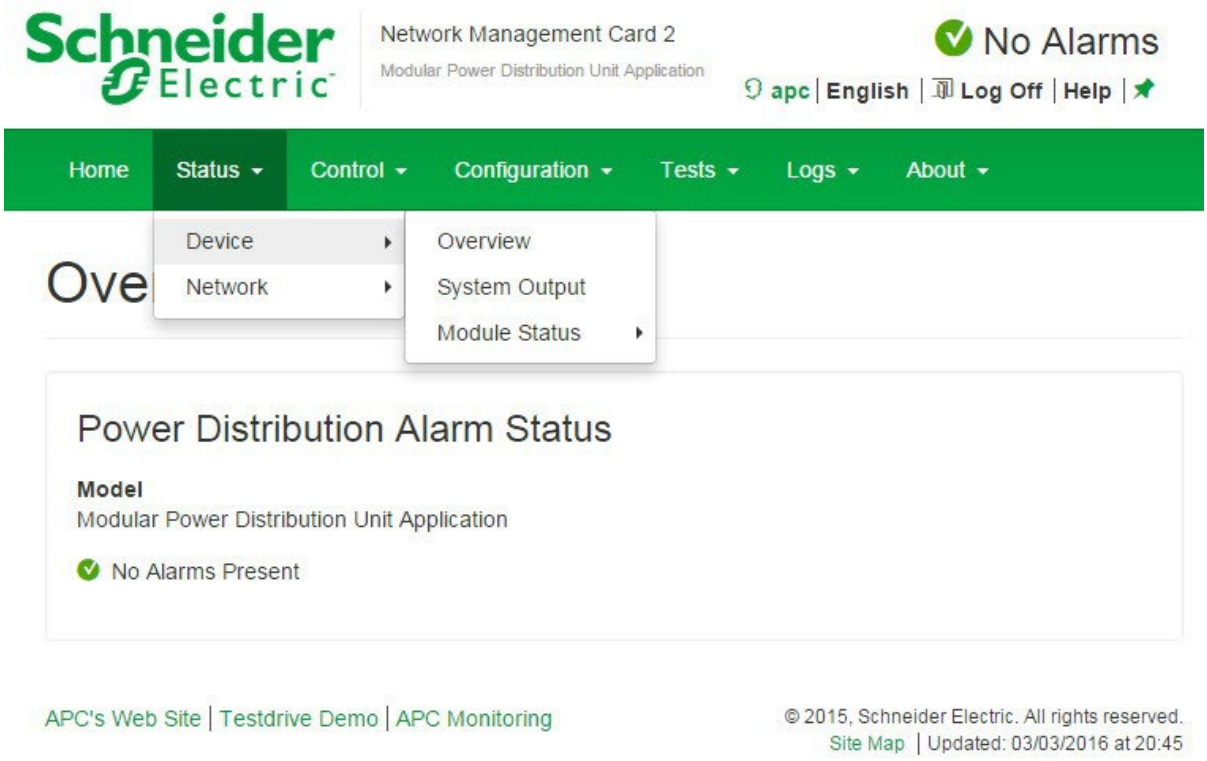
The **Home** page contains the following information: Active Alarms and Recent Device Events. Active Alarms will show if any alarms exist. If no alarms exist, a green check mark with the words ”No Alarms Present” will show. To see the Device Status select the **More** link at the bottom of the list. The Recent Device Events box will list the five most recent device Events bythe device by Date, Time and Event.



# The Status Tab

Use the **Status** tab to:

- Select **Device** to view the status of the unit and its modules.
  - View the Alarm Status of the unit
  - View the power output of the unit
  - View the status of the Modules by location or by all
- Select **Network** to view the current IPv4, IPv6 settings, the Domain Name System Status and Port Speed



## View the Network Status

**Path: Status > Network > Network**

The **Network** screen displays information about your network.

## Current IPv4 Settings

**System IP.** The IP address of the unit.

**Subnet Mask.** The IP address of the sub-network.

**Default Gateway.** The IP address of the router used to connect to the network.

**MAC Address.** The MAC address of the unit.

**Mode.** How the IPv4 settings are assigned: **Manual**, **DHCP**, or **BOOTP**.

**DHCP Server.** The IP address of the DHCP server. This is only displayed if **Mode** is **DHCP**.

**Lease Acquired.** The date/time that the IP address was accepted from the DHCP server.

**Lease Expires.** The date/time that the IP address accepted from the DHCP server expires and will need to be renewed.

## Current IPv6 Settings

**Type.** How the IPv6 settings are assigned.

**IP Address.** The IP address of the unit.

**Prefix Length.** The range of addresses for the sub-network.

## Domain Name System Status

**Active Primary DNS Server.** The IP address of the primary DNS server.

**Active Secondary DNS Server.** The IP address of the secondary DNS server.

**Active Host Name.** The host name of the active DNS server.

**Active Domain Name (IPv4/IPv6).** The IPv4/IPv6 domain name that is currently in use.

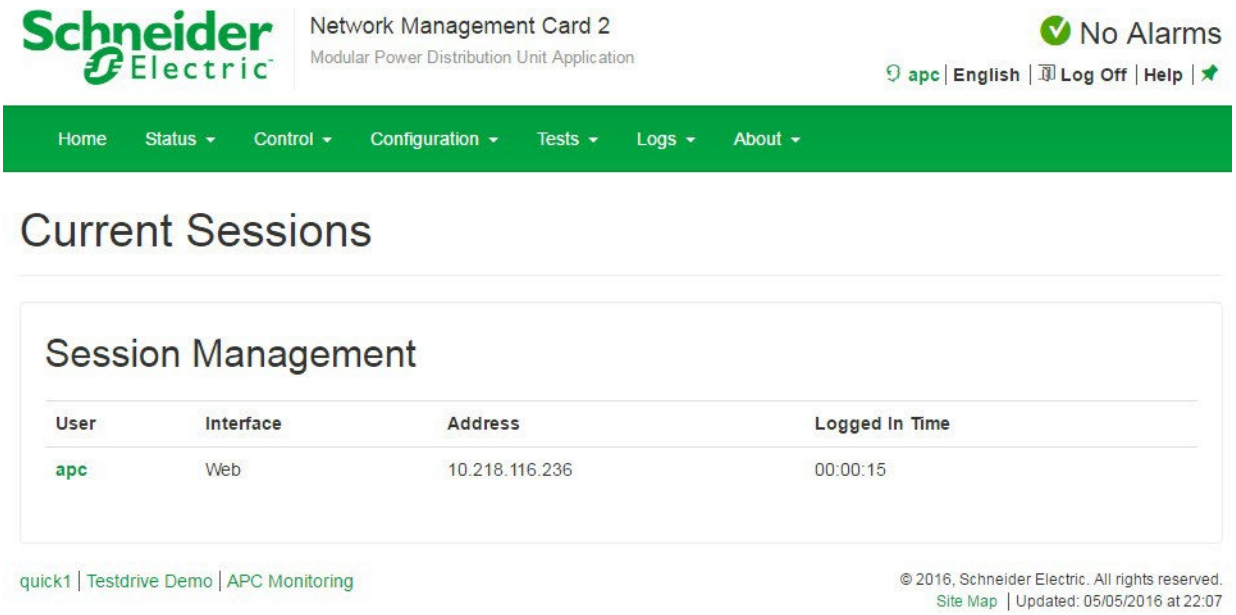
**Active Domain Name (IPv6).** The IPv6 domain name that is currently in use.

## Ethernet Port Speed

**Current Speed.** The current speed assigned to the Ethernet port.

# The Control Tab

The **Control** menu options enable you to take immediate actions affecting active user management and the security of your network.




## Session Management

**Path: Control > Security > Session Management**

The **Session Management** menu displays all active users currently connected to the unit. To view Information about a given user, click on their user name.

Click on a user name to open the **Session Details** screen. The Session Details screen displays basic information about the user including the interface into which they are logged, their IP address, authentication, and time logged in.

There is a **Terminate Session** button on the Session Details screen. The selected user's session can be terminated by clicking the Terminate Session button.

## Reset the Network Interface

**Path: Control > Network > Reset/Reboot**

This menu gives you the option to reset and reboot various components of the network interface. Users have the option to **Reboot Management Interface**,

**NOTE: Rebooting the Management Interface** only restarts the unit's Network Management Interface. It does not affect the ON/OFF status of the unit.

| Parameters | Description |
|---|---|
| Reboot Management Interface | Restarts the network interface of the device without turning off and restarting the unit. |
| Reset All | Clear the **Exclude TCP/IP** checkbox to reset all configuration values; mark the **Exclude TCP/IP** checkbox to reset all values except TCP/IP. |
| Reset Only | (Resetting may take up to a minute) Options include:<br>**TCP/IP settings**: Set TCP/IP Configuration to **DHCP & BOOTP**, its default setting, request requiring that the NMC receive its TCP/IP settings from a DHCP or BOOTP server. See "View the result of the test DNS in the Last Query Response field."<br>**Event configuration**: Reset all changes to event configuration, by event and by group, to their default settings. |

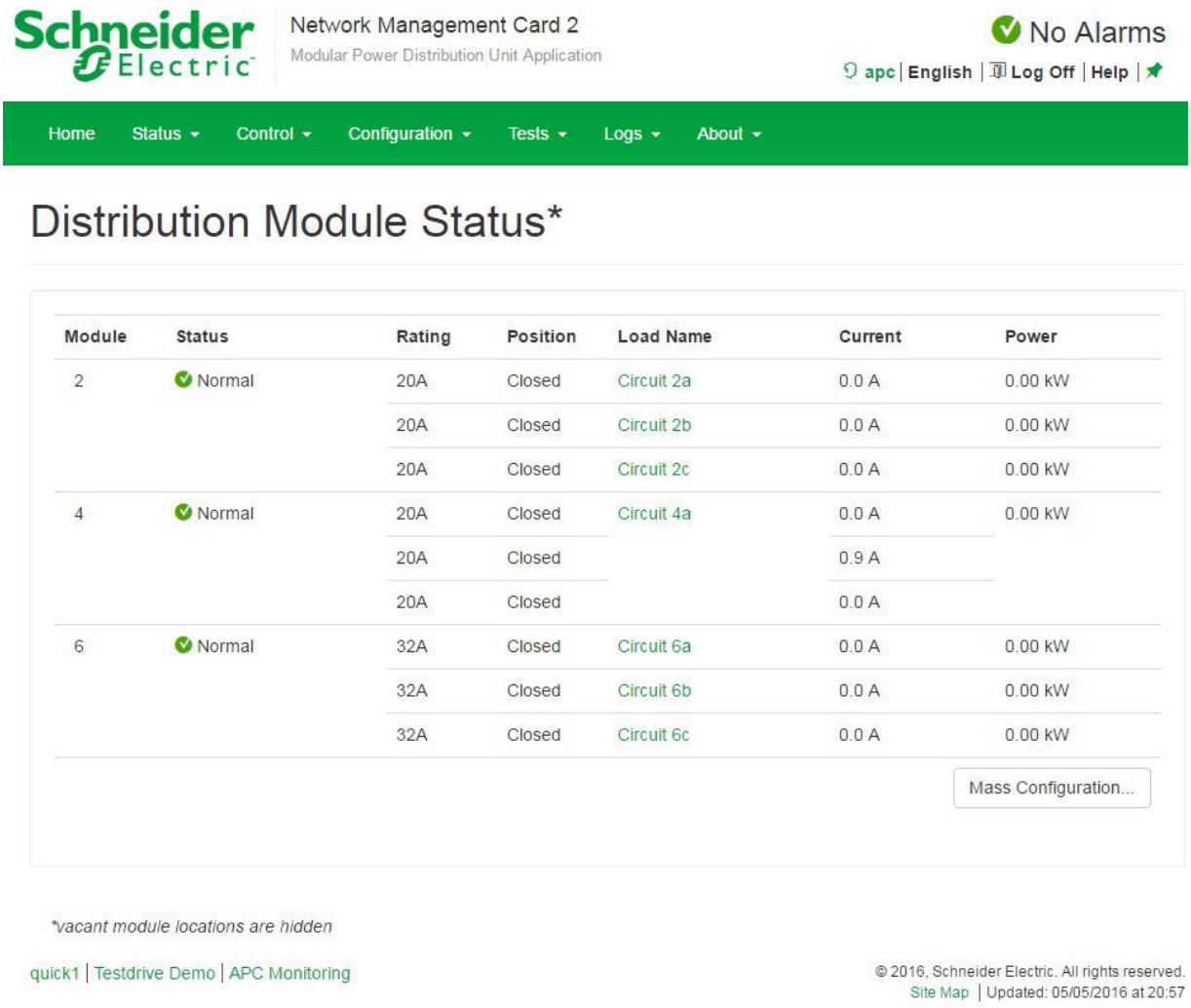
# The Configuration Tab

Under the Configuration tab, several menu options are available to make changes to the unit:

- Device
- Security
- Network
- Notification
- General
- Logs

## Device

**Path: Configuration > Device > Module Configuration**



Distribution Module Status can be shown **Populated Only** or by **All Locations**. Selecting **All Locations** will include vacant module locations on the status screen.

