Product Change Notification
Software Release Notice

MultiConnect® Conduit® Family of Programmable Gateways: Conduit IoT Programmable Gateway, Conduit IP67 Base Station, and Conduit AP Access Point

mPower™ Edge Intelligence -- New Firmware Available

Date: June 26, 2019

Product Change Notification Number
PCN 062619-AEP-01

I. Overview

MultiTech announces new firmware for the MultiConnect® Conduit® family of products, including:

- MultiConnect® Conduit®
- MultiConnect® Conduit® IP67 Base Station
- MultiConnect® Conduit® AP Access Point

The purpose of this Product Change Notification is to

1. Alert customers that updated code is available for evaluation
2. Provide customers important information on this new code, including the schedule for the final firmware release

New Application Enablement Platform (AEP) Versions:

- MTCDT AEP 5.x (Conduit and Conduit IP67 Base Station)
- MTCAP AEP 5.x (Conduit AP Access Point)

New mLinux Platform Version:

- mLinux 5.x (Conduit, Conduit IP67 Base Station, Conduit AP Access Point)

Contents:

II. Release Schedule

The latest versions of mPower Edge Intelligence software is in the final stages of development and is available as beta code for customer evaluations and soon will be generally available as Final Release shortly. Here is the schedule for these releases and the source for the latest firmware code.

Final Release

- Firmware that has been fully tested and qualified by MultiTech.
- Download Version
  - Availability: July 2, 2019
  - AEP: http://www.multitech.net/developer/downloads/#aep
  - mLinux: http://www.multitech.net/developer/downloads/#mLinux
- Manufacturing
  - Availability: mid-July 2019
  - All shipments from MultiTech will include new AEP or mLinux firmware
- DeviceHQ
  - Cloud-based IoT Device Management
  - AEP models only
  - Availability: July 2, 2019
  - https://www.devicehq.com/sign_in

III. mPower™ Edge Intelligence

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

mPower represents the unification and evolution of well-established MultiTech smart router and gateway firmware platforms. In addition to ongoing support of the current feature-sets, MultiConnect Conduit gateway customers can now enjoy the additional security and usability features currently available on the MultiConnect rCell 100 Series router.

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 new security features including signed firmware validation, enhanced firewall and VPN settings, secure authentication and more.

IV. Models Impacted

The following Conduit models are impacted by these firmware updates:

- MultiConnect® Conduit® IoT Programmable Gateways
- MultiConnect® Conduit® IoT Programmable Gateways with LoRa Accessory Cards
- MultiConnect® Conduit® IP67 Base Stations
- MultiConnect® Conduit® IP67 Geolocation Base Station
- MultiConnect® Conduit® AP (Access Point)

For a specific list of the ordering part numbers impacted, reference Ordering Part Numbers Impacted

V. Terms and Definitions

Term	Definition
Device	Conduit IoT Programmable Gateways MultiConnect® Conduit® IoT Programmable Gateways with LoRa Accessory Cards Conduit IP67 Base Stations Conduit IP67 Geolocation Base Station Conduit AP (Access Point)
Continued Support	Previous firmware version **has** this feature and there are no changes to the functionality in the new firmware release
Added Support	Previous firmware version **does not** have this feature and this feature is included in the new firmware release
Updated Support	Previous firmware version **has** this feature and this feature has been updated in the new firmware release
Not Supported	Previous firmware version **has** this feature and support has been removed in the new firmware release

VI. AEP 5.x Overview

The AEP 5.X firmware release represents a major release for MultiTech. It not only consolidates the firmware used by several other MultiTech hardware devices into one firmware version, it also delivers several new features to the Conduit AEP firmware and enhances several of the features already available, including:

- Software Support
  - Updated User Interface (UI), including customizable Web UI
  - Updated Linux kernel (4.9) from previous kernel (3.12)
  - Updated LoRa capabilities
- Hardware Support
  - Added support for new cellular radios
  - Updated radio API references
- Security
  - Added security features and enhancements to existing security features, including:
    - Access to over 500 resolved Common Vulnerabilities and Exposures (CVE) in Linux kernel 4.9
    - Password authentication to access the device bootloader
    - Access to the device's internal system can be accessed securely via SSH

    - Signed firmware validation when upgrading AEP firmware
    - Defined firewall rules to determine how incoming and outgoing packets are handled
    - Web UI Ciphers and Hash algorithms verified
    - Customer has the ability to enable Silent Mode which turns off the output to the Debug Console
    - Bi-directional certificate authentication is available in the web UI
- Secure Access
    - Added support for multiple users
    - Added support for signed firmware updates
- Secure Connectivity
    - Added GRE tunnels and IPsec tunnels
- Remote Authentication
    - Continued support for RADIUS
    - Added support and management for multiple X.509 certificates
- Notifications
    - Added support for sending time-stamped notifications via email, SMS, and SNMP trap
- Debugging
    - Updated utilities to help customers troubleshoot and solve technical issues.
    - Updated Global DNS with three configuration options
- Serial Port Protocols
    - Updated support for configuring the RS-232 serial connection using TCP, UDP, or SSL/TLS server protocol
- Remote Management
    - Updated cloud-based tools to manage, monitor, upgrade a population of devices
- Bug Fixes
    - A number of bugs were identified in previous firmware versions have been corrected

