NetShelter™ Rack Power Distribution Units and In-Line Current Meters with NMC3

For APDU11•••, APDU10••• with APDU9640NMC3, APDU9•••, AP8•••, AP7•••B, and AP71••B Devices with NMC3

What's in This Document

Affected Revision Levels 2
New Features 3
Fixed Issues 4
Known Issues 5
Miscellaneous 6
- Additional Software and Documentation 6
- Event Support List 7
- Hash Signatures 7

Schneider Electric;
70 Mechanic Street
02035 Foxboro, MA
USA
www.se.com

Affected Revision Levels

Component	Version	Details
Network Management Card 3 (NMC3) Operating System and NetShelter rPDU Application	AOS: 3.4.0.7 APP: 3.4.0.2	Not available for download
Secure NMC System (SNS) Tool for rPDU	3.0.0.4	Linux: snst_3.0.0.4_nmc3_rpdu2g_3.4.0.2.tar.gz macOS: snst_3.0.0.4_nmc3_rpdu2g_3.4.0.2.tar.gz Windows: snst_3.0.0.4_nmc3_rpdu2g_3-4-0-2.exe
PowerNet® SNMP Management Information Base (MIB)	4.6.2	powernet462.mib

IMPORTANT: You must have a valid Secure NMC System (SNS) subscription (SWNMC3PDU-●Y-DIGI) for PDU devices to update the firmware to version 3.0 or later.

You must use the SNS tool for Rack Power Distribution Units (rPDUs) to upgrade to firmware version 3.0 or later. This is the only supported upgrade method. See “Additional Software and Documentation” on page 6 for instructions to download the SNS Tool and its User Guide.

New Features

APC Operating System (AOS 3.4.0.7)

- Support added for viewing the ARP cache in the Command Line Interface (CLI).
- Security Update:

  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.

  Note: Ensure that NMC user credentials used for SNS Tool, EcoStruxure IT, and Data Centre Expert communications do not have email addresses configured. For additional details, refer to Knowledge Base article FAQ000276382.

APDU11•••, APDU10••• with APDU9640NMC3, APDU9•••, AP8•••, AP7•••B, and AP71••B (rPDU2g 3.4.0.2) Applications

- The rPDU LCD displays the "Alarm Status" to view the details of all the alarms present in the device.
- Support added for Power Sharing in advanced PDUs with Network Port Sharing (NPS). This enables continuous network connectivity and management functions across cascaded units even during individual PDU power loss, preventing the loss of monitoring, alerts, and remote control for the affected PDU.
- Support added for the Redfish protocol.

Fixed Issues

APC Operating System (AOS 3.4.0.7)

- Unsuccessful e-mail tests are now displayed as expected in the Web UI.
- Styling for the “Password Change Required” web page now displays as expected in the latest update of Chrome.
- You can now cancel an initiated firewall test as expected in the Web UI.
- CIDR (Classless Inter-Domain Routing) notation is now allowed in SNMP NMS fields and in firewall fields when operating in subnet mode.
- The CIDR notation is now functional in the DNS field and NMP access is now allowed or blocked based on the ranges associated with the network.
- DNS lookups previously returned unusable IPv6 addresses in certain scenarios when both IPv4 and IPv6 were enabled (default settings). IPv4 is now prioritized if the NMC has an IPv4 address and only a link-local IPv6 address.
- The LDAP TLS connection now works as expected when connecting to an IP address and server certificate using SAN type "iPAddress".
- DHCPv6 no longer intermittently reboots when the network interface starts or when the Ethernet cable is reseated.
- Improved logging for disabled account events.
- The expiration date of self-signed certificates has been updated.
- You can now send emails as expected when the SMTP server uses an IPv6 address.
- The severity of Syslog-related events in the configuration file has been corrected.
- SSH and Telnet sessions now terminate correctly as expected.
- The Web UI now supports the Primary and Secondary DNS fields with a maximum length of 40 characters.
- An error no longer appears when trying to access certain Web UI pages as a Network-Only user.

Security Updates:

- The following security vulnerabilities have been addressed in this release:
  a) CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could cause the device to become unresponsive when malformed SNMP requests are received over the network.
  b) CWE-476: NULL Pointer Dereference vulnerability exists that could cause the device to become temporarily inaccessible when receiving malformed IPv4 packets.
  c) CWE-613: Insufficient Session Expiration vulnerability exists that could cause a user to maintain access to an existing session when their password has been changed.
  d) CWE-863: Incorrect Authorization
  The Network-Only user can only perform actions within the Web UI that corresponds to their access level.
  e) CWE-20: Improper Input Validation
  Incoming BACnet packet sizes are now validated.