The Status details include:

- Module: The physical location of this distribution module in the system.
- Configuration: The status of the modules.
- Rating: The ampere rating of the breaker(s) within the module. Three ratings are shown, one for each module breaker (L1, L2, L3).
- Position: The operational state of the module breaker. Closed means that the circuit can receive operating voltage. Open represents a breaker that is off. Breakers can be opened and closed manually, but they may also be tripped open due to a short circuit or overload.
- The Module's Load Name, Current, and Power are shown on each page.

**Quick status icons.** Color-coded icons show the status of the Modules:

- Red: The Module is causing one or more critical alarms.
- Yellow: The Module is causing one or more warning alarms.
- Gray: The Module is not influencing the status of the unit or is not installed.
- Green: The unit is operating normally.

To configure a selected module: You can open a selected module's configuration page by clicking on its Load Name on the Populated Only status page. The page will show:

- Name: To configure the name of the load equipment attached to this distribution cable, enter a name (up to 20 characters). If no name is configured, the default value is displayed.
- Location: To configure the location of the load equipment attached to this distribution cable, click the device's name, and enter a location (up to 20 characters). If no location is configured, Unknown is displayed.
- Alarm Status: The operational status of this distribution cable, Critical (device requires immediate attention), Warning (attention required), or Normal.
- Total Power: The total power being drawn by the load equipment attached to this distribution cable.
- Energy Usage: The total energy, in kilo-watt hours (kWh), that has been consumed by the load equipment attached to this distribution cable since the reset date. To reset this value, click Reset kWh link, and press the Apply button on the confirmation screen.
- Date of kWh Reset: The date that the energy usage was reset for this distribution cable.
- Alarm Generation: A check in this check box enables all alarms for this distribution cable.
- Module Breaker Table: The table shows the status of all the module breakers that are associated with this distribution cable. Each line in the table defines on breaker. There can be up to three breakers per module meaning there can be up to three lines per table.
- Breaker: The breaker within the module. The indications L1, L2 and L3 match up with the markings on the front of the distribution module.
- Rating: The ampere rating of this breaker within the module.
- Position: The operational state of the module breaker. A position of closed means that the circuit can receive operating voltage. A position of open represents a breaker that is off. The breaker may have been opened manually, or tripped due to a short circuit or overload.

- Position Alarm: A check in this check box enables breaker open alarms for this module breaker. Typically this check box would be left unchecked to disable alarms for breakers that are intentionally left open.
- Current: The load current of this breaker in amps.
- Percent: The load current of this breaker expressed as a percentage of the breaker rating.
- Load Alarms: Load alarm thresholds allow you to be notified when the load for a distribution cable is outside its normal operating range. Individual load alarms maybe enabled/disabled by checking/un-checking the check box next to the threshold. To configure load alarm threshold values for the distribution cable, click Thresholds. On the threshold page, enter the minimum, low, high, maximum, values for loading, and click Apply to save your changes.

**Mass Configuration.** All modules can be configured at the same time by clicking on **Mass Configuration** at the bottom right of either the **Populated Only** or by **All Locations** pages. Alarm generation and current threshold settings are selected on this page.

- Alarm Generation: Threshold and position violations will only generate alarms when this setting is enabled
- Maximum Threshold: Load current above this threshold will generate a critical alarm.
- High Threshold: Load current above this threshold will generate a warning alarm.
- Low Threshold: Load current below this threshold will generate a warning alarm.
- Minimum Threshold: Load current below this threshold will generate a critical alarm.
- Breaker Position: Generate an alarm when the breaker is tripped

Click on **Apply to All Modules** at the bottom of the page to enable the selections.

**Module Current Thresholds .** Module current thresholds allow you to be notified when the loading for a distribution cable is outside its normal operating range. Alarm generation maybe enabled, disabled or left unchanged for any threshold by toggling the corresponding radio button.

To adjust the minimum, low, high, and maximum values for loading, first select the "Set thresholds" radio button. Then enter threshold values as percentages.

- Maximum Threshold: Load current above this threshold will generate a critical alarm.
- High Threshold: Load current above this threshold will generate a warning alarm.
- Low Threshold: Load current below this threshold will generate a warning alarm.
- Minimum Threshold: Load current below this threshold will generate a critical alarm.

**NOTE:** System events are not visible from the front panel display, and therefore will never cause the light to illuminate.

**Path: Configuration > Device > Local Display**

The **Local Display** page allows you to change the display parameters of the display interface of the unit.

**Display Behavior.** The Display Behavior page shows:

- The Display Type on the unit - The hardware revision number
- The Check Log Light - Choose alarm level you want from Informational, Critical, and Warning. You can also choose to Disable the Check Log Light.
- Local Alarm Beeper - Check the box to Enable the beeper on the unit.

Select **Apply** to Save your changes or **Cancel** to void your changes before you leave the page.

**Display Password.** You can change your password on this page.

- New Password - Enter the new password to log into the display interface of the unit
- Confirm Password - Confirm the new password
- Password Timeout - Change the password timeout interval (in minutes). This is the amount of time you have before the system logs you out after there is no activity through the display interface.

## Security

**Path: Configuration > Security**

### Session Management

**Allow Concurrent Logins.** Enabling **Allow Concurrent Logins** means that two or more users can log on at the same time. Each user has equal access and each interface (HTTP, FTP, telnet console, serial console (CLI), etc.) counts as a logged-in user.

**Remote Authentication Override:** Radius storage of passwords on a server is supported. However, if you enable this override, the unit will allow a local user to log on using locally stored password on the unit. See also “Local Users” and “Remote Users authentication”.

### Ping Response

Select the Enable check box for **IPv4 Ping Response** to allow the unit to respond to network pings. Clear the check box to disable an unit response. This does not apply to IPv6.

### Local Users

**Management.** Allows the Super User (or Administrator created by the Super User) to set user access for other users on the network.

- Set the case-sensitive user name and password for each account. 10 characters maximum for user names and 32 characters for passwords. Blank passwords are not allowed.
- Levels of access are protected by user name and password requirements. During authentication, the user's credentials are compared against the Local User Database and/or are validated against a RADIUS server (depending on configuration). If valid, access with appropriate permissions is granted.
  - An Administrator can use all the menus in the Web interface. The default user name is **apc**.
  - The default user name for the Device User is **device**. A Device User can access only the device related menus authorized by the Super User or Administrator.
  - A Read-Only User has only Web interface access. The same menus as Device User are visible but no changes can be made. Links to configuration options are visible but disabled. Event and data logs display no button to clear the log. The default user name is **readonly**.
  - A Network Only User has read-write access to the network related menus only

- Click on **Add User** to add a user. On the resulting **User Configuration** screen, you can add a user and withhold access by clearing the **Access** check box. User names and passwords are case-sensitive. The maximum length for both the name and password is 64 bytes, with less for multi-byte characters. You have to enter a password. Blank passwords, (passwords with no characters) are not allowed.

  **NOTE:** Values greater than 64 bytes in Name and Password might get truncated. To change an Administrator/Super User setting, you must enter all three password fields.

- Use **Session Timeout** to configure the time (3 minutes by default) that the UI waits before logging off an inactive user. If you change this value, you must log off for the change to take effect.

  **NOTE:** This timer continues to run if a user closes the browser window without first logging Off by clicking **Log Off** at the upper right. Because that user is still considered tobe logged on, no user can log on until the time specified as **Minutes of Inactivity** expires. For example, with the default value for **Minutes of Inactivity**, if a user closes the browser window without logging off, no user can log on for 3 minutes.
- **Serial Remote Authentication Override:** By selecting this option, you can bypass RADIUS by using the serial console (CLI) connection. This screen enables it for the selected user, but it must also be enabled globally to work, (through the “Session Management” screen).

**Default 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.

- **Default User Settings:**
  – Access: Put a check in the Enable box to allow access.
  – User Type: Select the user type from the dropdown menu.
  – User Description: Type the user Description in the box.
  – Session Timeout: Select from 1 to 60 seconds.
  – Bad Login Attempts. Set the number of failed login attempts the user can have. Select from 0 to 99 attempts. 0= unlimited.
- **User Preferences:** This option is enabled by default.
  – **Event Log Color Coding:** Mark the checkbox to enable color-coding of alarm text recorded in the event log. System event entries and configuration change entries do not change color.

| Text Color | Alarm Severity |
|---|---|
| Red | **Critical**: A critical alarm exists, which requires immediate action. |
| Orange | **Warning**: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed. |
| Green | **Alarm Cleared**: The conditions that caused the alarm have improved. |
| Black | **Normal**: No alarms are present. The Modular PDU and all connected devices are operating normally. |

  – **Change the default temperature scale:** Select the temperature scale, **US Customary** (Fahrenheit) or **Metric** (Celsius), in which to display all temperature measurements in this user interface.
  – **Export Log Format:** Configure which format the event log should be displayed in when exported (downloaded). Tab (default) allows fields to be tab-delimited whereas CSV is comma-separated.
  – **Date Format:** Select the numerical format in which to display all dates in this user interface. In the selections, 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.

- **Password Requirements:**
  - **Strong Passwords:** Configure whether new passwords created for user accounts will require additional rules such as at least one lowercase character, one uppercase character, one number, and one symbol.
  - **Password Policy:** Select the duration (in days) to which the user will be required to change their password. A value of 0 days disables this feature (by default).

