

APC by Schneider Electric
(www.apc.com)
APC part number: 990-4633A

RELEASE NOTES for PDPM150G6F, PDPM150L6F, PDPM175G6H

Released: 31 January 2013

Affected Revision Levels:

apc_hw05_aos_519.bin	Network Management Card Operating System & TCP/IP Stack for Hardware Platform v05
apc_hw05_xrdp_512.bin	Application for Modular Distribution
powernet407.mib	PowerNet(R) SNMP Management Information Base (MIB)

For details on upgrading the Network Management Card's firmware, see the User's Guide on the Utility CD or on the APC Web site (www.apc.com).

APC Device IP Configuration Wizard v5.0.1

The wizard is a windows application designed specifically to remotely configure the basic TCP/IP settings of Network Management Cards. The wizard runs on windows(R) 2000, windows 2003, windows Vista, windows XP, windows 7, and windows Server 2008.

The wizard is available as a free download from the APC web site. On the web site, search by part number SFDIPW501 to find the downloadable file.

Table of Contents:

- 1.0 OS & TCP/IP Stack Modifications (apc_hw05_aos_519.bin)
 - 1.1 COMPATIBILITY
 - 1.2 KNOWN ISSUES IN THIS VERSION
 - 1.3 NEW FEATURES & ENHANCEMENTS SINCE AOS v5.1.8
 - 1.4 BUGS FIXED IN THIS VERSION SINCE AOS v5.1.8
- 2.0 Application for Modular Distribution (apc_hw05_xrdp_512.bin)
 - 2.1 COMPATIBILITY
 - 2.2 KNOWN ISSUES IN THIS VERSION
 - 2.3 NEW FEATURES & ENHANCEMENTS SINCE APP v5.1.1
 - 2.4 BUGS FIXED IN THIS VERSION SINCE APP v5.1.1
- 3.0 APC Device IP Configuration Wizard v5.0.1
 - 3.1 COMPATIBILITY
- 4.0 Miscellaneous
 - 4.1 RECOVERING FROM A LOST PASSWORD
 - 4.2 EVENT SUPPORT LIST
 - 4.3 POWERNET MIB REFERENCE GUIDE

1.0 OS & TCP/IP Stack Modifications (apc_hw05_aos_519.bin)

1.1 COMPATIBILITY

apc_hw05_xrdp_512.bin Application for Modular Distribution

1.2 KNOWN ISSUES IN THIS VERSION

1. Performing manual edits (using some editors, e.g. Notepad) to the Config.ini file with UTF-8 characters may result in unrecognized characters being appended to the file. This may result in error messages being logged when these characters are processed. However, the Config.ini file is still processed correctly.
2. The SNMPv1 "communityString" OID allows 15 characters but should allow 16.
3. The NMC Upgrade utility supports ASCII characters only for username and password.
4. When upgrading from 5.0x systems, IP addresses in the event log for preexisting events (that is, events which PRECEDED the upgrade) will cause the creation of miscellaneous odd characters in the log. This will NOT corrupt the log. Log entries made after the upgrade will represent properly as expected.
5. When upgrading from 5.0x systems, if NTP (network time protocol) is not enabled, the NMC clock will need to be set manually.
6. Non-ASCII characters conveyed to an ISX Manager will not display properly in ISXM.
7. The following fields do not accept UTF-8 characters (they accept ASCII only):
 - any numeric field (only Arabic numbers are accepted)
 - the Datalog FTP Server name.
8. The following warning events do NOT cause the Network Management Card to send an SNMP trap:
 - System: Detected an unauthorized user attempting to access the FTP interface.
 - System: Password Changed
9. In the Config.ini file, the [EventActionConfig] keys may report incorrect data when performing a mass configuration.
10. In the CLI, the "system" command accepts Name, Contact, and Location values that exceed the character limit, but the UI truncates those values in the logon banner.
11. The device and outlet user privileges in the CLI are not consistent with the device and outlet user privileges in the web interface.
12. Using the Config.ini file to configure the following keys in the [SystemUserManager] and [SystemDateTime] sections may cause the web interface to display the following values incorrectly:
 - ReadOnlyUserName
 - DeviceUserName
 - AdminUserName
 - NTPPrimaryServer
 - NTPSecondaryServer

