

Product Change Notification Software Release Notes

mPower™ Edge Intelligence Software mPower 5.3.3

MultiTech Conduit® AP Access Point MultiTech Conduit® Programmable Gateway MultiTech Conduit® IP67 Base Station MultiTech Conduit® IP67 200 Series Base Station



Date: March 29, 2021

Product Change Notification (PCN) Number
PCN 03292021-001 (mPower - Conduit)

I. Overview

mPower 5.3.3 is for use on the MultiTech Conduit® Programmable Gateway, Conduit® AP Access Point, and Conduit® IP67 Base Station. mPower 5.3.3 is built using Yocto Thud (version 2.6.X)

- Includes:
 1. New Hardware Support:
 - [Conduit AP Access Point with Power over Ethernet](#)
 - [Conduit IP67 200 Series Base Station](#)
 2. Critical bug fix:
 - [LoRa AS923 with Listen Before Talk Updates](#)
 3. Critical bug fix:
 - [mts-io error](#)
 4. Deprecated Feature:
 - [Native Node-RED, Node.js support](#)
 5. New Features:
 - [Node-RED Custom Application](#)
 - Upgraded CipheSuite
 - Updated factory default behavior
 - LoRa Basics Station
 - LoRa Network Server
 - Differential Updates (delta File)
 - AS923 Frequency Plans
 - Package management and Updates
 6. [Feature Enhancements](#)
- Available for download and included in select devices starting March 2021. See [part numbers impacted](#) for details

Contents

- I. [Overview](#)
- II. [Suggested Action Plan](#)
- III. [mPower 5.3.3 Overview](#)
- IV. [Schedule](#)
- V. [Upgrade Process](#)
- VI. [Part Numbers Impacted](#)
- VII. [mPower Edge Intelligence](#)
- VIII. [Additional Information](#)

II. Suggested Action Plan

Customers

1. Download mPower 5.3.3
2. Evaluate in their environment
3. Deploy to fleet of devices
4. Additional information
 - Technical inquiries: email support@multitech.com
 - Sales inquiries: email sales@multitech.com

Distributors

- Forward this announcement to others within your organization who are actively involved in the sale or support of programmable IoT gateways
- Notify existing customers of this upcoming change and encourage them to evaluate the new firmware with their custom application

III. mPower 5.3.3 Overview

mPower 5.3.3 is built upon mPower 5.2.1.

For details about mPower 5.2.1, refer to [Software Release Notes - mPower 5.2.1](#)

New Hardware Support (mPower 5.3.3):

mPower 5.3.3 includes support for the following new hardware:

1. MultiTech Conduit® AP Access Point – Power over Ethernet models.
 - See [part numbers impacted](#) for details
 - <https://www.multitech.com/documents/publications/data-sheets/86002211.pdf>
2. MultiTech Conduit® IP67 200 Series Base Station
 - See [part numbers impacted](#) for details
 - <https://www.multitech.com/brands/conduit-ip67-200>
3. Support for new Gateway Accessory Card: MTAC-LORA-2G4-3
 - 2.4GHz Gateway Accessory Card [GP-393]
 - Requires MCU version 1.0.1
 - Additional Information: <https://www.multitech.net/developer/software/lora/mtac-lora-2g4-3/>
 - Sales inquiries: email sales@multitech.com

Critical Bug Fix (mPower 5.3.3): LoRa AS923 with Listen Before Talk Updates

mPower 5.3.3 includes the following critical bug fix [GP-964] [GP-997]

Model Numbers Impacted by Bug Fix:

- Japan models: Conduit Programmable Gateway and Conduit IP67 Base Station
- Korea Models: Conduit Programmable Gateway and Conduit IP67 Base Station
- See [part numbers impacted](#) for details

Overview of Bug:

