Release Notes
Rack Power Distribution Unit
with Network Management Card 2

Revised: October 2018
Release Notes for: AP7xxxB and AP8xxx series Rack PDUs and AP71xxB Inline Current Meters

Affected Revision Levels

Component	File	Details
APC Operating System	apc_hw05_aos_664.bin	Network Management Card (NMC) Operating System & TCP/IP Stack for Hardware Platform v05.
rpdu2g Application	apc_hw05_rpdu2g_664.bin	Rack Power Distribution Unit Application
PowerNet® Application	powernet427.mib	PowerNet SNMP Management Information Base (MIB)

For details on upgrading the firmware for your Rack PDU, see the User Guide on the website, www.apc.com.

Device IP Configuration Wizard

The Device IP Configuration Wizard is a Windows application designed specifically to remotely configure the basic TCP/IP settings of Network Management Cards. The Wizard runs on Windows® 2000, Windows Server 2003, Windows Server 2012, and, on 32- and 64-bit versions of Windows Vista, Windows XP, Windows Server 2008, Windows 7, Windows 8, and Windows 10 operating systems. This utility supports cards that have firmware version 3.X.X or higher and is for IPv4 only.

The Wizard is available as a free download from the APC by Schneider Electric website at www.apc.com:

1. Go to www.apc.com/tools/download and select '**Software Upgrades - Wizards and Configurators**' from the '**Filter by Software/Firmware**' drop-down list
2. Click '**Submit**' to view the list of utilities available for download.
3. Click on the '**Download**' button to download the **'Network Management Device IP Configuration Wizard**'.

Table of Contents

- New Features
- Fixed Issues
- Known Issues
- Miscellaneous
  - Recovering from a Lost Password
  - Event Support List
  - PowerNet MIB Reference Guide
  - Hash Signatures

New Features

APC Operating System (apc_hw05_aos_664.bin)

- **NMC Security Wizard Command Line Interface (CLI) Utility.** Soon-to-release updated tool with CLI-only interface and security enhancements. Includes fix for "-32 Bad Data" with non-default template MS Cas.
- **ROBOT Vulnerability Mitigation.** Added support for ROBOT TLS vulnerability mitigation using new `cipher` CLI command or INI configuration option. **NOTE:** This mitigation is not compatible with some web browsers.

rpdu2g Application (apc_hw05_rpdu2g_664.bin)

- Added new feature for LCD to display loads numerically. The user can choose whether to display certain loads in graph form (default) or numerically on the LCD
- Added SNMP MIB support for bank circuit breaker rating to rPDU2BankPropertiesTable. New OID name is rPDU2BankPropertiesBreakerRating

Fixed Issues

APC Operating System (apc_hw05_aos_664.bin)

- **Web-Based White Screen Fix.** Fixed an issue which caused a blank white screen for some users caused by an abnormally large number of cookies present in the Web browser client accessing the NMC.
- **SSL/TLS certificates issued by third party now accepted.** Fixed issue which prevented NMC from accepting SSL/TLS certificates issued by third party Certificate Authorities such as Microsoft Certificate Services, especially those using custom certificate templates.

rpdu2g Application (apc_hw05_rpdu2g_664.bin)

- AP8XXX only : Fixed to correctly display the environmental alarms on the Environmental Configuration page of the web interface when in a Network Port Sharing (NPS) configuration.
- Fixed to clear "Firmware Mismatch" warning message without reboot when PDUs are in a Network Port Sharing (NPS) configuration and when host and guest are updated with the same firmware version.
- Fixed a firmware update issue when using Network Port Sharing (NPS).

Known Issues

APC Operating System (apc_hw05_aos_664.bin)

- Disabling an individual event for email notification may cause an unexpected network interface restart.
- Modifying RADIUS settings via config.ini may cause an unexpected network interface restart.
- The NMC may experience an unexpected network interface restart while editing a firewall policy.
- Modifying large groups of vent actions by severity may cause an unexpected network interface restart.
- IPv6 connectivity outside of local subnet does not work in all environments.
- When using Syslog TCP, there is no line break at the end of the payload message.
- SNMPv3 communication and monitoring on some third-party SNMP management tools such as ManageEngine OpManager does not work properly.
- When using Syslog TCP, there is no line break at the end of the payload message.
  SNMPv3 communication and monitoring on some third party SNMP management tools such as ManageEngine OpManager does not work properly.

rpdu2g Application (apc_hw05_rpdu2g_664.bin)

- Should a user attempt to configure a phase's Overload Alarm with a value that is above the maximum load value, configuration errors in Near Overload and Low Load Warning values to obtain environmental sensor status (if connected) will not be reported on the screen. These entries will be rejected along with the Overload Alarm entry, but notification will not be put on the screen for those fields.
- AP8XXX only: In a Network Port Sharing group, if a unit has an active alarm upon startup and the unit changes its display ID, the alarm may remain in the active alarm list even after the alarm condition clears.
- If a breaker is tripped on an AP84xx or AP86xx SKU with two outlet banks (AP8441, AP8453, AP8641, AP8653), outlets 9 through 16 may report incorrect measurements.
- AP8XXX only: A complete config.ini upload to a Rack PDU in a Network Port Sharing group may take a long time. For example: A Rack PDU in a Network Port Sharing group with three other Rack PDUs may take 30 minutes to complete the upload.
- AP8XXX only: A unit in a Network Port Sharing group with a letter in the seventh or eighth positions of its serial number may generate a communication lost alarm upon upgrading from 6.1.0 or earlier to 6.3.3 or later. This alarm may be cleared and should not repeat in future upgrades.
- A unit with over 24 switched outlets (such as AP8965X671) may show a load reading on phase L1, even with no load connected on outlets. This is due to the number of outlet relays drawing power from the input phase.
- AP8XXX only: In Network Port Sharing configuration, StruxureWare Data Center Expert may take more than 4 minutes to discover a Rack PDU.
- When controlling a synchronized outlet group with the Web UI, the Outlet User may receive a warning that the control action was not successful when it actually was successful.

Miscellaneous

Recovering from a Lost Password

See the User Guide on the website, www.apc.com for instructions on how to recover from a lost password.

Event Support List

To obtain the event names and event codes for all events supported by a currently connected APC by Schneider Electric device, first retrieve the config.ini file from the Network Management Card.
To use FTP to retrieve config.ini from a configured Network Management Card:

1. Open a connection to the NMC, using its IP Address:
   `ftp > open <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:
   `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.

PowerNet MIB Reference Guide

NOTE: The MIB Reference Guide, available on the website, www.apc.com, explains the structure of the MIB, types of OIDs, and the procedure for defining SNMP 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 (the file powernet427.mib downloadable from the website, www.apc.com).

Hash Signatures

MD5 Hash: 8eb60fe151c90533ec4b1f7f4d86be84
SHA-1 Hash: c7040197208dddd718a7e1a42849535cdc5cf42d
SHA-256 Hash: c6cc4d953ba0edc3409d335a8fcb5236c8bd18a2c6e86790b707bd9933bf22b1

Copyright © 2018 Schneider Electric. All rights reserved.

990-9958D

10-2018