Firmware Versions (MTCDT AEP 5.x, MTCAP AEP 5.x)

Model Name	Current AEP Firmware Version	NEW AEP Firmware Version
Conduit IoT Programmable Gateway **Conduit IP67 Base Station**	MTCDT AEP 1.7.4	MTCDT AEP 5.x
Conduit IP67 Geolocation Base Station	MTCDT AEP 1.7.3	MTCDT AEP 5.x
Conduit AP Access Point	MTCAP AEP 1.7.3	MTCAP AEP 5.x

Minimum System Requirements (MTCDT AEP 5.x, MTCAP AEP 5.x)

To install AEP 5.x, the Conduit gateway must have the proper firmware version:

- AEP 1.4.3 or higher
- If running a firmware version lower than AEP 1.4.3, please install AEP 1.4.3 before loading the appropriate version of AEP 5.x

Feature Enhancements (AEP 5.x):

An overview of the features and feature enhancements for firmware version AEP 5.x is listed below. For more information on the products and firmware features, visit http://www.multitech.net/developer/downloads/#aep

1. Software Support
   a. User Interface (UI)
      i. Updated look and feel
      ii. Updated UI that can be customized by the customer to include the customer name, look-and-feel, logo, and supporting information (address, phone numbers, website)

   b. Operating System
      i. Continued support for Yocto v2.2
      ii. Linux kernel support upgraded from v3.12.70 to v4.9
         - Common Vulnerabilities and Exposures (CVE) resolved: 529 identified Linux vulnerabilities have been resolved, including some "higher profile" CVE:

CVE Addressed	Nickname/Kernel Area
CVE-2016-5195	Dirty Cow
CVE-2017-18017	netfilter:xt_TCPMSS
CVE-2016-10229	udp.c
CVE-2014-2523	netfilter/nf_conntrack_proto_dccp.c
CVE-2016-7117	net/socket.c
CVE-2015-8787	net/netfilter/nf_nat_redirect.c

         - For a list of all CVE resolved, visit Common CVE Resolved
         - For more information on CVE vulnerabilities, visit https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures
      iii. Continued support for custom applications and Node-RED
         - Enable/Disable Node-RED
         - Custom applications can be started, stopped, or deleted from/on device
      iv. Package upgrade support for Java, Ruby, Python, C/C++, and Javascript

   c. LoRa Features Supported

LoRa Features	**Firmware Version**	
	MTCDT AEP 5.x	**MTCAP AEP 5.x**
	Conduit Conduit IP67	Access Point
Continued support for LoRa Network Server v 2.2.18	X	
Continued support for LoRa Packet Forwarder v4.0.1	X	X
Continued support for two MTAC-LORA-H cards	X	

      i. Continued support for LoRaWAN 1.0.1 and LoRaWAN 1.0.2
      ii. Updated support for LoRaWAN 1.0.3rA, including
         - Changes to AU915 Channel Plan (dwelltime settings, CFList with Join Accept)
         - Changes to US915 Channel Plan (CFList with Join Accept)

iii. Continued support for LoRaWAN Class A end-devices
Class A end-devices are ideal for minimal power applications where the majority of data is transmitted to the network server with only occasional downlinks. Each uplink transmission is followed by two short downlink receive windows in which only one packet can be received. The second receive window is only opened when a packet is not received within the first window. Downlink communications from the server must wait for the next received uplink.

iv. Updated support for LoRaWAN Class B end-devices (beacons)
Class B end-devices operate according to Class A and additionally open extra receive windows at scheduled times
- Send beacon from gateway at 128s intervals if GPS is available
- Scheduled downlink will be queued for next available ping slot. Ping slots are adjustable by the end-device to be one per interval up to one second
- Beacon frequency and power can be configured as well as the info descriptor of the transmitted beacon

v. Updated support for LoRaWAN Class C end-devices (multicast)
Class C end-devices have an always-open receive window except when transmitting.
- Now schedule downlinks for all connected gateways

2. Hardware Support
   a. Cellular Radio Support

Cellular WAN Support	**Wireless Carrier**	**Firmware Version**	
		MTCDT AEP 5.x	**MTCAP AEP 5.x**
		Conduit Conduit IP67	Access Point
Radio support **added** for the following cellular technologies			
4G-LTE Category 4 Europe (-L4E1 models)	European Carriers	X	X
4G-LTE Category 4 North America (-L4N1 models)	AT&T Verizon	X	X
Radio support **continued** for the following cellular technologies:			
3G-HSPA+ Global (-H5 models)	AT&T Global	X	
4G-LTE Category 1 North America (-LAT3 models)	AT&T	X	
4G-LTE Category 1 North America (-LVW3 models)	Verizon	X	
4G-LTE Category 1 North America (-LSP3 models)	Sprint		X
4G-LTE Category 1 Australia (-LAP3 models)	Telstra	X	
4G-LTE Category 1 Japan (-LDC3 models)	NTT Docomo	X	
4G-LTE Category 1 Japan (-LSB3 models)	Softbank	X	
4G-LTE Category 3 Europe (-LEU1 models)	European Carriers	X	X
4G-LTE Category 1 North America (-LNA3 models)	AT&T Verizon		X
4G-LTE Category 3 North America (-LAT1 models)	AT&T	X	
4G-LTE Category 3 North America (-LVW2 models)	Verizon	X	