### Authentication and Remote Users

**Path: Configuration > Security > Remote Users**

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

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

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

Select one of the following:

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

| | |
|---|---|
| **RADIUS** | You can set up the device to use a RADIUS server to authenticate remote users. Specify up to two properly configured RADIUS servers. To add a server, click Add Server. To modify an existing server, click the server's name. |
| **RADIUS Server** | The name or IP address of the RADIUS server. |
| **Port** | The port (1812 by default) that the RADIUS server listens on.<br>**NOTE:** You can change the port setting to any unused port from 5000 to 32768. |
| **Secret** | The shared secret between the RADIUS server and the NMC. |
| **Reply Timeout** | The time in seconds that the unit waits for a response from the RADIUS server. |
| **Test Settings** | Enter the Administrator user name and password to test the RADIUS server path that you have configured. |
| **Skip Test and Apply** | Do not test the RADIUS server path. |
| **Switch Server Priority** | Change which RADIUS server will authenticate users if two configured servers are listed and **RADIUS, then Local Authentication** or **RADIUS Only** is the enabled authentication method. |

**Summary of the Configuration Procedure.**

You must configure your RADIUS server to work with the PDU. For examples of the RADIUS users file with the Vendor Specific Attributes (VSAs) and an example of an entry in the dictionary file on the RADIUS server, See the Security Handbook (available online at **www.apc.com**).

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

**Configure a RADIUS Server on UNIX® with Shadow Passwords:**

Two methods can be used to authenticate users:

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

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

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

– Add user names and attributes to RADIUS "user" file. Verify passwords against `/etc/passwd`. The following example is for users `bconners` and `thawk`:

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

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

## Firewall

**Path: Configuration > Security > Firewall**

A configurable network firewall is provided. The firewall can allow or deny network traffic to and from the device, based on user-configured rules that are ordered by priority. In the Web User Interface, you can use the firewall policy editor to create or edit a custom firewall policy.

The Web UI offers the following firewall options:

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

**NOTE:** The firewall is disabled by default.

Multiple firewall policies can be stored but only one policy can be active at once. When a firewall is enabled and a custom policy file is applied, the policy is checked for syntax errors. If an error is found, the policy will not be loaded.

A sample firewall policy (.fwl) is provided in the file system for reference. It is available for download via FTP or SCP, from the /fwl directory of the file system.

Use the Test Policy option to test and verify a custom firewall policy. It is recommended that a firewall policy is tested before it is applied to a production environment.

## Network Settings

**Path: Configuration > Network**

### TCP/IP

**IPv4 settings.** The **IPv4** option, displays the current IPv4 address, subnet mask, default gateway, MAC address, and boot mode of the unit. For information on DHCP and DHCP options, see **RFC2131** and **RFC2132**.

| Setting | Description |
|---|---|
| Enable | Enable or disable IPv4 with this check box. |
| Manual | Configure IPv4 manually by entering the IP address, subnet mask, and default gateway. |
| BOOTP | A BOOTP server provides the TCP/IP settings. At 32-second intervals, the unit requests network assignment from any BOOTP server:<br>• If the unit receives a valid response, it starts the network services.<br>• If the unit finds a BOOTP server, but a request to that server fails or times out, the unit stops requesting network settings until it is restarted.<br>• By default, if previously configured network settings exist, and the unit receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible.<br><br>Click **Next>>** to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail:[1]<br>• **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.<br>• **If retries fail**: Select **Use prior settings** (the default) or **Stop BOOTP request**. |
| DHCP | The default setting. At 32-second intervals, the unit requests network assignment from any DHCP server.<br>• If the unit receives a valid response, it does not (as previously) require the APC cookie from the DHCP server in order to accept the lease and start the network services.<br>• If the unit finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted.[1]<br>• **Require vendor specific cookie to accept DHCP Address**: By selecting this check box, you can require the DHCP server to provide a cookie which supplies information to the unit. |

[1]. The default values for these three settings on the configuration pages generally do not need to be changed:
- **Vendor Class**: APC
- **Client ID**: The MAC address of the NMC, which uniquely identifies it on the local area network (LAN)
- **User Class**: The name of the application firmware module

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

**Vendor Specific Information (option 43).** The unit uses this option in a DHCP response to determine whether the DHCP response is valid. This option contains an APC-specific option in a TAG/LEN/DATA format, called the APC Cookie. This is disabled by default.

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

Option 43 communicates to the NMC that a DHCP server is configured to service devices.

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

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

**TCP/IP options.** The unit uses the following options within a valid DHCP response to define its TCP/IP settings. All of these options except the first are described in **RFC2132**.

- **IP Address** (from the **yiaddr** field of the DHCP response, described in **RFC2131)**: The IP address that the DHCP server is leasing to the unit.
- **Subnet Mask** (option 1): The Subnet Mask value that the unit needs to operate on the network.
- **Router,** i.e., Default Gateway (option 3): The default gateway address that the unit needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the unit.
- **Renewal Time, T1** (option 58): The time that the unit must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): The time that the unit must wait after an IP address lease is assigned before it can seek to rebind that lease.

**Other options.** The unit also uses these options within a valid DHCP response. All of these options except the last are described in **RFC2132**.

- **Network Time Protocol Servers** (option 42): Up to two NTP servers (primary and secondary) that the unit can use.
- **Time Offset** (option 2): The offset of the unit's subnet, in seconds, from Coordinated Universal Time (UTC).
- **Domain Name Server** (option 6): Up to two Domain Name System (DNS) servers (primary and secondary) that the unit can use.
- **Host Name** (option 12): The host name that the unit will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the unit will use (64-character maximum length).
- **Boot File Name** (from the **file** field of the DHCP response, described in **RFC2131**): The fully qualified directory-path to a user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the NMC will download the .ini file. After the download, the .ini file is used as a boot file to reconfigure the settings.

**IPv6 settings.**

**Path: Configuration > Network > TCP/IP > IPv6 settings**

| Setting | Description |
|---|---|
| Enable | Enable or disable IPv6 with this check box. |
| Manual | Configure IPv6 manually by entering the IP address and the default gateway. |
| Auto Configuration | When the Auto Configuration check box is selected, the system obtains addressing prefixes from the router (if available). It uses those prefixes to automatically configure IPv6 addresses. |
| DHCPv6 Mode | **Router Controlled**: Selecting this option means that DHCPv6 is controlled by the Managed(M) and Other(O) flags received in IPv6 router advertisements. When a router advertisement is received, the NMC checks whether the M or the O flag is set. The NMC interprets the state of the M (Managed Address Configuration Flag) and O (Other Stateful Configuration Flag) "bits" for the following cases:<br>• *Neither is set*: Indicates the local network has no DHCPv6 infrastructure. The NMC uses router advertisements and manual configuration to get addresses that are not link-local and other settings.<br>• *M, or M and O are set*: In this situation, full DHCPv6 address configuration occurs. DHCPv6 is used to obtain addresses AND other configuration settings. This is known as `DHCPv6 stateful`. Once the M flag has been received, the DHCPv6 address configuration stays in effect until the interface in question has been closed. This is true even if subsequent router advertisement packets are received in which the M flag is not set.<br>If an O flag is received first, then an M flag is received subsequently, the NMC performs full address configuration upon receipt of the M flag<br>• *Only O is set*: In this situation, the NMC sends a DHCPv6 Info-Request packet. DHCPv6 will be used to configure “other” settings (such as location of DNS servers), but NOT to provide addresses. This is known as `DHCPv6 stateless`.<br>**Address and Other Information:** With this radio box selected, DHCPv6 is used to obtain addresses AND other configuration settings. This is known as `DHCPv6 stateful`.<br>**Non-Address Information Only**: With this radio box selected, DHCPv6 will be used to configure "other" settings (such as location of DNS servers), but NOT to provide addresses. This is known as `DHCPv6 stateless`.<br>**Never**: Select this to disable DHCPv6. |

## Port Speed

**Path: Configuration > Network > Port Speed**

The **Port Speed** setting defines the communication speed of the TCP/IP port.

- For **Auto-negotiation** (the default), Ethernet devices negotiate to transmit at the highest possible speed. If the supported speeds of two devices are unmatched, the slower speed is used.
- Choose 10 Mbps or 100 Mbps, with the option of half-duplex (communication in only one direction at a time) or full-duplex (communication in both directions simultaneously).

### DNS Configuration

**Path: Configuration > Network > DNS**

**Configuration.** Use the options under **Configuration** to configure and test the Domain Name System (DNS):

- **Override Manual DNS Settings:** Selection of Override Manual DNS Settings will result in configuration data from other sources (typically DHCP) taking precedence over the manual configurations set here.
- Select **Primary DNS Server** or **Secondary DNS Server** to specify the IPv4 or IPv6 addresses of the primary and optional secondary DNS server. For the NMC to send e-mail, you must at least define the IP address of the primary DNS server.
  - The system waits up to 15 seconds for a response from the primary DNS server or secondary DNS server (if specified). If the NMC does not receive a response within that time, e-mail cannot be sent. Use DNS servers on the same segment as the NMC or on a nearby segment (but not across a wide-area network [WAN]).
  - Define the IP addresses of the DNS servers then enter the DNS name of a computer on your network to look up the IP address for that computer to verify correct operation.
- **System Name Synchronization:** Allow the system name to be synchronized with the host name so both fields automatically contain the same value.
  **NOTE:** When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the host name field).
- **Host Name**: Configure a host name here and a domain name in the **Domain Name** field then users can enter a host name in any field in the interface (except e-mail addresses) that accepts a domain name.
- **Domain Name (IPv4/IPv6)**: Configure the domain name here only. In all other fields in the interface (except e-mail addresses) that accept domain names, the unit adds this domain name when only a host name is entered.
  - To override all instances of the expansion of a specified host name by the addition of the domain name, set the domain name field to its default, `somedomain.com`, or to `0.0.0.0`.
  - To override the expansion of a specific host name entry, include a trailing period. The NMC recognizes a host name with a trailing period (such as *`mySnmpServer.`*) as if it were a fully-qualified domain name and does not append the domain name.
- **Domain Name (IPv6)**: Specify the IPv6 domain name here.

**Test.** Use this option to send a DNS query that tests the setup of your DNS servers by looking up the IP address. View the result of a test in the **Last Query Response** field.

- Select **test** to send a DNS query that tests the setup of your DNS servers:
  - As **Query Question**, identify the value to be used for the selected query type:

| Query Type Selected | Query Question to Use |
|---|---|
| by Host | The URL |
| by FQDN | The fully qualified domain name, *`my_server.my_domain`* |
| by IP | The IP address |
| by MX | The Mail Exchange address |

**Web Configuration**

**Path: Configuration > Network > Web**

| Option | Description |
|---|---|
| Access | • **Enable HTTP**: Enables Hypertext Transfer Protocol (HTTP), which provides Web access by user name and password, but does not encrypt user names, passwords, and data during transmission.<br>• **Enable HTTPS**: Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL). SSL encrypts user names, passwords, and data during transmission, and authenticates the Rack PDU by digital certificate. When HTTPS is enabled, your browser displays a small lock icon.<br>See "Creating and Installing Digital Certificates" in the *Security Handbook*, available at **www.apc.com**.<br>**HTTP Port**: The TCP/IP port (80 by default) used to communicate by HTTP with the unit.<br>**HTTPS Port**: The TCP/IP port (443 by default) used to communicate by HTTPS with the unit.<br>For either of these ports, you can change the port setting to any unused port from 5000 to 32768 for additional security. 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:<br>`http://152.214.12.114:5000`<br>`https://152.214.12.114:5000`<br>**Minimum Protocol:** The minimum HTTPS protocol to use. Select SSL 3.0, TLS 1.0,<br>TLS 1.1 or TLS 1.2.<br>**Require Authentication Cookie:** Click to Enable<br>**Limited Status Access:** Click to Enable. Click to check the box to Use as Default Page.<br>Click the **Apply** button at the bottom of the page to save your changes. Click **Cancel** to void your changes before leaving the page. |
| SSL Certificate | Add, replace, or remove a security certificate.<br>**Status**:<br>• **Not installed**: A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Using **Add or Replace Certificate File** installs the certificate to the correct location, **/ssl** on the unit.<br>• **Generating**: The unit is generating a certificate because no valid certificate was found.<br>• **Loading**: A certificate is being activated on the unit.<br>• **Valid certificate**: A valid certificate was installed or was generated by the unit. Click on this link to view the contents of the certificate.<br>**If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the unit generates a default certificate, a process which delays access to the interface for up to one minute.** You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on.<br>**Add or Replace Certificate File**: Enter or browse to the certificate file created with the Security Wizard.<br>See "Creating and Installing Digital Certificates" in the *Security Handbook,* available at **www.apc.com***,* to choose a method for using digital certificates created by the Security Wizard or generated by the unit.<br>**Remove**: Delete the current certificate. |