1. Bug has been identified in mPower 5.2.1 and mPower 5.3.0.
2. Bug has also been fixed in mPower 5.2.5 ([Software Release Notes – mPower 5.2.5](#))
3. A combination of FPGA code, LoRa Packet Forwarder, and LoRa Network Server performance results in LoRa sensors not being able to join the network.
4. Products Impacted
 - Gateways using the AS923 LoRa channel plan which mandates Listen Before Talk (LBT). Currently, these gateways use FPGA code v33.
 - Gateways shipping with (or upgraded to) mPower 5.2.1 software.
 - See [part numbers impacted](#) for details
5. Listen-Before-Talk FPGA Bug
 - An issue has been identified with the v.33 firmware used in the MultiTech mCard™ gateway accessory card.
 - After several hours of operations, the gateway stops blocking transmissions when an interfering signal is present.
6. Listen-Before-Talk Packet Forwarder Bug
 - After several days of operation, the gateway is not able to transmit packets and end-devices do not receive the LoRaWAN acknowledgement (ACK) from the network server.
 - When the end-devices do not receive the LoRaWAN ACK messages from the network server, the end-devices start to send new join requests.
 - These repeated join requests impact the LoRa Network Server performance (see below) due to the rejected join requests.
 - Packet Forwarder version: 4.0.1-r32.0
7. LoRa Network Server Performance
 - The Join Nonce Table saves nonce values from every join request from known end-devices.
 - When end-devices cannot join because of the above packet forwarder bug, the database grows in size due to the ongoing join requests.
 - LoRa Network Server version: 2.3.12

Overview of Bug Fix:

1. mPower 5.3.3 includes the fix to this critical issue and allows LoRa sensors to join the LoRa network as intended.
 - LoRa Packet Forwarder is upgraded to version 4.0.1-r35.0
 - LoRa Network Server is upgraded to version 2.4.22-r0.0
 - In mPower 5.3.3, the Join Nonce Table records join requests as a counter, and only the last nonce value is saved
 - This limits the size of the database, because the table is limited to one row per end-device
2. FPGA code in the Conduit gateways and MTAC-LORA-H cards will have been upgraded to FPGA v35

Critical Bug Fix (mPower 5.3.3) – mts-io - kernel Oops on no-radio devices [5103807]

Model Numbers Impacted by Bug Fix:

- Conduit AP Access Point – Ethernet only models
- Conduit IoT Programmable Gateway – Ethernet only models
- Conduit IP67 Base Station – Ethernet only models

Overview of Bug:

- This issue manifests itself as a Linux kernel Oops and is a direct result of a bug in the mts-io kernel module.
- The exact place in the kernel that the Oops backtrace would point to varies due to the fact that this issue results from writing beyond the end of an array in the code of the mts-io kernel module."
- See [part numbers impacted](#) for details

Overview of Bug Fix: mPower 5.3.3 has been updated to overcome this critical bug.

Deprecation (mPower 5.3.3) – Native support for Node.js and Node-RED

1. mPower 5.3.3 does not include native support for Node.js or Node-RED applications
 - Current mPower versions (mPower 5.2.X and earlier) include native support for Node.JS version 0.10.48-r1.7 and Node-RED version 0.15.3.
 - The requirement to upgrade to OpenSSL 1.1 in mPower 5.3.3 means that the Conduit family of programmable gateways can no longer support Node.js and Node-RED applications natively due to security protocol vulnerabilities that exist within Node.js and Node-RED.
 - Node.js and Node-RED are supported by a custom application available through DeviceHQ® or the Web User Interface. See [new features](#) for details.
 - For details on other methods to create custom applications, see [creating a custom application](#).
 - Devices impacted: Limited to Atmel-based devices. See [part numbers impacted](#).

New Features (mPower 5.3.3):

1. Upgrade to OpenSSL 1.1 [GP-39]
 - mPower version 5.2.X supports OpenSSL 1.0.2k
 - Customer applications written to earlier OpenSSL versions do not require porting to the latest version.
2. Upgrade Cipher Suite to TLS 1.3 [GP-382]
 - mPower version 5.2.1 supports configurable TLS 1.0, 1.1, and 1.2.
 - The benefits of TLS 1.3 are:
 - Increased speed of encrypted connections
 - Improved security due to the removal of obsolete and insecure features from TLS 1.2
 - Greater browser support
 - Increased SSL server support

3. Node-RED Custom Application

- A separate custom application has been developed. The user can install it using DeviceHQ or the Web Interface. **node-red-app-v23.tar.gz**
- The Node-RED custom application includes 8 packages that are installed within the application, so the installation process will take up to 10 minutes and a reboot will be required when all packages are installed.