13. User names can be defined using the Config.ini file, but by default password keys are no longer included. Transferring an unedited Config.ini file in the old format (with password keys) can cause unintended user name/password pairs unless the user name field is removed from the file.
14. When SNMPV3 access is enabled, disabling SNMPV1 access by clearing the "Enable SNMPV1 access" check box has no effect.
15. If the manual upload of the data log is repeated at 90-second intervals, the third upload attempt will fail.
16. In the Config.ini file, the [SystemPreference] key EventLogDisplay shows:
 - 0 instead of Disabled and
 - 1 instead of Enabled.
17. In SNMP browsers, UDP ports are not reported correctly and all TCP ports except the web port are not shown.
18. The NMC supports six SNMP trap receivers, but only four can be configured to receive event notifications.
19. When using Mozilla Firefox, access using HTTP port 6000 is blocked. Microsoft Internet Explorer 6 allows access using HTTP port 6000.
20. In the Web interface, the Primary and Secondary RADIUS servers accept invalid IP address values.
21. In the CLI, the Primary and Secondary RADIUS server commands append the previous server secret to the end of the new server secret.
22. In the Config.ini: the SystemUserManager username keys return strange values when the value is greater than 10 characters in length.
23. In the Config.ini: the SystemDateTime Server keys return strange values when long strings are applied.
24. Domain Name parameter displays result as "Success" for Invalid value in the CLI.
25. The usernames for Admin, Device and Read-only users allow longer strings than the 64-character limit in the Config.ini file.
26. The User Link Display name configuration exceeds 20 characters when using a Config.ini file.
27. The Quick Links Display name configuration only allows 6 characters in the web text box.
28. The snmp mib2 udp/tcp connection tables are incorrect.
29. There are different Date Formats on the NMC General/About page.
30. The CLI does not process HOME or END keys properly.
31. The CLI command history buffer continuously wraps around, instead of stopping at the end/beginning.
32. In the Config.ini: SystemLinks, LinkName and LinkDisplay fields truncate values which are too long.

33. The Web UI Device and Read Only Username fields don't report a form failure when submitting an empty string.
34. The DNS Domain Name validation doesn't conform to RFC 1035 Standards for formatting.
35. The Config.ini keywords "LinkDisplay" and "LinkName" in the [SystemLinks] section accept a NULL value.
36. The Trap receiver NMS settings incorrectly allow for a NULL entry.
37. The SNMP v1 and v3 Community Access Addresses incorrectly allow for a NULL entry.
38. The SNMP v1 Trap Community Name incorrectly accepts values greater than the max of 15 and NULL.
39. The Syslog Server address incorrectly accepts a NULL entry.
40. The Config.ini for RMS Configuration incorrectly accepts values greater than allowed.
41. Browsing to a logon page directly after a previous logon results in a temporary logon failure.
42. When data log rotation is enabled or disabled, the event log will log the same event "System: Configuration change. Data log rotation enable". This is misleading if the rotation was disabled.
43. NMC does not respond to ipAdEntNetMask OID via SNMP.
44. NMC may warmstart during periods of large network activity.
45. Some event logs may not be displayed when the event log filter is set to an option other than "All Logs".
46. In SNMP: sysUpTime OID is continuously lagging from actual NMC UP time value.
47. Configuring a fourth email recipient may cause the following event, "System: Email: Could not mail, queue full."
48. May not be able to upload a config.ini file via the web interface when HTTPS is enabled. Workaround is to use FTP method.

1.3 NEW FEATURES & ENHANCEMENTS SINCE AOS v5.1.8

1. None.

1.4 BUGS FIXED IN THIS VERSION SINCE AOS v5.1.8

1. Fixed small memory leak when DHCP bootfile option is in use.

2.0 Application for Modular Distribution (apc_hw05_xrdp_512.bin)

2.1 COMPATIBILITY

apc_hw05_aos_519.bin Network Management Card OS & TCP/IP Stack

See 1.0 OS & TCP/IP Stack Modifications (apc_hw05_aos_519.bin) for a list of modifications and enhancements that affect this application version.

2.2 KNOWN ISSUES IN THIS VERSION

1. None.

2.3 NEW FEATURES & ENHANCEMENTS SINCE APP v5.1.1

- Section 1.3 enumerates the features & enhancements for the 5.1.9 system.

1. Improved support for 2-pole breaker modules.
2. Added support for automatic update of embedded metering board processors during initialization if applicable.

2.4 BUGS FIXED IN THIS VERSION SINCE APP v5.1.1

1. Alarms reported for non-existent pole of 2-pole breakers. (MODPDUFULL-171)

3.0 APC Device IP Configuration Wizard v5.0.1

3.1 COMPATIBILITY

apc_hw05_aos_519.bin and prior Network Management Card OS & TCP/IP Stack

4.0 Miscellaneous

4.1 RECOVERING FROM A LOST PASSWORD

See the User's Guide on the APC web site (www.apc.com) for instructions on how to recover from a lost password.

4.2 EVENT SUPPORT LIST

For the event names and event codes for all events supported for a currently connected APC device, first retrieve the config.ini file from the attached Network Management Card.

To use FTP to retrieve config.ini from a configured Network Management Card:

1. Open a connection to the Network Management Card, using its IP Address:
2. Log on using the Administrator user name and password.
3. Retrieve the config.ini file containing the settings of the Network Management Card of the UPS.

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

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

In the config.ini file, find the section heading [EventActionConfig]. In the list of events under that section heading, substitute 0x for the initial E in the code for any event to obtain the hexadecimal event code shown in the user interface and in the documentation.

For example, the hexadecimal code for the code "E0033" in the config.ini file (for the event "System: Configuration change") is "0x0033".

4.3 POWERNET MIB REFERENCE GUIDE

NOTE: The MIB Reference Guide, available on the APC web site (www.apc.com), explains the structure of the MIB, types of OIDs, and the procedure for defining trap receivers. For information on specific OIDs, use a MIB browser to view their definitions and available values directly from the MIB itself. You can view the definitions of traps at the end of the MIB itself (powernet407.mib, downloadable from the APC web site, www.apc.com).