### Console Configuration

**Path: Configuration > Network > Console**

| Option | Description |
|---|---|
| Access | • **Enable Telnet**: Telnet transmits user names, passwords, and data without encryption.<br>• **Enable SSH**: SSH transmits user names, passwords, and data in encrypted form, providing protection from attempts to intercept, forge, or alter data during transmission.<br>• To Disable, click in the Enable box to remove the check mark.<br>Configure the ports to be used by these protocols:<br>• **Telnet Port**: The Telnet port used to communicate with the unit (23 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) or a space, as required by your Telnet client program, to specify the non-default port. For example, for port 5000 and an IP address of 152.214.12.114, your Telnet client requires one of the these commands:<br>`telnet 152.214.12.114:5000`<br>`telnet 152.214.12.114 5000`<br>• **SSH Port**: The SSH port used to communicate with the unit (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port.<br>Click the **Apply** button at the bottom of the page to save your changes. Click **Cancel** to void your changes before leaving the page. |
| **NOTE:** To enhance security, the port setting can be changed to any unused port from 5000 to 32768. Users must then specify the non-default port to gain access. Telnet clients require users to append either a space and the port number or a colon and the port number to the command line to access the command line interface. For SSH, see your SSH client documentation to specify a non-default port in the command line that starts SSH. | |
| SSH Host Key | This page allows the user to view the status of an installed SSH Host Key, as well as Add, Replace, or Remove a Host Key.<br>• Status: Indicates whether the current SSH Host Key is valid.<br>• Add or Replace Host Key: To use a host key you created with the Security Wizard, load the host key before you enable SSH. Browse to or enter the path name of the host key file created with the Security Wizard, and click Apply.<br>If the host key has been removed or if no host key was loaded, and you enable SSH, the device restarts, and it generates a host key. Allowing the device to generate its own host key could make the SSH server unavailable for use for as long as 1 minute.<br>Host Key Fingerprint: A fingerprint helps authenticate a server. If the Security Wizard is used to generate the host key, it also generates the fingerprint, which is displayed here when SSH is enabled and the host key is in use. When you first connect to the device using SSH, compare the fingerprint presented by the SSH client to the fingerprint that the Security Wizard generated to ensure that they match. (Almost all SSH clients display the fingerprint.)<br>Remove: Remove the current host key.<br>Click the **Apply** button at the bottom of the page to save your changes. Click **Cancel** to void your changes before leaving the page. |

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

### SNMP

All user names, passwords, and community names for SNMP are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMP access or set the access for each community to Read. (A community with Read access can receive status information and use SNMP traps.)

When using StruxureWare to manage a unit on the public network, you must have SNMP enabled in the interface. Read access will allow StruxureWare to receive traps from the NMC, but Write access is required while you use the interface to set StruxureWare as a trap receiver.

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

### SNMPv1

**Path: Configuration > Network > SNMPv1**

| Option | Description |
|---|---|
| Access | **Enable SNMPv1 Access:** Enables SNMP version 1 as a method of communication with this device. |
| Access Control | Configure up to four access control entries to specify which NMSs have access to this device. The access control opening page, by default, assigns one entry to each of the four SNMPv1 communities. Edit to apply more than one entry to a community to grant access by several IP addresses, host names, or IP address masks. To edit the access control settings, click its community name.<br>• Leave the default access control entry unchanged and the community has access from any location on the network.<br>• Multiple access control entries for one community name means one or more of the other communities will have no access control entry. If no access control entry is listed, that community has no access to the device.<br>**Community Name:** The name that a NMS uses to access the community. The maximum length is 15 ASCII characters. The default names are public, private, public2, and private2.<br>**NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address allows access only by the NMS at that location.<br>IP addresses that contain 255 restrict access as follows:<br>• 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment.<br>• 149.225.**255.255**: Access only by an NMS on the 149.225 segment.<br>• 149.**255.255.255**: Access only by an NMS on the 149 segment.<br>• 0.0.0.0 (default) can also be expressed as 255.255.255.255: Access by any NMS on any segment.<br>**Access Type**: The actions an NMS can perform through the community.<br>• **Read**: GETS only, at any time<br>• **Write**: GETS at any time, and SETS when no user is logged onto the Web interface.<br>• **Write+**: GETS and SETS at any time.<br>• **Disabled**: No GETS or SETS at any time. |

### SNMPv3

**Path: Configuration > Network > SNMPv3**

For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users. An SNMPv3 user must have a user profile assigned in the MIB software program to perform GETs and SETs, browse the MIB, and receive traps.

You must have a MIB program that supports SNMPv3. The NMC supports only MD5 authentication and DES encryption.

| Option | Description |
|---|---|
| Access | **SNMPv3 Access:** Enables SNMPv3 as a method of communication with this device. |
| User Profiles | By default, lists the settings of four user profiles, configured with the user names **apc snmp profile1** through **apc snmp profile4**, no authentication and no privacy (no encryption). To edit the following settings for a user profile, click a user name in the list.<br><br>**User Name:** The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters.<br><br>**Authentication Passphrase:** A phrase of 15 to 32 ASCII characters (apc auth passphrase, by default) that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time.<br><br>**Privacy Passphrase:** A phrase of 15 to 32 ASCII characters (apc crypt passphrase, by default) that ensures the privacy of the data (by means of encryption) that an NMS is sending to this device or receiving from this device through SNMPv3.<br><br>**Authentication Protocol:** Supports MD5 authentication. Authentication will not occur unless MD5 is selected as the authentication protocol.<br><br>**Privacy Protocol:** Supports DES as the protocol for encrypting and decrypting data. Privacy of transmitted data requires that DES is selected. It cannot be selected unless an authentication protocol is selected. |
| Access Control | Configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles. Edit the settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks.<br>• Leave the default access control entry unchanged for a user profile and all NMSs that use that profile have access to this device.<br>• Multiple access entries for one user profile, means there can be no access control entry for one or more of the other user profiles. If no access control entry is listed for a user profile, NMSs using that profile have no access to this device.<br><br>To edit the access control settings for a user profile, click its user name.<br><br>**Access:** Mark the **Enable** checkbox to activate access control.<br><br>**User Name:** Select the user profile to which access control will apply. The choices are the four user names you configured in the **user profiles** option.<br><br>**NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows:<br>• 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment.<br>• 149.225.**255**.**255**: Access only by an NMS on the 149.225 segment.<br>• 149.**255**.**255**.**255**: Access only by an NMS on the 149 segment.<br>• 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. |

### Modbus Configuration

**Path: Configuration > Network > Modbus**

Enabling Modbus allows a Building Management System to monitor the NMC of the PDU. The system supports Modbus serial (RTU) and Modbus TCP.

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

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

You must log off for the changes to take effect. See your unit's Operation manual for Modbus installation information.

### FTP Server Configuration

**Path: Configuration > Network > FTP Server**

**FTP Server.** The **FTP Server** settings enable (by default) or disable access to the FTP server and specify the TCP/IP port (21 by default) that the FTP server uses to communicate with the unit. The FTP server uses both the specified port and the port one number lower than the specified port.

You can change the **Port** setting to the number of any unused port from 5001 to 32768 for added security. Users must then use a colon (:) to specify the non-default port number. For example, for port 5001 and IP address 152.214.12.114, the command would be `ftp 152.214.12.114:5001`.

**NOTE:** FTP transfers files without encryption. For higher security, disable the FTP server, and transfer files with SCP. Selecting and configuring Secure SHell (SSH) enables SCP automatically.
At any time that you want a unit to be accessible for management by StruxureWare, FTP Server must be enabled in the unit interface.

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

## Notification

### Event Actions

**Path: Configuration > Notification > Event Actions**

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

- Active, automatic notification. The specified users or monitoring devices are contacted directly.
  - E-mail notification
  - SNMP traps
  - Remote Monitoring Service
  - Syslog notification
- Indirect notification
  - Event log. If no direct notification is configured, users must check the log to determine which events have occurred

    You can also log system performance data to use for device monitoring. See “Logs in the Configuration Menu” on page 90 for information on how to configure and use this data logging option.
  - Queries (SNMP GETs)

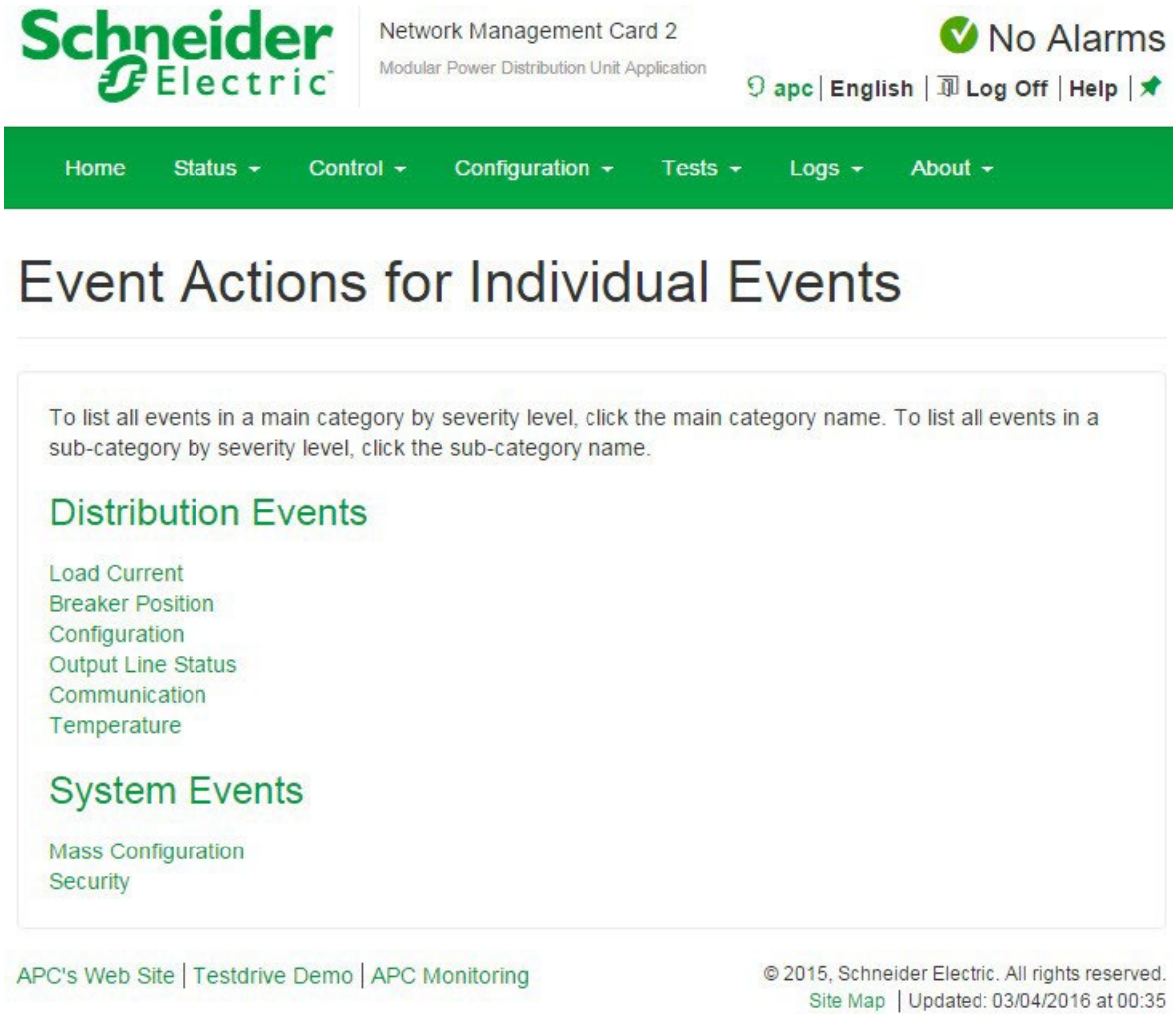
    For more information, see “SNMP” on page 78. SNMP enables an NMS to perform informational queries. For SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without the risk of allowing remote configuration changes.