Package Name	Version
node-red-stub	1.0-r0.0
node-red-stunnel	0.1-r3.0
node-red	0.15.3-r64.0
nodejs-npm	0.10.48-r2.7.0
nodejs	0.10.48-r2.7.0
python-compiler	2.7.15-r1.0
python-misc	2.7.15-r1.0
python-multiprocessing	2.7.15-r1.0

- The system supports deleting any package manually, but this will cause failure of the Node-RED application.
- As soon as the custom application is installed and Node-RED starts, the user can launch Node-RED and work with Node-RED applications.
- To use Node-RED as a custom application, see [Installing Node-RED as a Custom App.](#)
- The Node-RED application is statically linked with OpenSSL 1.0
- All other applications will only be able to use OpenSSL 1.1

4. Updated Reset Behavior [GP-775]

- Save and Restore Configuration page changes
 - Factory Default and User-Defined default panes have been added. These options are not dependent on each other.
 - Now it is possible to reset the configuration to factory defaults when the user-defined default configuration is set.
 - Factory Default: Reset to factory default configuration.
 - User-Defined Default: Three options available:
 1. Reset to User-Defined Configuration
 2. Set current Configuration as User-Defined Default
 3. Clear user-Defined Default
 - Reset Button Configuration: Four options available
 1. Enable Reset to Factory Default. When the RESET button is held for 5 seconds or more, the unit will be reset to the factory default settings.
 2. Enable Reset to User-Defined Default. When the RESET button on the device is held for 5 seconds or more, the unit will be reset to the user-defined default settings.
 3. If both Factory Default and User-Defined Default are enabled:
 - If the button is pressed for between zero and 5 seconds the device will perform a soft reset.
 - If the button is pressed for 5 to 30 seconds, the device will perform a User-Defined Default reset.
 - If the reset button is pressed for greater than 30 seconds a Factory Default reset will be performed.

4. If no option is selected. The RESET button will always restart the system and will not allow you to restore the unit to factory or user-defined default.
 - Once the RESET Button Configuration is changed, the user must first submit the changes, followed by a confirmation message.
 - Once the user confirms the RESET Button Configuration, the changes are applied immediately. The device does not need to be rebooted for this change to be applied.
5. Reset to Factory Default changes
 - The Web server self-signed certificate and SSH certificates are generated every time during factory reset
 - The following items are removed and/or regenerated during the factory reset:
 - Web Server CA Certificate is deleted and new certificate is generated (new behavior)
 - SSH certificates are removed and new certificates are generated (new behavior)
 - User Defined Defaults configuration is deleted (if set)
 - Root CA certificates are deleted
 - Custom applications are deleted
 - Custom image, favicon and logo are deleted
 - Custom Applications are REMOVED when the user resets the system to USER-DEFINED DEFAULT or restores the configuration from file.
 - Reset Button Configuration
 - Reset Button Configuration is a new feature. New settings that allow to enable and disable reset to factory and user-defined configuration are implemented.
 - RESET Button Configuration pane is added to the Save and Restore Configuration page. By default, the option “Enable Reset to Factory Default” is enabled, and “Enable Reset to User-Defined Default” is disabled. This configuration corresponds to the default settings in the Release 5.3.0 and older versions.
 - The changes are available in **/api/resetButton**:

```
{
  "code" : 200,
  "result" : {
    "resetToFactoryDefault" : true,
    "resetToUserDefinedDefault" : false
  },
  "status" : "success"
}
```
6. Added support for LoRa Basics Station from Semtech [GP-98, GP-687], a LoRa packet forwarder which can be remotely managed by a configuration and update server (CUPS).
<https://github.com/lorabasics/basicstation>

Features Include:

- Ready for LoRaWAN Classes A, B, and C
- Unified Radio Abstraction Layer supporting Concentrator Reference Designs v1.5 and v2
- Powerful Backend Protocols
 - Centralized update and configuration management
 - Centralized channel-plan management
 - Centralized time synchronization and transfer
 - Various authentication schemes (client certificate, auth tokens)
 - Remote interactive shell

