

## Product Change Notification Software Release Notice

### MultiTech® Conduit®

#### Family of Programmable Gateways:

- Conduit IoT Programmable Gateway
- Conduit IP67 Base Station
- Conduit AP Access Point



## mPower™ Edge Intelligence Now Available - mPower 5.3.X Firmware Deprecated Features - Node.js and Node-RED

---

Date: October 29, 2020

**Product Change Notification (PCN) Number**  
PCN 10292020-001 (mPower)

### I. Overview

MultiTech announces the schedule for the next version of mPower firmware for the MultiTech® Conduit® family of products, including:

- MultiTech Conduit® IoT Programmable Gateway
- MultiTech Conduit® IP67 Base Station
- MultiTech Conduit® AP Access Point

#### DEPRECATED FEATURES

**mPower 5.3.X will NOT support Node.js applications**  
**mPower 5.3.X will NOT support Node-RED applications**

### Contents

I. <a href="#">Overview</a>	V. <a href="#">Upgrading Firmware</a>
II. <a href="#">Suggested Action Plan</a>	<a href="#">DeviceHQ</a>
III. <a href="#">mPower 5.3 Overview</a>	<a href="#">Web Interface</a>
<a href="#">Deprecation – Node.js and Node-RED</a>	VI. <a href="#">Ordering Part Numbers Impacted</a>
<a href="#">New Features</a>	VII. <a href="#">mPower™ Edge Intelligence</a>
IV. <a href="#">Schedule</a>	VIII. <a href="#">Conduit Family Overview</a>
	IX. <a href="#">Additional Information</a>

## II. Suggested Action Plan

To help accelerate the acceptance of mPower 5.3.X and understand any impact on custom applications, we recommend that the following actions be taken.

### Upcoming mPower Versions

- MTCAP 5.3.X (Conduit AP Access Point)
- MTCDT 5.3.X (Conduit Gateway and Conduit IP67 Base Station)

### Customers

- Please review the information in this PCN and forward to others within your organization who are actively involved with the development of IoT applications using the Conduit AP Access Point, Conduit IoT Programmable Gateway, or Conduit IP67 Base Station.
- If your application is using a hosted LoRaWAN® Network Server, contact your provider and understand how mPower 5.3.X may impact your deployment.

### Deprecated Features

- mPower 5.3.X will **not** support Node.js applications.
- mPower 5.3.X will **not** support Node-RED applications.
- Recommendation: Transition Node.js and Node-RED applications to Python programming language.

### Released Firmware Schedule

- Review the [Ordering Part Numbers Impacted](#) to understand how mPower 5.3.X impacts the devices you are using
- If your application is using a hosted LoRaWAN Network Server, contact your provider and understand how mPower 5.3.X may impact your deployment
- Consider downloading mPower 5.3.X firmware prior to the transition
- Technical inquiries: email [support@multitech.com](mailto:support@multitech.com)
- Sales inquiries: email [sales@multitech.com](mailto: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.X Overview

#### Deprecation (MTCAP 5.3.X, MTCDT 5.3.X) – Node.js and Node-RED Support

1. mPower 5.3.X does not include support for Node.js or Node-RED applications
  - Current mPower versions (mPower 5.2.X and earlier) support 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.X means that the Conduit family of programmable gateways can no longer support Node.js and Node-RED applications due to security protocol vulnerabilities that exist within Node.js and Node-RED.
2. Node-RED BACKGROUND:
  - Node-RED is a flow-based development tool for visual programming developed originally by IBM for wiring together hardware devices, APIs and online services as part of the Internet of Things.
  - Node-RED provides a web browser-based flow editor, which can be used to create JavaScript functions. Elements of applications can be saved or shared for re-use.
  - The runtime is built on Node.js. The flows created in Node-RED are stored using JSON.
3. CUSTOMER ACTION PLAN:

Customers that have developed custom applications using Node.js or Node-RED applications for use on Conduit gateways should consider the following options:

  - Transition application to Python programming language.
  - Additional resources are available:  
<http://www.multitech.net/developer/software/aep/creating-a-custom-application/>
  - Node.js and Node-RED will be supported in a new MultiTech gateway: The Conduit 300 IoT Programmable Gateway. The Conduit 300 is currently available as a [developer kit](#) and is expected to be released for general availability in 2021.