**Path: Configuration > Notification > Event Actions > By Event**

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

- To find an event, click on a column heading to see the lists under the **Device Events** or **System Events** categories.
  Or you can click on a sub-category under these headings, like **Security** or **Temperature**.
- Click on the event name to view or change the current configuration, such as recipients to be notified by e-mail, or Network Management Systems (NMSs) to be notified by SNMP traps.

If no Syslog server is configured, items related to Syslog configuration are not displayed.




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

- “Servers” on page 90
- “Path: Configuration > Notification > E-mail > Recipients” on page 85
- “Path: Configuration > Notification > SNMP Traps > Trap Receivers” on page 86

**Path: Configuration > Notification > Event Actions > By Group**

To configure a group of events simultaneously:

1. Select how to group events for configuration:
   – Select **Events by Severity**, and then select one or more severity levels. You cannot change the severity of an event.
   – Select **Events by Category**, and then select all events in one or more pre-defined categories.
2. Click **Next** to move to the next screen to do the following:
   a. Select event actions for the group of events.
      • To select any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
      • If you selected **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** on the next screen. See “Logs in the Configuration Menu” on page 90
3. Click **Next** to move to the next screen to do the following:
   a. If you selected **Logging** on the previous screen, select **Enable Notifications** or **Disable Notification**.
   b. If you selected **Email Recipients** on the previous screen, select the e-mail recipients to configure.
   c. If you selected **Trap Receivers** on the previous screen, select the trap receiver to configure.
4. Click **Next** to move to the next screen to do the following:
   **a.** If you are configuring **Logging** settings, view the pending actions and click **Apply** to accept the changes or click **Cancel** to revert to the previous settings.
   b. If you are configuring **Email Recipients** or **Trap Receivers,** select **Enable Notifications** or **Disable Notification** and set the notification timing settings (see “Notification parameters” for more information on these settings).
5. Click **Next** to move to the next screen to do the following:
   a. View the pending actions and click **Apply** to accept the changes or click **Cancel** to revert to the previous settings.

**Notification parameters.** These configuration fields define e-mail parameters for sending notifications of events.

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

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

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

### E-mail notification

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

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

**Path: Configuration > Notification > E-mail > Server**

This screen lists your primary and secondary DNS servers and displays the following fields:

**From Address.** The contents of the From field in e-mail messages sent by the unit:

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

**SMTP Server.** The IPv4/ IPv6 address or DNS name of the local SMTP server.

**NOTE:** This definition is required only when the SMTP server is set to **Local**.

**Authentication.** Enable this if the SMTP server requires authentication.

**Port.** The SMTP port number, with a default of 25. The range is 25, 465, 587, 5000 to 32768.

**User Name, Password, and Confirm Password.** If your mail server requires authentication, enter your user name and password here. This performs a simple authentication, not SSL.

**Use SSL/TLS.** Select when encryption is used.

- **Never:** The SMTP server does not require nor support encryption.
- **If Supported:** The SMTP server advertises support for STARTTLS but doesn't require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given.
- **Always:** The SMTP server requires the STARTTLS command to be sent on connection to it.
- **Implicitly:** The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.

**Require CA Root Certificate.** This should only be enabled if the security policy of your organization does not allow for implicit trust of SSL connections. If this is enabled, a valid root CA certificate must be loaded onto the unit for encrypted e-mails to be sent.

**File Name.** This field is dependent on the root CA certificates installed on the unit and whether or not a root CA certificate is required.

**Path: Configuration > Notification > E-mail > Recipients**

Specify up to four e-mail recipients. Click on a name to configure the settings.

**Generation.** Enables (default) or disables sending e-mail to the recipient.

**To Address.** The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page.

To bypass the DNS lookup of the IP address of the mail server, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.

**Language.** The language which the e-mail notification will be sent in. This is dependent on the installed language pack (if applicable).

**Port.** The SMTP port number, with a default of 25. The range is 25, 465, 587, 5000 to 32768.

**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.

**Server.** Select one of the following methods for routing e-mail:

- **Local:** This is through the site-local SMTP server. This recommended setting ensures that the e-mail is sent using the site-local SMTP server. Choosing this setting limits delays and network outages and retries sending e-mail for many hours. When choosing the Local setting you must also enable forwarding at the SMTP server of your device and set up a special external e-mail account to receive the forwarded e-mail. Check with your SMTP server administrator before making these changes.
- **Recipient:** This is the SMTP server of the recipient. The unit performs an MX record look-up on the recipients e-mail address and uses that as its SMTP server. The e-mail is only sent once so it could easily be lost.
- **Custom:** This setting enables each e-mail recipient to have its own server settings. These settings are independent of the settings given under "SMTP Server" above.

**Path: Configuration > Notification > E-mail > SSL Certificates**

Load a mail SSL certificate on the unit for greater security. The file must have an extension of `.crt` or `.cer`. Up to five files can be loaded at any given time.

When installed, the certificate details also display here. An invalid certificate will display "n/a" for all fields except **File Name**.

Certificates can be deleted using this screen. Any e-mail recipients using the certificate should be manually modified to remove reference to this certificate.

**Path: Configuration > Notification > E-mail > Test**

Send a test message to a configured recipient.

## SNMP trap receiver screen

**Path: Configuration > Notification > SNMP Traps > Trap Receivers**

With Simple Network Management Protocol (SNMP) traps, you can automatically get notifications for significant unit events. They are a useful tool for monitoring devices on your network.

The trap receivers are displayed by **NMS IP/Host Name**, where NMS stands for Network Management System. You can configure up to six trap receivers.

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

**Trap Generation.** Enable (the default) or disable trap generation for this trap receiver.

**NMS IP/Host Name.** The IPv4/ IPv6 address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.

**Language.** Select a language from the drop-down list. This can differ from the UI and from other trap receivers.

Select either the **SNMPv1** or **SNMPv3** radio button to specify the trap type. For an NMS to receive both types of traps, you must separately configure two trap receivers for that NMS, one for each trap type.

**SNMPv1.** Settings for SNMPv1.

- **Community Name:** The name (“public” by default) used as an identifier when SNMPv1 traps are sent to this trap receiver.
- **Authenticate Traps:** When this option is enabled (the default), the NMS identified by the NMS IP/Host Name setting will receive authentication traps (traps generated by invalid attempts to log on to this device).

**SNMPv3.** Settings for SNMPv3.

- **User Name:** Select the identifier of the user profile for this trap receiver.

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

## SNMP traps test screen

**Path: Configuration > Notification > SNMP Traps > Test**

**Last Test Result.** The result of the most recent SNMP trap test. A successful SNMP trap test verifies only that a trap was sent; it does not verify that the trap was received by the selected trap receiver. A trap test succeeds if all of the following are true:

- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver itself is enabled.
- If a host name is selected for the **To** address, that host name can be mapped to a valid IP address.

To Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver is configured, a link to the **Trap Receiver** configuration screen is displayed.

## Remote Monitoring Service

**Path: Configuration > Notification > Remote Monitoring**

The remote monitoring service (RMS) is an optional service from Schneider Electric that monitors your system from a remote operation center 24 hours a day, 7 days a week, and notifies you of device and system events.

To purchase the RMS service, contact your vendor or click on the link on this screen: APC Monitoring.

**Registration.** To activate APC Monitoring for the unit, select **Enable Remote Monitoring Service.,** choose between **Register Company and Device** and **Register Device Only**, complete the form, and click **Send APC RMS Registration**.

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

## General Options

### NMC Information

**Path: Configuration > General > Identification**

Define values for **Name** (the device name), **Location** (the physical location), and **Contact** (the person responsible for the device) used by the NMC's SNMP agent. These settings are the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifiers (OIDs).

### Set the Date and Time

**Path: Configuration > General > Date & Time**

**Mode.** Set the time and date used by the NMC. You can change the current settings manually or through a Network Time Protocol (NTP) Server:
Do one of the following:

– Enter the date and time for the NMC.

– Mark the check box **Apply Local Computer Time** to match the date and time settings of the computer you are using.

Synchronize with NTP Server: Have an NTP Server define the date and time for the NMC.

| Setting | Definition |
|---|---|
| Primary NTP Server | Enter the IP address or domain name of the primary NTP server. |
| Secondary NTP Server | Enter the IP address or domain name of the secondary NTP server, when a secondary server is available. |
| Time Zone | Select a time zone. The number of hours preceding each time zone in the list is the offset from Coordinated Universal Time (UTC), formerly Greenwich Mean Time). |
| Update Interval | Define how often, in hours, the NMC accesses the NTP Server for an update. *Minimum*: 1; *Maximum*: 8760 (1 year). |
| Update Using NTP Now | Initiate an immediate update of date and time by the NTP Server. |

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

- If the local DST always starts or ends on the fourth occurrence of a specific weekday of a month (the fourth Sunday, for example), choose **Fourth/Last**. If a fifth Sunday occurs in that month in a subsequent year, the time setting still changes on the fourth Sunday.
- If the local DST always starts or ends on the last occurrence of a specific weekday of a month, whether it is the fourth or the fifth occurrence, choose **Fifth/Last**.
- Format: Select the format 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 display with a leading zero.

**Path: Configuration > General > User Config File**

**.ini file.** Use the settings from one NMC to configure another. Retrieve the config.ini file from the configured NMC, customize that file (e.g., to change the IP address), and upload the customized file to the new NMC. The file name can be up to 64 characters, and must have the.ini suffix.

| | |
|---|---|
| Status | Reports the progress of the upload. The upload succeeds even if the file contains errors, but a system event reports the errors in the event log. |
| Upload | Browse to the customized file and upload it so the current NMC can use it to set its configuration. |

Instead of uploading the file to one NMC, you can export the file to multiple NMCs by using an FTP script or a batch file and the APC .ini file utility, available from **www.apc.com/tools/download**.

## Logs in the Configuration Menu

**Path: Configuration > Logs > Syslog**

### Servers

Click **Add Server** to configure a new Syslog server.

**Syslog Server.** Uses IPv4/ IPv6 addresses or host names to identify from one to four servers to receive Syslog messages sent by the unit.

