

# Network Management Card 2 (NMC 2) Firmware v7.1.2 for InfraStruxure 40 and 60 kVA PDU Release Notes

## Table of Contents

Affected Revision Levels .....	1
Schneider Electric Network Management Device IP Configuration Wizard .....	2
New Features .....	2
Fixed Issues .....	3
Known Issues .....	3
Miscellaneous .....	4
Hash Signatures .....	4

The InfraStruxure 40 and 60 kVA PDU application firmware v7.1.2 release notes apply to the following products:

- PD40G6FK1-M, PD40F6FK1-M, PD40L6FK1-M, PDRPPNX10-M, PD60G6FK1, PD60F6FK1, PD60L6FK1, PDRPPNX10, PD40E5EK20-M, PD40H5EK20-M

## Affected Revision Levels

Component	File	Details
APC Operating System	apc_hw05_aos_712.bin	Network Management Card Operating System & TCP/IP Stack
InfraStruxure 40 and 60 kVA PDU	apc_hw05_xpdu_712.bin	Application for InfraStruxure 40 and 60 kVA PDU

For details on upgrading the UPS firmware, see the [User Guide](#).

## Schneider Electric Network Management 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.

### NOTES:

- In firmware version v1.4.x and higher, it is not supported to assign IP addresses to Network Management Cards using the Wizard.
- 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 https.

The Wizard is available as a free download from the [APC website](#):

1. Go to [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
InfraStruxure 40 and 60 kVA PDU has been updated with the latest aos version 7.1.2.

## Fixed Issues

Fixed Issue
<p style="text-align: center;"><b>Security Vulnerabilities</b></p> <ul style="list-style-type: none"><li>• <b>CWE-16:</b> Configuration – The vulnerabilities in this category during the configuration of the software are now resolved.</li><li>• <b>Cipher Block Chaining (CBC)</b> – Support has been removed as it does not meet modern cryptographic needs, and contains cybersecurity vulnerabilities.</li><li>• <b>CWE-834:</b> Excessive Iteration – The software performs an iteration or loop and now sufficiently limits the number of times that the loop is executed.</li><li>• <b>CWE-79:</b> Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') – The software now correctly neutralizes the user-controllable input before it is placed in a web page output served to other users.</li><li>• <b>CWE-425:</b> Direct Request ('Forced Browsing') – The web application now enforces appropriate authorization on all restricted URLs, scripts, or files.</li><li>• <b>CWE-327:</b> Use of a Broken or Risky Cryptographic Algorithm: This software no longer uses a vulnerable cryptographic algorithm or protocol.</li></ul>
<p style="text-align: center;"><b>Cybersecurity Vulnerabilities</b></p> <p>The following third-part components have been updated to address cybersecurity vulnerabilities.</p> <ul style="list-style-type: none"><li>• SSH Server provided by Cryptlib - CVE-2008-5161</li><li>• TCP/IP provided by Treck - CVE-2004-0230</li><li>• TCP/IP provided by Treck - CVE-2004-0790</li><li>• Treck stack - CVE-2012-5364</li><li>• CWE-200: Exposure of Sensitive Information to an Unauthorized Actor</li><li>• JQuery - CVE-2019-11358</li></ul>

## Known Issues

Known Issue
<p>There are no known issues in this release.</p>

## 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 SCP to retrieve `config.ini` from a configured NMC:

1. Open a connection to the NMC, using its IP Address:  
`scp <admin_username>@<ip_address>:config.ini <filename_to_be_stored>`
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 SCP.

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 `powernet442.mib` on the [APC website](#)).

### Hash Signatures

Signatures	apc_hw05_xpdu_712.bin
MD5	8baca58f6e8238997e866eb92664d989
SHA-1	66e183db1cdf5189c118668bd9accf30a3958145
SHA-256	935c7c9bda67e5dced032b740d3be6a37e0b08ffe496c15d63981e5caef6d531

Copyright © 2024 Schneider Electric. All rights reserved.

<https://www.apc.com>

990-3850G

04-2024