- Lean Design
 - No external software dependencies (except mbedTLS and libloragw/-v2)
 - Portable C code, no C++, dependent only on GNU libc
 - Easily portable to Linux-based gateways and embedded systems
 - No dependency on local time keeping
 - No need for incoming connections
- 7. Firmware supports updates using differential updates (delta file) [GP-445]
 - Firmware releases following mPower 5.3.3 can be made using a differential update image.
 - When new mPower firmware versions are released, customers can update their devices using the full firmware image (today's solution) or using a differential update image.
 - The differential update image only contains updates to the firmware code that has changed.
 - The differential update image can be uploaded to the device faster than the full firmware image, reducing bandwidth and using less cellular data.
- 8. Support for updated AS923 frequency plans [GP-714]
 - AS923-1: AS923_FREQ_OFFSET_HZ = 0.0 MHz (formerly known as AS923)
 - AS923-2: AS923_FREQ_OFFSET_HZ = -1.80 MHz
 - AS923-3: AS923_FREQ_OFFSET_HZ = -6.60 MHz
- 9. Package management and updates added to administrative settings [GP-57] [CP-19]
 - Using DeviceHQ and mPower version 5.3 or later, customers can perform a package-based upgrade
 - Useful for delivering any security patches without rolling out a new firmware image

Feature Enhancements (mPower 5.3.3):

mPower 5.3.3 versions include the following enhancements to features announced in earlier mPower versions:

1. Cellular radio firmware upgrades added for the following cellular radios [GP-615, GP-397].
 - MTCDDT-L4N1, MTCDDTIP-L4N1 (Telit LE910C4-NF)
 - MTCDDT-L4E1, MTCDDTIP-L4E1 (Telit LE910C4-EU)There are two types of radio firmware upgrades:
 - Full Firmware Image Upgrade: When applied, the full firmware update replaces the current firmware image with the new image of the new version.
 - Differential (delta) Firmware Upgrade: When applied, the current firmware image is updated with the differences between it and the new version, and effectively becomes the new version of firmware.
2. Update lighttpd to latest version [GP-552]
 - mPower 5.3 updated to lighttpd version 1.4.51
 - Previous versions of mPower support lighttpd version 1.4.48
3. Cellular radio status updated to include additional details [GP-310]. Updates reported in the Web UI.
 - RSRP – LTE Signal Strength. Average power received from a single reference signal.
 - RSRQ – LTE Signal Quality. Signal-to-noise ratio for a given signal.
 - RSSI – Relative Received Signal Strength. Power level received by the cellular radio after the antenna and possible cable loss.
 - Service Domain – CS domain (video/voice service) and PS domain (data service) available.

4. Includes the following LoRa Network Server behavior:
 - The Join Nonce Table saves nonce values from every join request from known end-devices.
 - When end-devices cannot join, the database grows in size due to the ongoing join requests.
 - LoRa Network Server is upgraded to version 2.3.12
5. Includes the following LoRa Network Server improvement:
 - The Join Nonce Table records join requests as a counter, and only the last nonce value is saved
 - This limits the size of the database, because the table is limited to one row per end-device
 - LoRa Network Server is upgraded to version 2.4.22-r0.0

Known Behaviors (mPower 5.3.3)

1. Change in OpenSSL certificate validation and TLS 1.3 behavior [GP-843]
 - In mPower 5.3.3 the version of OpenSSL has been upgraded to 1.1.1b. This version includes support for TLS 1.3. TLS 1.3 is more restrictive with regards to certain behaviors in certificate authentication. One significant change in OpenSSL 1.1.1b is that TLS 1.3 will not accept certificates where the current time/date is not in the certificate lifetime (i.e. either the date on the verifying system is before the lifetime starts or after the certificate lifetime has expired)
 - The strict enforcement of certificate lifetime in TLS 1.3 has led to the following notable behaviors in the current mPower implementation:
 - (a) On firmware upgrade to mPower 5.3 from a previous version, TLS 1.3 will be disabled by default. This was done because it was found that upgrades could be performed while the device was utilizing an expired certificate. When this would happen with TLS 1.3 enabled, the user may not be able to successfully connect to the device via the Web UI if their system negotiated to use TLS 1.3 with the mPower device.
 - (b) On factory reset, TLS 1.3 will be disabled for the same reasons as above. A second reason for factory reset to disable TLS 1.3 is that if a customer has uploaded a signed certificate of their own, there is potential that the customer's certificate may not get deleted. If it is expired and TLS 1.3 is the default negotiated SSL protocol, the customer may also find themselves locked out.
2. Change in start-stop-daemon behavior [GP-813]
 - The mPower upgrade from Yocto 2.2 (Morty) to Yocto 2.6 (Thud) identified that the start-stop-daemon will not allow execution of files that do not have their execute permissions explicitly set.
 - The start-stop-daemon can be used in custom applications on mPower to start a customer program as a daemon without the customer having to implement all the "daemonization" code in their program.
 - In previous versions of start-stop-daemon it was possible for a file to be executed even though it did not have executable permissions (i.e. `-rw-r--r-- 1 root root myProgram.py`)
 - In the current version of start-stop-daemon the program file to be executed is required to have execute permissions (i.e. `-rwxr--r-- 1 root root myProgram.py`)