#### New Features (MTCAP 5.3.X, MTCDT 5.3.X):

mPower 5.3.X will include the following new features:

1. Upgrade to Yocto 2.6.4 (codename: Thud) [GP-444]
  - mPower versions 5.2.1 and earlier are built using Yocto 2.2.4 (codename: Morty).
2. Upgrade to OpenSSL 1.1 [GP-39]
  - mPower version 5.2.1 supports OpenSSL 1.0.2k
  - Customer applications written to earlier OpenSSL versions do not require porting to the latest version
3. 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

4. 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
5. mPower 5.3 firmware supports updates using differential updates [GP-445]
    - Firmware releases following mPower 5.3.X 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.
  6. 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
  7. Package management and updates added to administrative settings [GP-57] [CP-19]
    - Using Device HQ 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
  8. Support for 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/>

### Feature Enhancements (MTCAP 5.3.X, MTCDT 5.3.X):

mPower 5.3.X 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].
  - MTCDT-L4N1, MTCDTIP-L4N1 (Telit LE910C4-NF)
  - MTCDT-L4E1, MTCDTIP-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
  - 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 Web UI and Device HQ.
    - 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

### Known Behaviors (MTCAP 5.3.X, MTCDT 5.3.X)

1. Change in OpenSSL certificate validation and TLS 1.3 behavior [GP-843]
  - In mPower 5.3.X 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.X, 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 (MTCAP 5.3.X, MTCDDT 5.3.X):**

The Conduit devices use the RESTful JSON API for managing configurations, polling statistics, and issuing commands. mPower MTCAP 5.3.X and mPower MTCDDT 5.3.X versions include a number of API changes.

API Reference: <http://www.multitech.net/developer/software/mtr-api-reference/>

Changes from mPower 5.2.X to mPower 5.3.X:

<http://www.multitech.net/developer/software/mtr-software/mtr-api-reference/api-changes/>

#### **Minimum System Requirements (MTCAP 5.3.X, MTCDDT 5.3.X)**

To install mPower 5.3.X, 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:

- mPower AEP 1.7.4
  1. Upgrade to mPower 5.0.X
  2. Install mPower 5.3.X
- mPower AEP 1.6.4
  1. Upgrade to mPower AEP 1.7.4
  2. Upgrade to mPower 5.0.1
  3. Install mPower 5.3.X
- mPower versions earlier than mPower AEP 1.6.4
  1. Upgrade to mPower AEP 1.6.4
  2. Upgrade to mPower AEP 1.7.4
  3. Upgrade to mPower 5.0.1
  4. Install mPower 5.3.X

#### IV. Schedule

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

- Downloadable Versions
  - MTCAP 5.3.X Availability: October 2020
  - MTCDT 5.3.X Availability: October 2020
  - Conduit models: visit <http://www.multitech.net/developer/downloads/>
  - Instructions: [Upgrading Firmware Using Device Web Interface](#)
- Manufacturing
  - MTCAP 5.3.X Availability: April 2021
  - MTCDT 5.3.X Availability: April 2021
  - See [Ordering Numbers Impacted](#) for details on when MTCAP 5.3.X and MTCDT 5.3.X will be available for different devices
- DeviceHQ®
  - Cloud-based IoT Device Management
  - MTCAP 5.3.X Availability: October 2020
  - MTCDT 5.3.X Availability: October 2020
  - DeviceHQ login: [https://www.devicehq.com/sign\\_in](https://www.devicehq.com/sign_in)
  - Instructions: [Upgrading Firmware Using DeviceHQ](#)

## V. Upgrading Firmware

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

### Upgrading Using 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

### Upgrading Using the 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 the <http://www.multitech.net/developer/downloads/>

