Release Notes
Rack Power Distribution Unit
with Network Management Card 2

Revised: July 2019
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_682.bin	Network Management Card (NMC) Operating System & TCP/IP Stack for Hardware Platform v05.
rpdu2g Application	apc_hw05_rpdu2g_680.bin	Rack Power Distribution Unit Application
PowerNet® Application	powernet430.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

APC Operating System (apc_hw05_aos_682.bin)

- **California Law.** Due to the introduction of a US California state law (Senate Bill SB-327), which starts on January 1st, 2020, any manufacturer of a device that connects "directly or indirectly" to the internet must equip it with "reasonable" security features, designed to prevent unauthorized access, modification, or information disclosure. The following security features have been implemented:
  - The first time the Super User successfully logs on with the default credentials, they will be presented with a screen requiring them to change their password. It is strongly recommended that users create strong passwords which adhere to their company's password requirements.
  - The user accounts which are shipped on the NMC are disabled by default. These accounts cannot be enabled until the user changes the associated passwords for each account.
  - New User Account Creation: A user account can be created in the Web UI without a password being specified. These accounts cannot be enabled until a password is added. In the CLI, a password is required to create a user account.
  - Protocol Status Overview Screen: The protocol status overview screen contains a list of current system protocols and their current enabled values. This feature is available in the Web and CLI.
    - Web UI: On first logon, the user is directed to the Protocol Status Overview page. The web page can be accessed at any point thereafter from **Configuration > Network > Summary**.
    - CLI: The existing banner has been modified to permanently include the current system protocols and their current values. This will show every time the user logs in to the CLI as it currently does.
  - All login protocols are now disabled by default, with the exception of SSH, HTTPS, and console (serial or USB).
    - These protocols allow the user to change the password.
    - While FTP is a standard, albeit unsecure login method, there is no way to force the password change through this interface, so it is disabled by default.
    - HTTP and telnet are simply unsecure due to network data being transmitted in clear text, so it is disabled by default.
  - Some communication protocols have been disabled by default until the user changes their associated passwords, community names, or authentication/encryption phrases:
    - SNMPv1 is disabled by default and the community names are blank.
    - SNMPv3 auth priv phrases are blank by default.
  - SCP will not allow a file transfer until the initial super user password is changed.
- Remote Monitoring Service (RMS) has been removed.
- An EcoStruxure logo/link has been added to the login page and application header pages.

rpdu2g Application (apc_hw05_rpdu2g_680.bin)

None.

Fixed Issues

APC Operating System (apc_hw05_aos_682.bin)

- SNMPv3 settings changed on CLI now take effect correctly.
- The SNMPv3 configuration is applied properly when changed through the CLI.
- The NMC no longer hosts HTTP when HTTP is disabled.

rpdu2g Application (apc_hw05_rpdu2g_680.bin)

None.

Known Issues

APC Operating System (apc_hw05_aos_682.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 event actions by severity may cause an unexpected network interface restart.
- IPv6 connectivity outside of local subnet does not work in all environments.
- SNMPv3 communication and monitoring on some third-party SNMP management tools such as ManageEngine OpManager does not work properly.
- SNMP traps do not work for some AOS events.
- File transfers using SCP do not work properly with WinSCP client.
- Certain privileges in the CLI are not consistent with the user privileges in the Web UI.
- The Trap receiver NMS settings incorrectly allow for a NULL entry.
- SNMP Trap Recipients are activated only after a previous Trap recipient can send Traps.
- Firewall rules configured through the Web UI are active even when the firewall is not enabled. A fix to this issue is planned for an upcoming release.

rpdu2g Application (apc_hw05_rpdu2g_680.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 was successful.
- When the host of a Network Port Sharing group has a single phase, the Phase Balance table does not change color to reflect alarm status.
- If the clearing method for an outlet alarm action is set to **Auto**, outlets are automatically set to the non-action state when an alarm clears, regardless of what state they were in before the alarm. For example, if the alarm action is **Off**, the outlets are turned on when the alarm clears. This happens even if the outlets were off before the alarm started.
- The new CLI command `phBalAlGen` is not yet functional and returns "`Command not found`."
- Outlet Energy values are reset to 0 after a reboot.

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 powernet430.mib downloadable from the website, www.apc.com).

Hash Signatures

MD5 Hash: 959c598ede6e4999d8d450a63fc5def3
SHA-1 Hash: 967e71f76da903e5460d111ff8da1da110086406
SHA-256 Hash: f55af32265b1708f47eb16c9ccd555fe04340abc4034906693f7141143c6fa63

990-9958G

07-2019