3. OpenVPN - Encryption Cipher Configuration Issue [GP-846]
 - In the OpenVPN configuration of tunnels on the mPower 5.3.3, there is a change to the way that OpenVPN 2.6 effectively handles the encryption cipher parameter. The argument “--cipher” has been deprecated and the “Encryption Cipher” option in the mPower Web UI has been removed.
 - Instead of “--cipher” in OpenVPN 2.6 and “Encryption Cipher” in the Web UI the new parameter “--ncp-ciphers” that is named Negotiable Crypto Parameter (NCP) has essentially replaced “Encryption Cipher”.
4. Start-stop-daemon behavior change that may affect custom applications [IN-4100]
 - With the Thud upgrade the start-stop-daemon is more concerned with executable permissions.
 - Custom applications must have 755 versus 644 permissions regarding executions.

API Command Changes (mPower 5.3.3):

The Conduit devices use the RESTful JSON API for managing configurations, polling statistics, and issuing commands. mPower MTCAP 5.3.3 and mPower MTCDT 5.3.3 versions include a number of API changes.

- API Reference: <http://www.multitech.net/developer/software/mtr-api-reference/>
- Changes from mPower 5.2.1 to mPower 5.3.3:
<http://www.multitech.net/developer/software/mtr-software/mtr-api-reference/api-changes/>

IV. Schedule

There are multiple versions of mPower Edge Intelligence firmware available for customer evaluation and final release.

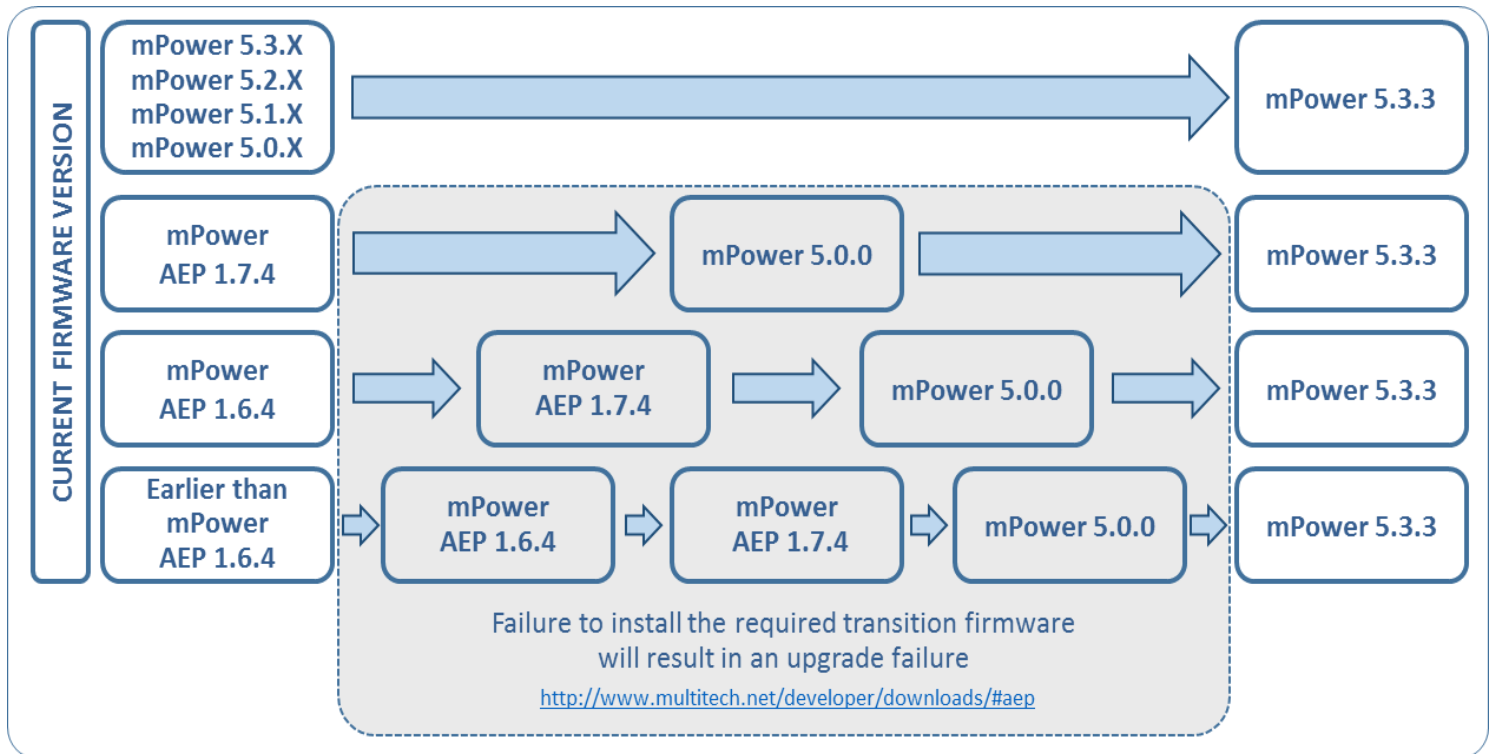
- Manufacturing (New Hardware)
 - MTCAP 5.3.3 Availability: March 2021
 - See [part numbers impacted](#) for details
- Manufacturing (Active Hardware)
 - MTCAP 5.3.3 Availability: April 2021
 - MTCDT 5.3.3 Availability: April 2021
 - See [part numbers impacted](#) for details
 - Devices shipping from MultiTech starting May 2021 will include mPower 5.3.3
- DeviceHQ
 - Cloud-based IoT Device Management
 - MTCAP 5.3.3 Availability: March 2021
 - MTCDT 5.3.3 Availability: March 2021
 - DeviceHQ login: https://www.devicehq.com/sign_in
 - Instructions: [Upgrading Firmware Using DeviceHQ](#)
- Downloadable Versions
 - MTCAP 5.3.3 Availability: March 2021
 - MTCDT 5.3.3 Availability: March 2021
 - MTCAP 5.3.0 Availability: October 2020
 - MTCDT 5.3.0 Availability: October 2020
 - Conduit models: visit <http://www.multitech.net/developer/downloads/>
 - Instructions: [Upgrading Firmware Using Device Web Interface](#)

