Rack ATS with Network Management Card 3

AP44XXA models

What's in This Document

Affected Revision Levels 1
Device IP Configuration Utility 2
New Features 3
Fixed Issues 4
Known Issues 4
Miscellaneous 5
Recover from a Lost Password 5
Event Support List 5
PowerNet MIB Reference Guide 5
Hash Signatures 6

Affected Revision Levels

Component	Version	Details
APC Operating System	3.4.0.7	Network Management Card (NMC) Operating System
ATS Application	apc_hw21_ats5g_3.4.0.2.nmc3	ATS 5G Application
Update Utility	apc_hw21_ats5g_3.4.0.2.exe	Update Utility
PowerNet® Application	powernet458.mib	PowerNet SNMP Management Information Base (MIB)

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

Device IP Configuration Utility

SNMP is disabled by default, and must be enabled for the Device IP configuration Utility to function. You can enable SNMP from the CLI. See your *User Guide* for instructions to enable snmp from the CLI.

The Device IP Configuration Utility can discover Rack ATS units that do not have an IP address assigned. Once discovered, you can configure the IP address settings for the Network Management Cards (NMCs).You can also search for devices already on the network by entering an IP range to define the search. The Utility scans the IP addresses in the defined range and discovers Rack ATS units that already have a DHCP-assigned IP address.

NOTE:

- For detailed information on the Wizard, see the FAQ article *How do I configure APC Network Management Card network settings?* (FA156064).
- To use the DHCP Option 12, see the FAQ article *Which DHCP options are used when an APC Network Management Device makes a DHCPv4 request?* (FA156110).
- To find an FAQ article, go to www.se.com, and select you location. Then select **Support > Documentation & Software Downloads** and enter the article number or title of the FAQ in the Search bar.

System Requirements

The Device IP Configuration Utility 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, Windows 8, and Windows 10 operating systems. The Device IP Configuration Utility supports Network Management Cards that have firmware version 3.0.x or higher and is for IPv4 only.

Install the Device IP Configuration Utility

1. Go to the download center at www.se.com/ww/en/download, click **Select location**, then select your country from the available options.
2. Enter “Network Management Card Device IP Configuration Utility” in the Search bar. Download the latest version of the Network Management Card Device IP Configuration Utility.
3. Extract the .zip file to your desktop, and run the executable file (*DevIPSetup.exe*).

   NOTE: If you leave the **Start a Web browser when finished** option enabled, you can use **apc** for both the user name and password to access the Rack ATS through your browser.

When Installed, the Device IP configuration Utility is available through the Windows **Start** menu options.

New Features

APC Operating System (AOS 3.4.0.7)

Support for Multi-Factor Authentication (MFA) has been added to enhance login security. MFA introduces an additional layer of protection by requiring users to enter a **One-Time Password (OTP)** sent to their registered email address after successfully authenticating with their username and password.

ATS Application (ATS5G 3.4.0.2)

- A new command has been added to the Command Line Interface (CLI) that allows users to change the **Display ID** of the device. See the *User Guide* on www.se.com for more details.
- SNMP traps have been implemented for **Open Fuse Alarms**, enabling real-time monitoring and alerting through SNMP-based network management systems.

Fixed Issues

APC Operating System (AOS 3.4.0.7)

- The following security vulnerabilities have been addressed in this release:
  - CWE-120: Buffer Copy Without Checking Size of Input

    Resolved an issue where malformed SNMP requests could cause the device to become unresponsive due to improper buffer handling.
  - CWE-613: Insufficient Session Expiration

    Fixed a vulnerability that allowed users to retain access to active sessions even after their password was changed.
  - CWE-476: NULL Pointer Dereference

    Addressed a flaw where malformed IPv4 packets could lead to temporary device inaccessibility due to null pointer dereferencing.
  - CWE-1285: Improper Validation of Specified Index, Position, or Offset in Input

    Improved input validation to prevent improper indexing caused by invalid user inputs.
- The following third-party component (open source or proprietary) has been updated to address a cyber security vulnerability:
  - RADIUS Protocol (RFC 2865)
    - **CVE-2024-3596**: Implemented support for the **Message-Authenticator** attribute to enhance security and mitigate potential vulnerabilities in RADIUS message validation.
- The LDAP TLS connection now functions correctly when connecting via an IP address and using a server certificate with a Subject Alternative Name (SAN) of type iPAddress.
- Resolved an issue where DHCPv6 would intermittently reboot when the network interface was initialized or when the Ethernet cable was reconnected.
- Enhanced logging to provide clearer visibility when user accounts are disabled.
- Updated the expiration date for self-signed certificates to ensure continued validity and compliance.
- Email functionality has been restored for SMTP servers using IPv6 addresses.
- Corrected the severity levels of Syslog-related events in the configuration file to ensure accurate event categorization.

ATS Application (ATS5G 3.4.0.2)

- Users can now reset peak temperature directly through the Web UI.
- Operations such as reboot all, reset to default all, and host selection are now supported via the Web UI for both host and guest devices when connected through NPS.
- Enhanced error handling for CLI commands related to source name, LCD blink, and load operations.
- The SNMP interface now correctly rejects out-of-range values for Line VRMS voltage, VRMS wide limit, and VRMS narrow/medium limits.
- Modbus registers now return “-1” when sensors are disconnected, instead of retaining outdated values.
- ATS now accurately detects sensor disconnection and displays the sensor type as “Not Connected.”
- Device-related sections are now disabled for users with network-only access privileges.
- Devices connected in NPS mode will no longer reboot during configuration of guest and host parameters via Config.ini.
- When enabling or disabling humidity alarms via SNMP, possible open fuse source alarms will no longer be logged in the event logs.

Known Issues

APC Operating System (AOS 3.4.0.7)
None.

ATS Application (ATS5G 3.4.0.2)
None.

Miscellaneous

Recover from a Lost Password

To recover from a lost password, you must reset the Rack ATS to its default configuration. Export the .ini file after configuring your Rack ATS and keep it in a safe place. If you have this file saved, you will be able to retrieve your configuration after a lost password event.

To reset the Rack ATS:

1. On the display interface, hold down the **Reset** button for 20–25 seconds, ensuring the status LED is flashing green during this time. When the status LED changes to orange, release the **Reset** button to allow the Rack ATS to complete its reboot process.
2. Access the Rack ATS through a secure connection with the default username and password (**apc** and **apc**).

   Secure connections include a local connection to the CLI by serial cable, a remote connection to the CLI by SSH, or a connection to the web UI by HTTPS. Instructions for each of these secure connections are covered in this manual. Insecure connections are disabled by default.
3. Reset the username and password, then configure the Rack ATS settings as needed.

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 use FTP to retrieve the config.ini file from the 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

The MIB Reference Guide, available on www.se.com, explains the structure of the MIB, types of OIDs, and the procedure for defining SNMP trap receivers. For information on specific OIDs, use an 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 powernet458.mib is downloadable from www.se.com).

Hash Signatures

apc_hw21_ats5g_3.4.0.2.exe

MD5	b9df04591737160307815e7b61920451
SHA-1	3a1ae5afc3698ba4994a739abbf39d2949db2403
SHA-256	56a54343bff56285a610cb774e0fd8b0267fbaae3ed4ac6e05623d143326ec56