Release Notes
Rack ATS AP44XX Series
with Network Management Card 2

Revised: April 2019

Release Notes for:

AP4421	AP4424	AP4432	AP4450	AP4453
AP4422	AP4430	AP4433	AP4452	
AP4423	AP4431	AP4434	AP4452J	

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.
ATS Application	apc_hw05_ats4g_680.bin	Automatic Transfer Switch Application
PowerNet® Application	powernet430.mib	PowerNet® SNMP Management Information Base (MIB)

For details on upgrading the firmware for your ATS, 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

Top ↑

APC Operating System (apc_hw05_aos_672.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.
- **802.1x (EAPoL) w/ TLS.** EAPoL is network-port access which is necessary for sites which require the network device to authenticate with a RADIUS server (through a network switch) prior to being granted general access to the target network.
- **Elliptical Curve Cryptography (ECC).** ECDHE has been implemented and provides more secure communication for HTTPS Web access. RC4 and MD5 are no longer available.

ATS4G Application (apc_hw05_ats4g_680.bin)

None.

Fixed Issues

Top ↑

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.
- Added configuration option for Limited Status Web page to CLI and config.ini.
- CVE-2018-7820: Fixed in v6.7.2. A clear text password vulnerability has been fixed in the Remote Monitoring Service (RMS). APC by Schneider Electric recognizes Taran Dhillon of Hacklabs for identifying this vulnerability.

ATS4G Application (apc_hw05_ats4g_680.bin)

ATS models AP4423 and AP4422 no longer reset customer settings for Line VRMS and VRMS limits when power is removed from the ATS.

Known Issues

Top ↑

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 interface are active even when the firewall is not enabled. A fix to this issue is planned for an upcoming release.

ATS4G Application (apc_hw05_ats4g_680.bin)

- Voltage out checking is not currently supported; any approach to reading the output voltage will always result in a reading of voltage present, regardless of its actual status.
- False alarms may occur when the line voltage is set to the minimum or maximum value.
- If Source A is not active, a `resetToDef` (reset to default values) command may cause an output load drop for approximately 5 seconds
- A Spike/Dropout event may occur when operating with two nominal voltage sources at 50 Hz if the 10 Hz Frequency Deviation setting is used.
- If the frequency deviation is set to 10 Hz and the frequency of a source is offset by 10 Hz, the ATS will incorrectly disqualify that source.
- When both sources are set to 50 Hz or 60 Hz, the unit automatically changes the nominal frequency to match the source frequency.
- SNMP OID's Output Minimum Current & Output Maximum Current are not currently supported. Related parameters in Web UI and CLI are also not implemented yet.
- SNMP OID atsStatusVoltageOutStatus is not currently supported and will always return Vout = OFF.
- In rare cases, a fast source switch may occur and may cause internal fuses to open when there is a voltage spike or dropout on the selected input.
- When line voltage is set to the minimum allowable value, the ATS may fail to report an over-voltage alarm. The ATS will still switch sources in the case of an over-voltage alarm.
- When line voltage is set to the minimum allowable value, the ATS may fail to report an over-voltage alarm. The ATS will still switch sources in the case of an over-voltage alarm.Continuous source switching may occur when there is a frequency deviation from the set value (50 or 60 Hz) and the Voltage Transfer Range has been set below 10 V.
- Users may not be able to be clear some lost communication events.
- Freq Out of Range events may not appear in the Event Log if they are of short duration.
- In some cases, the power supply status shows "Normal" even though one of the sources is unavailable.
- Location details cannot be modified via SNMP protocol.
- The SNMP “Contact” OID is not available.

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:

4. Open a connection to the NMC, using its IP Address:
   `ftp > open <ip_address>`
5. Log on using the Administrator user name and password.
6. 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 powernet430.mib file is downloadable from the website, www.apc.com).

Hash Signatures

MD5 Hash:
SHA-1 Hash:
SHA-256 Hash:

990-91032E

8-2019