V. Upgrade Process

At any time in the upgrade process, customers can send an email to support@multitech.com or call +1(763) 717-5863.

Minimum System Requirements (mPower 5.3.3)

To install mPower 5.3.3, the Conduit gateway must be upgraded to mPower 5.0.0 or higher. Customers that are running earlier versions of mPower should use the following upgrade process:



V. Upgrade Process (continued)

Upgrade Using MultiTech DeviceHQ

DeviceHQ can update the firmware running on any supported device. Since devices have no live connection to DeviceHQ, firmware updates are made the next time a device checks into DeviceHQ.

Instructions:

1. Visit <https://www.devicehq.com>
2. Sign in to your account using your **email address** and **password**.
3. Click **Devices**. The device list page opens.
4. Click the name of the device you want to update. You can update firmware on filtered devices or selected devices.
 - If you select individual devices, you update firmware on selected devices or the filtered devices.
 - If you do not select devices you update the firmware on the filtered devices.
5. Click **Schedule** and select **Upgrade Firmware**. From the list of firmware that appears, select the name of the firmware file. A confirmation message appears, informing you that the new firmware is to be applied to the device when the device next checks in.
6. To confirm that you want to update the firmware click **OK**.

NOTE: To schedule multiple devices at once, see help file within DeviceHQ

Upgrade Using Device Web Interface

It is recommended that customers backup their configuration before performing an upgrade.

- If the firmware upgrade fails, or it does not show the login page again, wait an additional 10 minutes.
- Power off and on the hardware and log in using the web interface to check the version.
- If the version does not show the latest, then the upgrade was not successful.
- Try to perform the firmware upgrade again by repeating all the steps.

Instructions:

1. Download the latest firmware file from <http://www.multitech.net/developer/downloads/#aep>

NOTE: There are multiple versions of mPower firmware available.
Please select the file that matches the hardware model being upgraded.

2. Log into the mPower Web interface.
3. In the left navigation pane, click **Administration > Firmware Upgrade**.
4. Click Browse and select the appropriate file.
5. Click **Start Upgrade**.
6. After the firmware upgrade is complete, log back into the web GUI and verify the firmware version shown at the top of the page.