**Port.** The port that the unit will use to send Syslog messages. The default UDP port assigned to Syslog is 514.

**Language.** Select the language for any Syslog messages.

**Protocol.** Select either UDP or TCP.

### Settings

**Message Generation.** Enable the generation and the logging of Syslog messages for events that have Syslog configured as a notification method.

**Facility Code.** Selects the facility code assigned to the Syslog messages of the unit (User, by default).

**NOTE: User** best defines the Syslog messages sent by the unit. Do not change this selection unless advised to do so by the Syslog network or system administrator.

**Severity Mapping.** This section maps each severity level of the unit or environment events to available Syslog priorities. The local options are **Critical**, **Warning**, and **Informational**. You should not need to change the mappings.

- **Emergency**: The system is unusable
- **Alert**: Action must be taken immediately
- **Critical**: Critical conditions
- **Error**: Error conditions
- **Warning**: Warning conditions
- **Notice**: Normal but significant conditions
- **Informational**: Informational messages
- **Debug**: Debug-level messages

The following are the default settings for the **Local Priority** settings:

- **Critical** is mapped to **Critical**
- **Warning** is mapped to **Warning**
- **Informational** is mapped to **Info**

### Test

**Syslog test and format example. .** Send a test message to the Syslog servers (configured through the “Identifying Syslog servers” option above). The result will be sent to all configured Syslog servers.

Select a severity to assign to the test message and then define the test message. Format the message to consist of the event type (for example, APC, System, or Device) followed by a colon, a space, and the event text. The message can have a maximum of 50 characters.

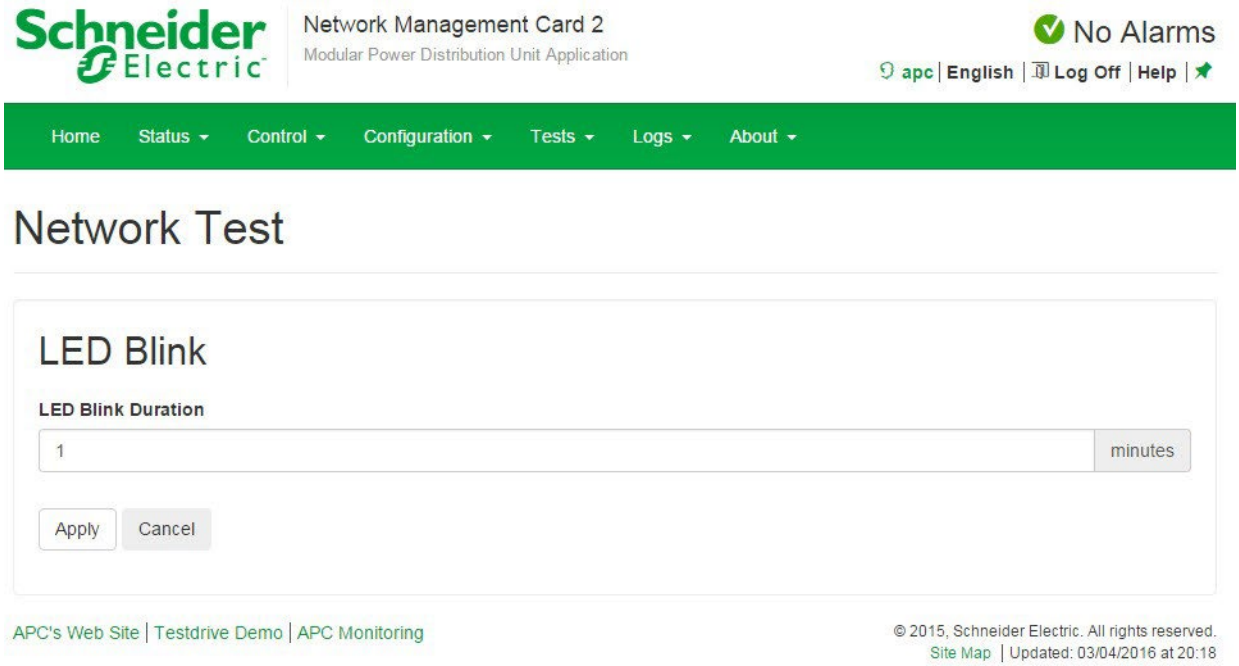
- The priority (PRI): the Syslog priority assigned to the message event, and the facility code of messages sent by the unit.
- The Header: a time stamp and the IP address of the unit.
- The message (MSG) part:
- The **TAG** field, followed by a colon and space, identifies the event type.
- The **CONTENT** field is the event text, followed (optionally) by a space and the event code.

  Example: `APC: Test Syslog is valid.`

# The Tests Tab

**Path: Tests > Network > LED Blink**

If you are having trouble finding your unit, enter a number of minutes in the **LED Blink Duration** field, click **Apply**, and the Status LED light on the Network Management Interface will blink.



# Logs Tab

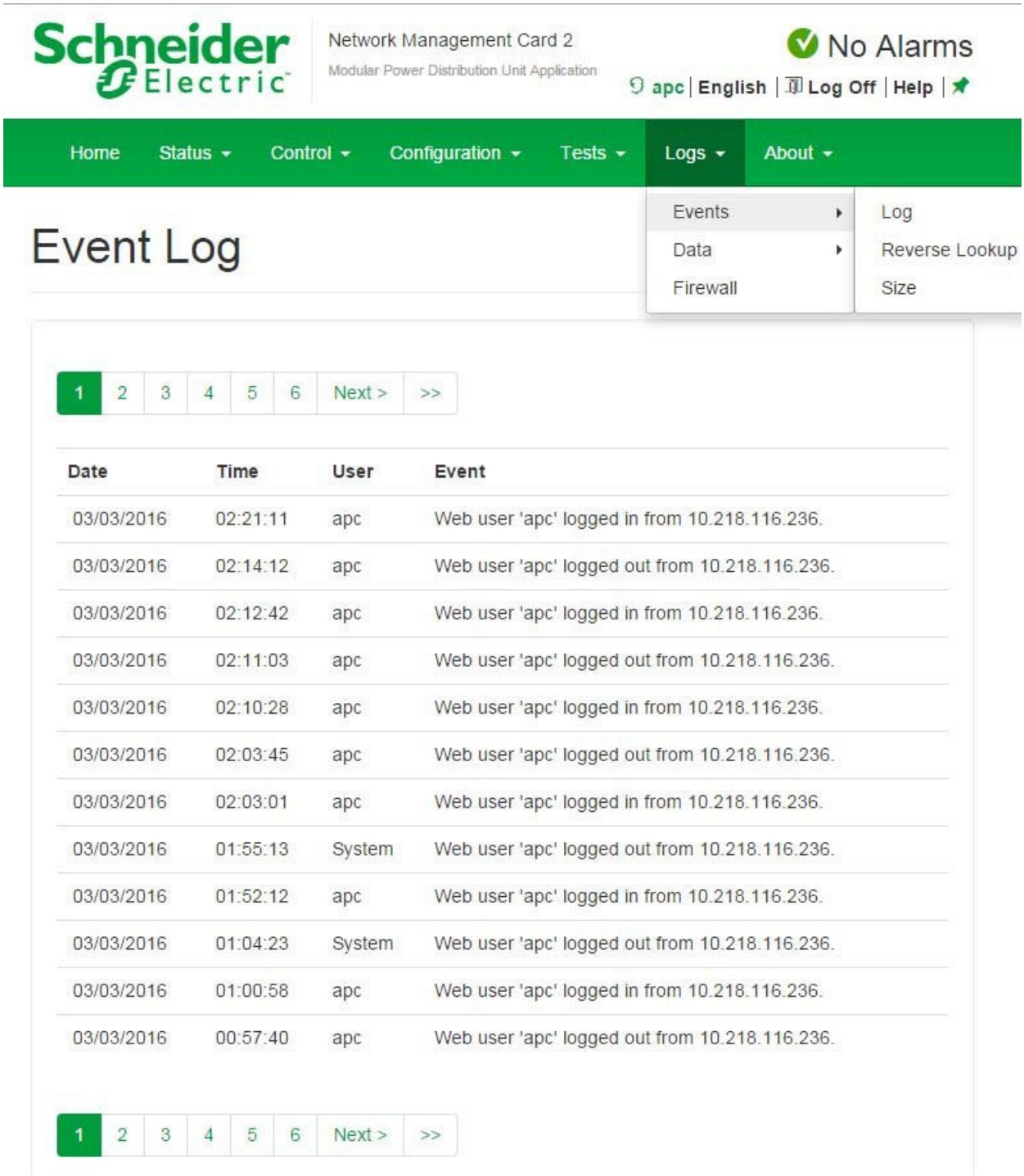
## Event, Data, and Firewall Logs

**Path: Logs > Events**

By default, the log displays all events recorded during the last two days, starting with the latest events.

Additionally, the log records any event that sends an SNMP trap, except SNMP authentication failures, and abnormal internal system events.

You can enable color coding for events on the **Configuration > Security > Local Users Management** screen.



### Log

By default, the event log displays the most recent events first. To see the events listed together on a Web page, click **Launch Log in New Window**.

To open the log in a text file or to save the log to disk, click on the floppy disk icon( ) on the same line as the **Event Log** heading.

You can also use FTP or Secure CoPy (SCP) to view the event log. See “Use FTP or SCP to retrieve log files” on page 96.

**Filtering event logs.** Use filtering to omit information you don’t want to display.

- Filtering the log by date or time: Use the **Last** or **From** radio buttons. (The filter configuration is saved until the RPDU restarts.)
- Filtering the log by event severity or category:
  - Click **Filter Log**.
  - Clear a check box to remove it from view.
  - After you click **Apply**, text at the upper right corner of the **Event Log** page indicates that a filter is active. The filter is active until you clear it or until the RPDU restarts.
- Removing an active filter:
  - Click **Filter Log.**
  - Click **Clear Filter (Show All)**.
  - As Administrator, click **Save As Default** to save this filter as the new default log view for all users.

Important points on filtering:

- Events are processed through the filter using OR logic. If you apply a filter, it works regardless of the other filters.
- Events that you cleared in the **Filter By Severity** list never display in the filtered Event Log, even if selected in the **Filter by Category** list.
- Similarly, events that you clear in the Filter by Category list never display in the filtered Event Log.

**Deleting event logs.** To delete all events, click **Clear Log**. Deleted events cannot be retrieved.

To disable the logging of events based on their assigned severity level or their event category, see “Configure event actions” on page 81

### Reverse Lookup

With reverse lookup enabled, when a network-related event occurs, both the IP address and the domain name for the networked device with the event are logged in the event log. If no domain name entry exists for the device, only its IP address is logged with the event.

Since domain names generally change less frequently than IP addresses, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events.

Reverse lookup is disabled by default. You should not need to enable it if you have no DNS server configured or have poor network performance because of heavy network traffic.

### Size

Use **Event Log Size** to specify the maximum number of log entries.

**NOTE:** When you resize the event log in order to specify a maximum size, all existing log entries are deleted. When the log subsequently reaches the maximum size, the older entries are deleted.

## Data log

**Path: Logs > Data**

Use the data log to display measurements about the unit, the power input to the unit, and the ambient temperature of the unit.

The steps to display and resize the data log are the same as for the event log, except that you use menu options under **Data** instead of **Events**.

**Filtering data logs.** Use filtering to omit information you don't want to display from view. To view data from a different unit, select the desired unit from the "Filter Log" pull-down list.

Similarly for data log graphing, you can select a different unit by clicking on the **Change Data Filter** button.

