Network Management Card 3 (NMC 3) Firmware v1.3.2 for Single-Phase Symmetra Release Notes

Table of Contents

The Single-Phase Symmetra application firmware v1.3.2 release notes apply to the following NMC cards:

- **AP9640 UPS Network Management Card 3**
- **AP9641 UPS Network Management Card 3**

Affected Revision Levels

Component	File	Details
Symmetra Application	apc_hw21_sy_1-3-2.nmc3	UPS Application for Single Phase Symmetra, Symmetra LX

For details on upgrading the UPS Network Management Card 3 (NMC 3) firmware, see the **User Guide** on the APC website.

Schneider Electric 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® Server 2012, Windows Server 2016, Windows Server 2019, Windows 8.1, and Windows 10. This utility is for IPv4 only.

NOTE:

- You cannot search for assigned devices already on the network using an IP range unless you enable SNMPv1 and set the **Community Name** to "public". For more information on SNMPv1, see the **User Guide**.
- When the NMC IP address settings are configured, to access the NMC Web UI in a browser, you must update the URL from http to http**s**.

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

1. Go to https://www.apc.com/shop/us/en/tools/software-firmware and click **Show More** from the list of checkboxes in **Filter by > Software / Firmware**.
2. Select **Wizards and Configurators** to view the list of utilities available for download.
3. Click the Download button to download the **Device IP Configuration Wizard**.

New Features

New Feature
Ripple20 Vulnerability Fixes v1.3.2 addresses Ripple20 vulnerabilities affecting Treck Inc.'s embedded TCP/IP stack, defined in the following CVEs: CVE-2020-11896, CVE-2020-11898, CVE-2020-11899, CVE-2020-11898, CVE-2020-11901, CVE-2020-11902, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-1191. For more information, see Schneider Electric/APC security bulletin: https://www.se.com/ww/en/download/document/SEVD-2020-174-01/

Known Issues

Known Issue
When two NMCs are inserted in a compatible UPS and the firmware version of the NMC in slot 1 is upgraded/downgraded via FTP/SCP, the NMC in slot 2 will lose communications with the UPS. The "UPS: Lost the local network management interface-to-UPS communication" event is logged to the Event Log for the NMC in slot 2.

Miscellaneous

Recovering from a Lost Password

See the User Guide on the APC website 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 device, first retrieve the config.ini file from the attached NMC. To use FTP to retrieve config.ini from a configured NMC:

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 NMC of the UPS:

    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 on the APC website 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 powernet432.mib on the APC website, www.apc.com).

Hash Signatures

Signatures	apc_hw21_sy_1-3-2.nmc3
CRC32	819F5C92
CRC64	76CD59B3A7605B95
SHA-256	BC19528657F82EBB3F6112A3BF3E45F3196E8439B8D93C6AA4DD0F300E5333BA
SHA-1	5532E1AD468693C0C45417620119198556FC6C4E
BLAKE2sp	4982E463D758A46B1BE3190DC205145AE94169020BB5951AA5A54C1B25666253

http://www.apc.com

990-6322A-001

07-2020