Security Updates:

- The following third-party component (open source or proprietary) has been updated to address a cybersecurity vulnerability:
  a) RADIUS Protocol under RFC 2865 - CVE-2024-3596
  Implemented support for the Message-Authenticator attribute.

APDU11•••, APDU10••• with APDU9640NMC3, APDU9•••, AP8•••, AP7•••B, and AP71••B (rPDU2g 3.4.0.2) Applications

- If a sensor is not connected to the device, none of the interfaces will display any parameter values.
- The Bank and Phase current thresholds now support decimals to the tenths place. This feature is supported in the Web UI, CLI, SNMP, and in the configuration file. New OIDs have been added to handle this adaptation on SNMP interfaces.
- "Outlet Name" and "External Link" can be configured through the configuration file.
- Implemented outlet name and threshold configuration through NMC Web UI, Telnet, and CLI for Metered-by-Outlet devices, along with error handling for invalid overload, near-overload, and low-load warning thresholds.
- Resolved an issue that caused Metered-by-Outlet and Metered-by-Outlet with Switching devices to display incorrect phase or bank names when monitoring outlet current.
- Addressed an issue causing the 8K rPDU (Metered/Metered-by-Outlet) devices display to go blank after navigating to outlet current readings.
- Corrected line-to-line voltage display in Delta configuration PDUs across all devices.
- Fixed outlet alarm actions for abnormal state and verified critical severity alarm behavior.
- CLI command "lcdBlink" correctly reports an error when invalid values (e.g. decimal values) are assigned.
- Range is specified in the NMC Web UI for Network-LED blink duration.

Known Issues

None.

Miscellaneous

Additional Software and Documentation

You can download additional software and documentation from the Schneider Electric download center, www.se.com/ww/en/download.

1 Go to www.se.com/ww/en/download.

2 Click **Select Location**, then select your location from the provided list. You cannot download software or documentation until you specify your location.

3 Use the Search bar and the filter fields to find the needed file.

To find a document, enter the name or part number for your equipment in the Search bar. Then select **Installation & User Guides** under **Document Category**.

To find a firmware file, enter the name or part number for the firmware in the Search bar. Then select **Software & Firmware** under **Document Category**.

Software

- The Secure NMC System (SNS) tool for RPDUs (SFNMC3FMTRPDU) upgrades the firmware on your RPDU or In-Line Current Meter. This is the only supported upgrade method for firmware version 3.0 or later.
- The PowerNet MIB allows your SNMP manager to process messages from your RPDU or In-Line Current Meter.
- The Network Management Device IP Configuration Utility (the Utility) is a Windows® application designed specifically to remotely configure the basic TCP/IP settings of Network Management Cards (NMCs). The Utility runs on Windows Vista®, Windows XP®, Windows 2000, Windows 2003, Windows 7, Windows 8, Windows Server® 2008, and Windows Server 2012. The Utility is for IPv4 only.
  To install the Utility, download the latest version of the utility from the Schneider Electric download center. Extract the zip file, then double-click DevIPSetup.exe to install the Utility. You can find instructions to use the Utility in the Utility interface under Help.

Documentation

- The Secure NMC System (SNS) Tool User Guide provides instructions on how to use the SNS tool to upgrade your firmware.
- The *MIB Reference Guide* explains the structure of the MIB, types of OIDs, and the procedure to define SNMP trap receivers. You can download the *PowerNet MIB Reference Guide* from www.se.com.
- 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 powernet462.mib).
- The User Guide for your RPDU or In-Line Current Meter provides comprehensive user instructions, including instructions 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:

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.

Hash Signatures

Linux

snst_3.0.0.4_nmc3_rpdu2g_3.4.0.2.tar.gz

MD5 Hash	9cc1e45c455dece4e73eb43be048a254
SHA-1 Hash	051b1dfda35eaec9dab731d9b5bb1ef4bdb47653
SHA-256 Hash	1b8c4aec8557dd89c860ad122fe2ab77cc24caa1e0ac46a0a36922fb3a1b47c0

macOS

snst_3.0.0.4_nmc3_rpdu2g_3.4.0.2.tar.gz

MD5 Hash	0cd2d09454574fbb33ec48169ebb9000
SHA-1 Hash	e4b04e87ebfe6a7f1262e3d78efb111df685c6a0
SHA-256 Hash	b1d7c950f4065a5252b2edc168bdfca908534b41e0d613ff3ab3914e61cf2a94

Windows

snst_3.0.0.4_nmc3_rpdu2g_3-4-0-2.exe

MD5 Hash	7e77cfc90f93344140ea9658da5ed567
SHA-1 Hash	6d1db51f63e7517146624f2dc1ed1775b613b353
SHA-256 Hash	8be07ccd1845b38c6362a420ac7f5a7d00fe0a54003cdf872a3ea1f0d5e3f64b