VI. Ordering Part Numbers Impacted

The following ordering part numbers are impacted by these updates:

Model Name Ordering Part Numbers	Ordering Part Numbers	Ordering Part Numbers
Conduit® IoT Programmable Gateways		
Status: Active ⁽²⁾	Status: Active ⁽²⁾	Status: NEOL ⁽³⁾
MTCDT-246A-US-EU-GB ⁽²⁾ MTCDT-247A-US-EU-GB ⁽²⁾	MTCDT-L4E1-246A-EU-GB ⁽²⁾ MTCDT-L4E1-247A-EU-GB ⁽²⁾ MTCDT-L4N1-246A-US ⁽²⁾ MTCDT-L4N1-247A ⁽²⁾ MTCDT-L4N1-247A-US ⁽²⁾ MTCDT-LAP3-246A-AU ⁽²⁾ MTCDT-LDC3-246A-JP ⁽²⁾ MTCDT-LDC3-247A-JP ⁽²⁾ MTCDT-LSB3-246A-JP ⁽²⁾	MTCDT-H5-246A-US-EU-GB ⁽³⁾ MTCDT-H5-247A-US-EU-GB ⁽³⁾
Conduit® IoT Programmable Gateways with LoRa Accessory Cards		
Status: Active ⁽²⁾	Status: Active ⁽²⁾	Status: NEOL ⁽³⁾
MTCDT-246A-868-EU-GB ⁽²⁾ MTCDT-246A-915-US-EU-GB ⁽²⁾ MTCDT-246A-923-JP ⁽²⁾ MTCDT-246A-US-EU-GB-923KR ⁽²⁾ MTCDT-247A-868-EU-GB ⁽²⁾ MTCDT-247A-915-US-EU-GB ⁽²⁾	MTCDT-L4E1-246A-868-EU-GB ⁽²⁾ MTCDT-L4E1-246A-915-EU-GB ⁽²⁾ MTCDT-L4E1-247A-868-EU-GB ⁽²⁾ MTCDT-L4E1-247A-915-EU-GB ⁽²⁾ MTCDT-L4N1-246A-915-US ⁽²⁾ MTCDT-L4N1-247A-915-US ⁽²⁾ MTCDT-LAP3-246A-915-AU ⁽²⁾ MTCDT-LAP3-247A-915-AU ⁽²⁾ MTCDT-LDC3-246A-923-JP ⁽²⁾ MTCDT-LSB3-246A-923-JP ⁽²⁾	MTCDT-H5-246A-868-EU-GB ⁽³⁾ MTCDT-H5-247A-868-EU-GB ⁽³⁾ MTCDT-H5-247A-915-US ⁽³⁾
Conduit® IP67 Base Stations		
Status: Active ⁽²⁾	Status: Active ⁽²⁾	Status: Active ⁽²⁾
MTCDTIP-266A-868 ⁽²⁾ MTCDTIP-266A-868/2 ⁽²⁾ MTCDTIP-266A-915 ⁽²⁾ MTCDTIP-266A-915/2 ⁽²⁾ MTCDTIP-266A-923-JP ⁽²⁾ MTCDTIP-266A-923KR ⁽²⁾ MTCDTIP-267A-868 ⁽²⁾ MTCDTIP-267A-868/2 ⁽²⁾ MTCDTIP-267A-915 ⁽²⁾ MTCDTIP-267A-915/2 ⁽²⁾	MTCDTIP-L4E1-266A-868 ⁽²⁾ MTCDTIP-L4E1-266A-868/2 ⁽²⁾ MTCDTIP-L4E1-266A-915 ⁽²⁾ MTCDTIP-L4E1-267A-868 ⁽²⁾ MTCDTIP-L4N1-266A-915 ⁽²⁾ MTCDTIP-L4N1-266A-915/2 ⁽²⁾ MTCDTIP-L4N1-267A-915 ⁽²⁾ MTCDTIP-L4N1-267A-915/2 ⁽²⁾	MTCDTIP-LAP3-266A-915 ⁽²⁾ MTCDTIP-LAP3-266A-915/2 ⁽²⁾ MTCDTIP-LAP3-267A-915 ⁽²⁾ MTCDTIP-LDC3-266A-923-JP ⁽²⁾ MTCDTIP-LSB3-266A-923-JP ⁽²⁾