- Filtering the log by date or time: Use the **Last** or **From** radio buttons. (The filter configuration is saved until the unit restarts.)
- Filtering the log by event severity or category:
    a. Click **Filter Log**.
    b. Clear a check box to remove it from view.
    c. After you click **Apply**, text at the upper right corner of the **Data Log** page indicates that a filter is active. The filter is active until you clear it or until the unit restarts.
- Removing an active filter:
    **d.** Click **Filter Log.**
    e. Click **Clear Filter (Show All)**.
    f. As Administrator, click **Save As Default** to save this filter as the new default log view for all users.

**Deleting data logs.** To delete all data log records, click **Clear Data Log**. Deleted data log records cannot be retrieved.

### Interval

Define, in the **Log Interval** setting, how frequently data is searched for and stored in the data log. When you click **Apply**, the number of possible storage days is recalculated and display at the top of the screen. When the log is full, the oldest entries are deleted.

**NOTE:** Because the interval specifies how often the data is recorded, the smaller the interval, the more times the data is recorded and the larger the log file.

#### Rotation

Rotation causes the contents of the data log to be appended to the file you specify by name and location. Use this option to set up password-protection and other parameters.

- **FTP Server:** The IP address or host name of the server where the file will reside.
- **User Name/Password:** The user name with password required to send data to the repository file. This user must also be configured to have read and write access to the data repository file and the directory (folder) in which it is stored.
- **File Path:** The path to the repository file.
- **Filename:** The name of the repository file (an ASCII text file), e.g. datalog.txt. Any new data is appended to this file: it does not overwrite it.
- **Unique Filename:** Select this check box to save the log as *mmddyyyy_<filename>.txt*, where filename is what you specified in the **Filename** field above. Any new data is appended to the file but each day has its own file.
- **Delay *n* hours between uploads:** The number of hours between uploads of data to the file (max. 24 hours).
- **Upon failure, try uploading every *n* minutes:** The number of minutes between attempts to upload data to the file after a failed upload.
  - **Up to *n* times:** The maximum number of times the upload will be attempted after it fails initially.
  - **Until upload succeeds:** Attempt to upload the file until the transfer is completed.

#### Size

Use **Data Log Size** to specify the maximum number of log entries.

**NOTE:** When you resize the data log in order to specify a maximum size, all existing log entries are deleted. When the log subsequently reaches the maximum size, the older entries are deleted.

### Firewall Logs

#### Path: Logs > Firewall

If you create a firewall policy, firewall events will be logged here.

The information in the log can be useful to help the technical support team solve problems. Log entries contain information about the traffic and the rules action (allowed, discarded). When logged here, these events are not logged in the main Event Log (see “Event, Data, and Firewall Logs” on page 92).

A firewall log contains up to 50 of the most recent events. The firewall log is cleared when the management interface reboots.

## Use FTP or SCP to retrieve log files

An Administrator or Device User can use FTP or SCP to retrieve a tab-delineated event log file (`event.txt`) or data log file (`data.txt`) and import it into a spreadsheet.

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

**NOTE:** The uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits.

If you are using the encryption-based security protocols for your system, use SCP to retrieve the log file.

If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.

See the *Security Handbook*, available at **www.schneider-electric.com**, for information on available protocols and methods for setting up the type of security you need.

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

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

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

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

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

1. At a command prompt, type `ftp` and the IP address of the NMC, and press ENTER.

   If the **Port** setting for the **FTP Server** option (set through the **Network** menu of the **Administration** tab) has been changed from its default (**21**), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)
   ```
   ftp>open ip_address port_number
   ```

   To set a non-default port value to enhance security for the FTP Server, see “FTP Server” on page 80. You can specify any port from 5001 to 32768.
2. Use the case-sensitive **User Name** and **Password** for Administrator or Device User to log on.
3. Use the **get** command to transmit the text of a log to your local drive.

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

   or

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

# The About Tab

## About the Device

**Path: About > Device**

The hardware information is useful to Schneider Electric Customer Support for troubleshooting problems with the unit. The serial number and MAC address are also available on the unit itself. Device options include:

- Modules
- Metering System
- Electrical Configuration

**Path: About > Network**

Firmware information for the Application Module, APC OS (AOS), and APC Boot Monitor indicates the name, the firmware version, and the date and time each firmware module was created. This information is also useful in troubleshooting and enables you to determine if updated firmware is available at the web site, **www.apc.com**.

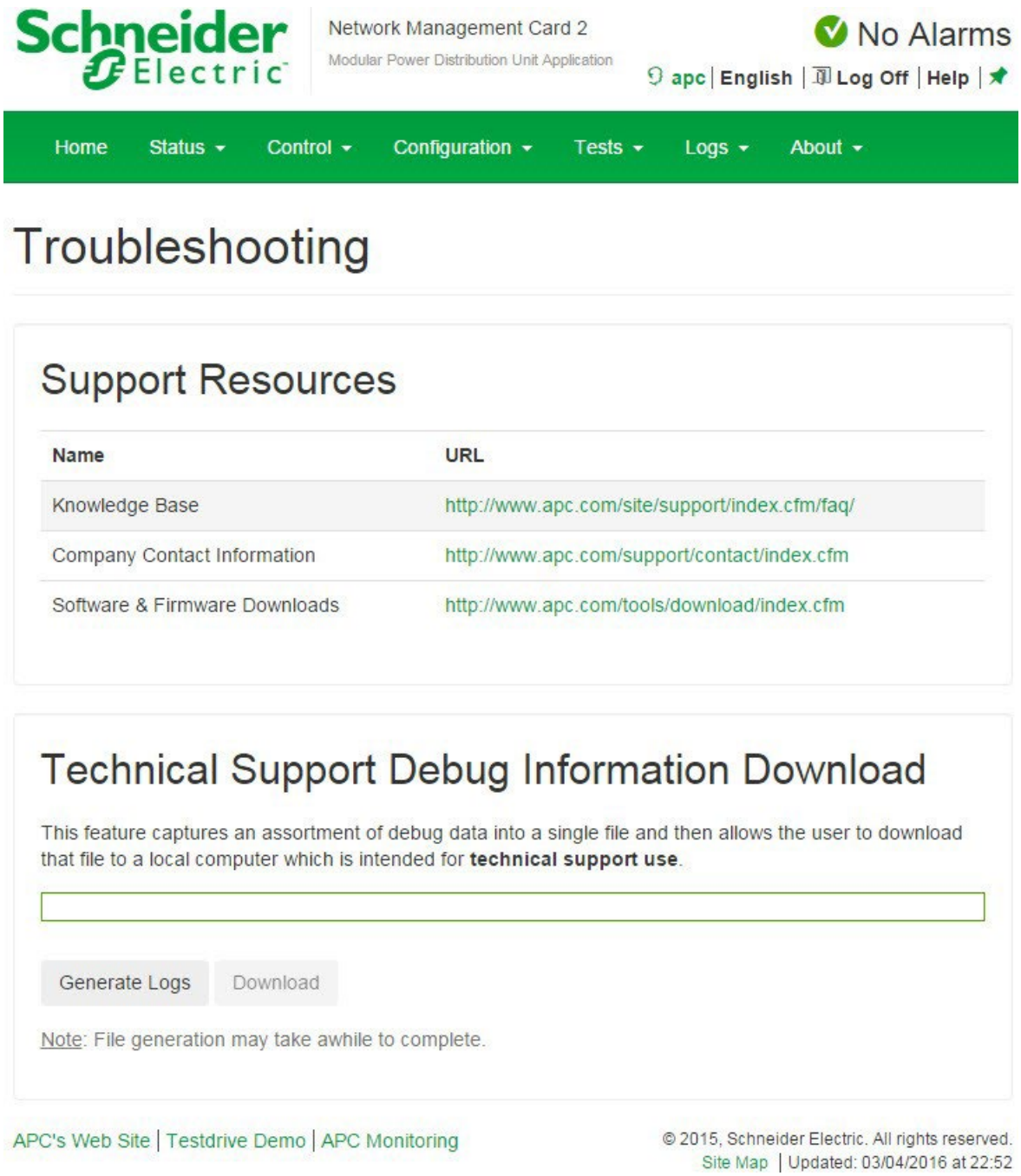
**Management Uptime** is the length of time the network management interface has been running continuously.

**Path: About > Support**

This page provides links to **Support Resources** including:

- Knowledge Base
- Company Contact Information
- Software and Firmware Downloads

The **Technical Support Debug Information Download** feature is provided at the bottom of the page.



# Device IP Configuration Wizard

The APC Device IP Configuration Wizard configures the IP address, subnet mask, and default gateway of one or more units. You can use the Wizard in either of the following ways:

- Remotely over your TCP/IP network to discover and configure unconfigured units on the same network segment as the computer running the Wizard.
- Through a direct connection from a serial port of your computer to the unit to configure or reconfigure it.

## System requirements

The Device IP Configuration Wizard runs on Microsoft® Windows® 2000, Windows Server® 2003, Windows Server® 2012, and on 32- and 64-bit versions of Windows XP, Windows Vista, Windows 2008, Windows 7, and Windows 8 operating systems.

## Installation

Install the Wizard from a downloaded executable file:

1. Go to **www.apc.com/tools/download**.
2. Download the Device IP Configuration Wizard.
3. Run the executable file in the folder in which it was downloaded.

## Launch the Wizard

The installation creates a shortcut link in the Windows **Start** menu to launch the Wizard. Most software firewalls must be temporarily disabled for the Wizard to discover unconfigured units.

# Export Configuration Settings

# Retrieving and Exporting the .ini File

### Summary of the procedure

A Super User/Administrator can retrieve the .ini file of a unit and export it to another unit or to multiple units. The steps are below; see details in the sections following.

1. Configure a unit with the desired settings and export them.
2. Retrieve the .ini file from that unit.
3. Customize the file to change the TCP/IP settings at least.
4. Use a file transfer protocol supported by the unit to transfer a copy to one or more other units. For a transfer to multiple units, use an FTP or SCP script or the .ini file utility.

Each receiving unit uses the file to reconfigure its own settings and then deletes it.

**NOTE:** Managing Users via the config.ini - Users are no longer managed via the config.ini in any form. Users are now managed via a separate file with the .csf extension. For further information on this topic, refer to article ID FA176542 in the Knowledge Base at **www.apc.com**.

### Contents of the .ini file

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

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

## Detailed procedures

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

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

      ```
      ftp> open ip_address
      ```

   b. Log on using the Super User/Administrator user name and password.
   c. Retrieve the *config.ini* file containing the settings of the unit:

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

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

      To retrieve configuration settings from multiple NMCs and export them to other units, see *Release Notes: ini File Utility, version 2.0,* available at **www.apc.com**.

**Customizing.** You must customize the file before you export it.

1. Use a text editor to customize the file.
   – Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   – Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   – Enclose in quotation marks any values that contain leading or trailing spaces or are already enclosed in quotation marks.
   – To export scheduled events, configure the values directly in the .ini file.
   – To export a system time with the greatest accuracy, if the receiving units can access a Network Time Protocol server, configure `enabled` for `NTPEnable`:

      ```
      NTPEnable=enabled
      ```

      Alternatively, reduce transmission time by exporting the `[SystemDate/Time]` section as a separate .ini file.
   – To add comments, start each comment line with a semicolon (`;`).
2. Copy the customized file to another file name in the same folder:
   – The file name can have up to 64 characters and must have the .ini suffix.
   – Retain the original customized file for future use. **The file that you retain is the only record of your comments.**

**Transferring the file to a single unit.** To transfer the .ini file to another unit, do either of the following:

- From the Web UI of the receiving unit, select **Configuration** > **General** > **User Config File**. Enter the full path of the file, or use Browse on your local PC.
- Use any file transfer protocol supported by units, i.e., FTP, FTP Client, SCP, or TFTP. The following example uses FTP:

  a. From the folder containing the copy of the customized .ini file, use FTP to log in to the unit to which you are exporting the .ini file:

  ```
  ftp> open ip_address
  ```

  b. Export the copy of the customized .ini file to the root directory of the receiving unit:

  ```
  ftp> put filename.ini
  ```

**Exporting the file to multiple units.** To export the .ini file to multiple units:

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

To create the batch file and use the utility, see *Release Notes: ini File Utility, version 2.0*, available at **www.apc.com**.