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:
  - MTCAP\_5.3\_upgrade-signed.bin
  - conduit\_5.3\_upgrade-signed.bin
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		
<b>Conduit® IoT Programmable Gateways</b>		
<b>Status: Active</b> <sup>(2)</sup>	<b>Status: Active</b> <sup>(2)</sup>	<b>Status: NEOL</b> <sup>(3)</sup>
MTCDDT-246A-US-EU-GB <sup>(2)</sup> MTCDDT-L4E1-246A-EU-GB <sup>(2)</sup> MTCDDT-L4N1-246A-US <sup>(2)</sup> MTCDDT-LAP3-246A-AU <sup>(2)</sup> MTCDDT-LDC3-246A-JP <sup>(2)</sup> MTCDDT-LSB3-246A-JP <sup>(2)</sup>	MTCDDT-247A-US-EU-GB <sup>(2)</sup> MTCDDT-L4E1-247A-EU-GB <sup>(2)</sup> MTCDDT-L4N1-247A <sup>(2)</sup> MTCDDT-L4N1-247A-US <sup>(2)</sup> MTCDDT-LDC3-247A-JP <sup>(2)</sup>	MTCDDT-H5-246A-US-EU-GB <sup>(3)</sup> MTCDDT-H5-247A-US-EU-GB <sup>(3)</sup>
<b>Conduit® IoT Programmable Gateways with LoRa Accessory Cards</b>		
<b>Status: Active</b> <sup>(2)</sup>	<b>Status: Active</b> <sup>(2)</sup>	<b>Status: NEOL</b> <sup>(3)</sup>
MTCDDT-246A-868-EU-GB <sup>(2)</sup> MTCDDT-246A-915-US-EU-GB <sup>(2)</sup> MTCDDT-246A-923-JP <sup>(2)</sup> MTCDDT-L4E1-246A-868-EU-GB <sup>(2)</sup> MTCDDT-L4E1-246A-915-EU-GB <sup>(2)</sup> MTCDDT-L4N1-246A-915-US <sup>(2)</sup> MTCDDT-LAP3-246A-915-AU <sup>(2)</sup> MTCDDT-LDC3-246A-923-JP <sup>(2)</sup> MTCDDT-LSB3-246A-923-JP <sup>(2)</sup>	MTCDDT-247A-868-EU-GB <sup>(2)</sup> MTCDDT-247A-915-US-EU-GB <sup>(2)</sup> MTCDDT-L4E1-247A-868-EU-GB <sup>(2)</sup> MTCDDT-L4E1-247A-915-EU-GB <sup>(2)</sup> MTCDDT-L4N1-247A-915-US <sup>(2)</sup> MTCDDT-LAP3-247A-915-AU <sup>(2)</sup> MTCDDT-LDC3-247A-JP <sup>(2)</sup>	MTCDDT-H5-246A-868-EU-GB <sup>(3)</sup> MTCDDT-H5-247A-868-EU-GB <sup>(3)</sup> MTCDDT-H5-247A-915-US <sup>(3)</sup>
<b>Conduit® IP67 Base Stations</b>		
<b>Status: Active</b> <sup>(2)</sup>	<b>Status: Active</b> <sup>(2)</sup>	<b>Status: NEOL</b> <sup>(3)</sup>
MTCDDTIP-266A-868 <sup>(2)</sup> MTCDDTIP-266A-868/2 <sup>(2)</sup> MTCDDTIP-266A-915 <sup>(2)</sup> MTCDDTIP-266A-915/2 <sup>(2)</sup> MTCDDTIP-266A-923-JP <sup>(2)</sup> MTCDDTIP-266A-923KR <sup>(2)</sup> MTCDDTIP-L4E1-266A-868 <sup>(2)</sup> MTCDDTIP-L4E1-266A-868/2 <sup>(2)</sup> MTCDDTIP-L4E1-266A-915 <sup>(2)</sup> MTCDDTIP-L4N1-266A-915 <sup>(2)</sup> MTCDDTIP-L4N1-266A-915/2 <sup>(2)</sup> MTCDDTIP-LAP3-266A-915 <sup>(2)</sup> MTCDDTIP-LAP3-266A-915/2 <sup>(2)</sup> MTCDDTIP-LDC3-266A-923-JP <sup>(2)</sup> MTCDDTIP-LSB3-266A-923-JP <sup>(2)</sup>	MTCDDTIP-267A-868 <sup>(2)</sup> MTCDDTIP-267A-868/2 <sup>(2)</sup> MTCDDTIP-267A-915 <sup>(2)</sup> MTCDDTIP-267A-915/2 <sup>(2)</sup> MTCDDTIP-L4E1-267A-868 <sup>(2)</sup> MTCDDTIP-L4N1-267A-915 <sup>(2)</sup> MTCDDTIP-L4N1-267A-915/2 <sup>(2)</sup> MTCDDTIP-LAP3-267A-915 <sup>(2)</sup>	none