VI. Ordering Part Numbers Impacted (continued)

The following ordering part numbers are impacted by these updates:

Model Name Ordering Part Numbers	Ordering Part Numbers	Ordering Part Numbers
Conduit® IP67 Geolocation Base Stations		
Status: Active ⁽²⁾		
MTCDTIP-L4E1-270A-868 ⁽²⁾		
Conduit® IP67 200 Series Base Stations		
Status: New Hardware ⁽¹⁾	Status: New Hardware ⁽¹⁾	
MTCDTIP2-EN-B11EKP-D1M ⁽¹⁾	MTCDTIP2-L4E1-B11EKP-D1M ⁽¹⁾	
MTCDTIP2-EN-B11EKP-L1M ⁽¹⁾	MTCDTIP2-L4E1-B11EKP-L1M ⁽¹⁾	
MTCDTIP2-EN-B11UKP-L1M ⁽¹⁾	MTCDTIP2-LNA3-B11UKP-L1M ⁽¹⁾	
Conduit® AP Access Points		
Status: New Hardware ⁽¹⁾	Status: Active ⁽²⁾	Status: Active ⁽²⁾
MTCAP2-868-002A-POE ⁽¹⁾	MTCAP-868-001A ⁽²⁾	MTCAP-L4E1-868-001A ⁽²⁾
MTCAP2-868-042A-POE ⁽¹⁾	MTCAP-868-041A ⁽²⁾	MTCAP-L4E1-868-041A ⁽²⁾
MTCAP2-915-042A-POE ⁽¹⁾	MTCAP-915-001A ⁽²⁾	MTCAP-LAP3-915-001A ⁽²⁾
MTCAP2-L4E1-868-002A-POE ⁽¹⁾	MTCAP-915-041A ⁽²⁾	MTCAP-LAP3-915-041A ⁽²⁾
MTCAP2-L4E1-868-042A-POE ⁽¹⁾	MTCAP-IN865-001A ⁽²⁾	MTCAP-LNA3-915-001A ⁽²⁾
MTCAP2-LNA3-915-042A-POE ⁽¹⁾		MTCAP-LNA3-915-041A ⁽²⁾

Footnotes:

	Hardware Status	Manufacturing Updates	Comments
(1)	New	March 2021	<ul style="list-style-type: none"> New device that is shipping for the first time Some customers may be testing devices with an earlier version of mPower firmware or a beta version of mPower firmware MultiTech recommends that customers update this hardware to mPower 5.3.3 firmware
(2)	Active	April 2021	<ul style="list-style-type: none"> Active devices continue to ship with earlier mPower versions Customers are encouraged to evaluate mPower 5.3.3 firmware prior to this transition
(3)	NEOL	n/a	<ul style="list-style-type: none"> NEOL devices continue to ship with earlier mPower versions Devices can be individually updated by customers

VII. mPower™ Edge Intelligence

mPower™ Edge Intelligence is MultiTech's embedded software offering, building on the popular application enablement platform, to deliver programmability, network flexibility, enhanced security and manageability for scalable Industrial Internet of Things (IIoT) solutions.

mPower Edge Intelligence simplifies integration with a variety of popular upstream IoT platforms to streamline edge-to-cloud data management and analytics, while also providing the programmability and processing capability to execute critical tasks at the edge of the network to reduce latency, control network and cloud services costs, and ensure core functionality – even in instances when network connectivity may not be available.

In response to evolving customer security requirements, mPower Edge Intelligence incorporates a host of security features including signed firmware validation, enhanced firewall and VPN settings, secure authentication and more.

VIII. Additional Information

If you have any questions regarding this Product Change Notification/Software Release Notice, please contact your MultiTech sales representative or visit the technical resources listed below:

World Headquarters – USA

+1 (763) 785-3500 | sales@multitech.com

EMEA Headquarters – UK

+(44) 118 959 7774 | sales@multitech.co.uk

MultiTech Developer Resources:

www.multitech.net

An open environment where you can ask development related questions and hear back from MultiTech engineering or a member of this community.

Knowledge Base:

<http://www.multitech.com/kb.go>

Immediate access to support information and resolutions for all MultiTech products.

MultiTech Support Portal:

<https://support.multitech.com/support/login.html>

Create an account and submit a support case directly to our technical support team.

MultiTech Website:

www.multitech.com