# The Upload Event and Error Messages

The following event occurs when the receiving unit completes using the .ini file to update its settings.

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

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

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

### Messages in config.ini

A unit from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the unit is not present or is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values. For example: `xRDU not discovered`

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

### Errors generated by overridden values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values. See “Contents of the .ini file” on page 100 for information about which values are overridden.

Because the overridden values are device-specific and not appropriate to export to other units, ignore these error messages. To prevent these error messages, delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

# Related Topics

On Windows operating systems, instead of transferring .ini files, you can use the Device IP Configuration Wizard to update the basic TCP/IP settings of the unit and configure other settings through its user interface. See “Device IP Configuration Wizard” on page 99.

# Firmware File Transfer Methods

**NOTE:** Upgrade the bootmon module first, then the AOS module, and finally, the application module by placing them on the unit in that order.

Obtain the free, latest firmware version from the Schneider Electric web site. To upgrade the firmware of one or more units, use 1 of these 5 methods:

- On a Windows operating system, use the **Firmware Upgrade Utility** downloaded from the web site **www.apc.com**.
- On any supported operating system, use **FTP or SCP** to transfer the individual AOS and application firmware modules.
- For a unit that is NOT on your network, use **XMODEM** through a serial connection to transfer the individual firmware modules from your computer to the unit.
- Use a **USB drive** to transfer the individual firmware modules from your computer.
- For upgrades to multiple units, see “Upgrading the firmware on multiple units” and “Using the Firmware Upgrade Utility for multiple upgrades on Windows”.

## Using the Firmware Upgrade Utility

This Firmware Upgrade Utility is part of the firmware upgrade package available on the **www.apc.com** website. (*Never* use an Upgrade Utility designated for one product to upgrade the firmware of another product).

**Using the Utility for upgrades on Windows-based systems.** On any supported Windows operating system, the Firmware Upgrade Utility automates the transferring of the firmware modules, *in the correct module order*.

Unzip the downloaded firmware upgrade file and double-click the .exe file. Then enter the IP address, the user name, and the password in the dialog fields and click **Upgrade Now**. You can use the **Ping** button to test your entered details.

**Using the Utility for manual upgrades, primarily on Linux.** On non-Windows operating systems, the Firmware Upgrade Utility extracts the individual firmware modules, but does not upgrade the unit.

To extract the firmware files:

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

### Use FTP or SCP to upgrade one unit

**FTP.** To use FTP to upgrade a unit over the network:

- The unit must be on the network, with its system IP, subnet mask, and default gateway configured.
- The FTP server must be enabled at the unit.

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

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

   ```
   C:\>cd apc

   C:\apc>dir
   ```

3. Open an FTP client session:

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

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

   - For Windows FTP clients, separate a non-default port number from the IP address by a space. For example (showing a space before 21000):
     `ftp> open 150.250.6.10 21000`
   - Some FTP clients require a colon instead before the port number.

5. Log on as Administrator.
6. Upgrade the AOS. (Always upgrade the AOS before the application module).
   `ftp> bin`
   `ftp> put apc_hw05_aos_`*`nnn`*`.bin` (where *`nnn`* is the firmware version number)
7. When FTP confirms the transfer, type `quit` to close the session.
8. After 20 seconds, repeat step 3 through step 7, using the application module file name at step 6,

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

1. Locate the firmware modules, see “Using the Utility for manual upgrades, primarily on Linux.” on page 104.
2. Use an SCP command line to transfer the AOS firmware module to the unit. The following example uses *`nnn`* to represent the version number of the AOS module:

   `scp apc_hw05_aos_`***`nnn`***`.bin apc@158.205.6.185:apc_hw05_aos_`***`nnn`***`.bin`

3. Use a similar SCP command line, with the name of the application module, to transfer the application firmware module to the unit. (Always upgrade the AOS before the application module).

### Use XMODEM to upgrade one unit

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

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

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect the provided serial configuration cable (part number 940-0144A) to the selected port and to the RJ-12 style serial port at the unit.
3. Run a terminal program such as HyperTerminal, and configure the selected port for 57600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press the **Reset** button on the unit, then immediately press the **Enter** key twice, or until the Boot Monitor prompt displays: `BM>`
5. Type `XMODEM`, then press ENTER.
6. From the terminal program’s menu, select XMODEM, then select the binary AOS firmware file to transfer using XMODEM. After the XMODEM transfer is complete, the Boot Monitor prompt returns.

   (Always upgrade the AOS before the application module).
7. To install the application module, repeat step 5 and step 6. In step 6, use the application module file name.
8. Type `reset` or press the **Reset** button to restart the unit’s management interface.

### Use a USB drive to transfer and upgrade the files

Use a USB drive to transfer and upgrade the files. Before starting the transfer, make sure the USB drive is formatted in FAT32.

1. Download the firmware upgrade files and unzip them.
2. Create a folder named **apcfirm** on the USB flash drive.
3. Place the extracted module files in the **apcfirm** directory.
4. Use a text editor to create a file named *upload.rcf*. (The file extension must be .rcf, not .txt for example.)
5. In *upload.rcf*, add a line for each firmware module that you want to upgrade. For example, to upgrade to **bootmon** version 1.0.5, **AOS** v6.0.9, and XRDP application version v6.0.9, type:

   ```
   BM=apc_hw05_bootmon_105.bin

   AOS=apc_hw05_aos_609.bin

   APP=apc_hw05_xrdp_609.bin
   ```
6. Place upload.rcf in the apcfirm folder on the flash drive.
7. Insert the flash drive into a USB port on your unit.
8. Press the display **Reset** button and wait for the card to reboot fully.
9. Check that the upgrade was completed successfully using the procedures in “Verifying Upgrades”.

## How to upgrade multiple units

Use one of these three methods:

- **Firmware Upgrade Utility:** Use this for multiple firmware updates in IPv4 if you have Windows. The utility records all upgrade steps in a log as a good reference to validate the upgrade.
- **Export configuration settings:** You can create batch files and use a utility to retrieve configuration settings from multiple units and export them to other units. See *Release Notes: ini File Utility, version 2.0,* available in the Knowledge Base at **www.apc.com**
- **Use FTP or SCP to upgrade multiple units:** To upgrade multiple units using an FTP client or using SCP, write a script which automatically performs the procedure.

**NOTE:** Utility is available from the Knowledge Base: **www.apc.com/support**

## Using the Firmware Upgrade Utility for multiple upgrades

After downloading the Upgrade Utility, double click on the .exe file to run the utility (which ONLY works with IPv4) and follow these steps to upgrade your firmware:

1. Type in an IP address, a user name, and a password, and choose the **Ping** button if you need to verify an IP address.
2. Choose the **Device List** button to open the `iplist.txt` file. This should list any device IP, user name, and password.

   For example,

   ```
   SystemIP=192.168.0.1
   SystemUserName=apc
   SystemPassword=apc
   ```

   You can use an existing *iplist.txt* file if it already exists.
3. Select the **Upgrade From Device List** check box to use the `iplist.txt` file.
4. Choose the **Upgrade Now** button to start the firmware version update(s).
5. Choose **View Log** to verify any upgrade.

# Verifying Upgrades and Updates

To verify a firmware upgrade succeeded, use the **Network** menu and select the **FTP Server** option to view **Last Transfer Result**, or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

### Last Transfer Result codes

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

### Verify the version numbers of installed firmware.

Verify the versions of the upgraded firmware modules: **Configuration** > **General** > **About**, or use an SNMP GET to the MIB II **sysDescr** OID.

# Troubleshooting

# Access Problems

For problems that persist or are not described here, contact Schneider Electric Customer Care at **www.apc.com**.

| Problem | Solution |
|---|---|
| Unable to ping the unit | The unit supports the ability to disable IPv4 Ping Response for security reasons.<br>This setting is located in the web UI under Configuration > Security > Ping Response or can be located in config.ini. Check this setting or verify other access methods such as HTTPS, FTP, Telnet, or SSH.<br>If the unit's Status LED is green, try to ping another node on the same network segment as the unit. If that fails, it is not a problem with the unit. If the Status LED is not green, or if the ping test succeeds, perform the following checks:<br>• Verify all network connections.<br>• Verify the IP addresses of the unit and the NMS.<br>• If the NMS is on a different physical network (or subnetwork) from the unit, verify the IP address of the default gateway (or router).<br>• Verify the number of subnet bits for the unit's subnet mask. |
| Cannot allocate the communications port through a terminal program | Before you can use a terminal program to configure the unit, you must shut down any application, service, or program using the communications port. |
| Cannot access the command line interface through a serial connection | Make sure that the correct serial cable is connected to the serial port.<br>Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400. |
| Cannot access the command line interface remotely | • Make sure you are using the correct access method, Telnet or Secure SHell (SSH). These can be enabled or disable independently. The Super User or an Administrator can enable these access methods. By default, Telnet is enabled..<br>• For SSH, the unit may be creating a host key. The unit can take up to one minute to create the host key, and SSH is inaccessible for that time. |
| Cannot access the web interface | • Verify that HTTP or HTTPS access is enabled.<br>• Make sure you are specifying the correct URL — one that is consistent with the security system used by the unit. SSL requires **https**, not **http**, at the beginning of the URL.<br>• Verify that you can ping the unit.<br>• Verify that you are using a Web browser supported for the unit.<br>• If the unit has just restarted and SSL security is being set up, the unit may be generating a server certificate. The unit can take up to one minute to create this certificate, and the SSL server is not available during that time. |

# SNMP Issues

| Problem | Solution |
|---|---|
| Unable to perform a GET | • Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3).<br>• Use the command line interface or UI to ensure that the NMS has access. |
| Unable to perform a SET | • Verify the read/write (SET) community name (SNMPv1) or the user profile configuration (SNMPv3).<br>• Use the command line interface or UI to ensure that the NMS has write (SET) access (SNMPv1) or is granted access to the target IP address through the access control list (SNMPv3). |
| Unable to receive traps at the NMS | • Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the NMS as a trap receiver.<br>• For SNMP v1, query the **mconfigTrapReceiverTable** MIB OID to verify that the NMS IP address is listed correctly and that the community name defined for the NMS matches the community name in the table. If either is not correct, use SETs to the **mconfigTrapReceiverTable** OIDs, or use the command line interface or UI to correct the trap receiver definition.<br>• For SNMPv3, check the user profile configuration for the NMS, and run a trap test. |
| Traps received at an NMS are not identified | See your NMS documentation to verify that the traps are properly integrated in the alarm/trap database. |

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France
+ 33 (0) 1 41 29 70 00
www.se.com
As standards, specifications, and design change from time to time,
please ask for confirmation of the information given in this publication.
© 2019 – 2024 Schneider Electric. All rights reserved.

**990-5787B** **2/2024**