## VI. Ordering Part Numbers Impacted (continued)

The following ordering part numbers are impacted by these updates:

Model Name Ordering Part Numbers		
<b>Conduit® IP67 Geolocation Base Stations</b>		
<b>Status: Active <sup>(2)</sup></b>	<b>Status: Active <sup>(2)</sup></b>	<b>Status: NEOL <sup>(3)</sup></b>
MTCDTIP-L4E1-270A-868 <sup>(2)</sup>	MTCDTIP-L4N1-270A-915 <sup>(2)</sup> MTCDTIP-L4N1-275A-915 <sup>(2)</sup>	none
<b>Conduit® AP Access Points</b>		
<b>Status: Active <sup>(2)</sup></b>	<b>Status: Active <sup>(2)</sup></b>	<b>Status: NEOL <sup>(3)</sup></b>
MTCAP-868-001A <sup>(2)</sup> MTCAP-915-001A <sup>(2)</sup> MTCAP-IN865-001A <sup>(2)</sup> MTCAP-L4E1-868-001A <sup>(2)</sup> MTCAP-LAP3-915-001A <sup>(2)</sup> MTCAP-LNA3-915-001A <sup>(2)</sup>	MTCAP-868-041A <sup>(2)</sup> MTCAP-915-041A <sup>(2)</sup> MTCAP-L4E1-868-041A <sup>(2)</sup> MTCAP-LAP3-915-041A <sup>(2)</sup> MTCAP-LNA3-915-041A <sup>(2)</sup>	none

### Footnotes:

	Hardware Status	Manufacturing Updates	Comments
(1)	<b>New</b>	October 2020	<ul style="list-style-type: none"> <li>New device that is shipping for the first time</li> <li>Some customers may be testing devices with an earlier version of mPower firmware or a beta version of mPower firmware</li> <li>MultiTech recommends that customers update this hardware to mPower 5.3.X firmware</li> </ul>
(2)	<b>Active</b>	April 2021	<ul style="list-style-type: none"> <li>Active devices continue to ship with earlier mPower versions</li> <li>Customers are encouraged to evaluate mPower 5.3.X firmware prior to this transition</li> </ul>
(3)	<b>NEOL</b>	n/a	<ul style="list-style-type: none"> <li>NEOL devices continue to ship with earlier mPower versions</li> <li>Devices can be individually updated by customers</li> </ul>

## 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. Conduit® IoT Gateways

Conduit® family of products is the industry's most configurable, manageable, and scalable cellular communications gateways for industrial IoT applications. Network engineers can remotely configure and optimize their Conduit performance through DeviceHQ®, the world's first IoT Application Store and Device Management platform. The award-winning Conduit series comes in three variants designed to address specific IoT gateway use cases:

- **Conduit**: Indoor industrial gateway, ideal for environments that require metal casing for protection against particles and debris and require an industrial temperature range.
- **Conduit IP67 Base Station**: Outdoor IP67-rated gateway ideal suited for performing in harsh environments such as rain, snow, extreme heat, and high winds.
- **Conduit AP**: Indoor access point ideal for commercial environments (e.g., hotels, offices, retail facilities) to deepen LoRa coverage in difficult to reach places where cell tower or rooftop deployments may not perform as well.

#### **IX. 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](mailto:sales@multitech.com)

##### **EMEA Headquarters – UK**

+(44) 118 959 7774 | [sales@multitech.co.uk](mailto:sales@multitech.co.uk)

##### **MultiTech Developer Resources:**

[www.multitech.net](http://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](http://www.multitech.com)