b. API References
   i. Devices use a RESTful JSON API for managing configurations, polling statistics, and issuing commands.
   ii. Additional information on the MultiConnect Conduit AEP API, including API information that has changed or is remaining the same, can be found at: http://www.multitech.net/developer/software/aep/conduit-aep-api/

c. Cellular Radio Configuration
Devices with a cellular radio continue to have several configuration options available, including connection timeout and retry, dial-on-demand, dial number settings, authentication, keep alive, wake-up on call, and radio status.

d. Wireless Support (MTCDT AEP 5.x only)
Devices with a Wi-Fi/BT radio continue to have several configuration options available.
   i. The device can be configured as a Wi-Fi access point (up to eight clients) or Wi-Fi as WAN station and connect to local Wi-Fi networks
   ii. Bluetooth data can be sent over the Internet to a target server or client and the device can scan for available Bluetooth devices and save Bluetooth devices for connection as a later time.
   iii. Bluetooth Low Energy (BLE) power settings can be configured and the device can scan for local BLE devices.

e. LoRa Channel Plan Support
Continued support for the following LoRa channel plans:

LoRa Channel Plan Support	**Firmware Version**	
	MTCDT AEP 5.x	**MTCAP AEP 5.x**
	Conduit Conduit IP67	Access Point
AS923 (Asia Pacific) with Listen Before Talk	X	X
AS923 (Japan)	X	X
AU915 (Australia)	X	X
EU868 (Europe)	X	X
IN865 (India)	X	X
KR920 (Korea)	X	X
RU864 (864 – 870 MHz) Russia)	X	X
US915 (North America)	X	X

f. GNSS/GPS Support (MTCDT AEP 5.x only)
Some devices are supplied with a GNSS/GPS receiver and antenna for location and timestamping information. Continued support for these features.

g. MultiConnect mCard Accessory Card Support (MTCDT AEP 5.x only)
The MultiConnect mCard Accessory Cards are for use in the Conduit IoT Programmable Gateway.
- Added support for two MTAC-LORA-H-XXX mCards (of the same channel plan) to be installed and configured as packet forwarder with use with:

- Built-in LoRa Network Server
  or
- 3rd party LoRa Network Server

- Continued support for the following MultiConnect mCards:

MultiConnect mCard Accessory Card Support	Firmware Version	
	MTCDT AEP 5.x	MTCAP AEP 5.x
	Conduit Conduit IP67	Access Point
MTAC-LORA-H-868	X	
MTAC-LORA-H-915	X	
MTAC-LORA-H-923-JP	X	
MTAC-GPIO	X	
MTAC-XDOT	X	
MTAC-PULSE (proprietary)	X	

3. Security

New security features added in this release:

- Access to over 500 resolved Common Vulnerabilities and Exposures (CVE) in Linux upgrade to 4.9 kernel from 3.12 kernel
- Password authentication to access the device bootloader
- Access to the device's internal system can be accessed securely via SSH
- Signed firmware validation when upgrading AEP firmware
- Defined firewall rules to determine how incoming and outgoing packets are handled
- Web UI Ciphers and Hash algorithms verified
- Customer has the ability to enable Silent Mode which turns off the output to the Debug Console
- Bi-directional certificate authentication is available in the web UI
- Bootloader password support has been added to the web UI

a. VPN

- Support for up to 5 concurrent tunnels
- IPSec IKE and IKEv2
- Open VPN, three configurations available
  Configuration 1 (Custom). Tunnel with TLS Authorization Mode (Device only)
  Configuration 2 (Server). Tunnel with TLS Authorization Mode (Device and Connected PC)
  Configuration 3 (Client). Tunnel with Static Key Authorization Mode (device server and client)
- Cipher suite: DHGroup 14
- Configurable encryption, configurable hash, configurable TLS: 1.0, 1.1, 1.2
- Encapsulation: ESP
- Encryption Methods: 3DES, AES-128, AES-192, AES-256
- Authentication: MD5, SHA-1, SHA-2, SHA2-256, SHA2-384, SHA2-512
- Key Group: DH2 (1024-bit), DH5 (1536-bit), DH14 (2048-bit), DH15 (3072-bit), DH16 (4096-bit), DH17 (6144-bit), DH18 (8192-bit), DH22 (1024-bit), DH23 (2048-bit), DH24 (2048-bit)

b. MAC Filtering
   - Accept, reject, drop or log packets based on MAC address

c. Firewall Rules
   - SPI Firewall
   - Configurable DNAT, NAT-T, SNAT

d. DHCP
   - IPv4 Mask settings allow the connected device to obtain LAN settings automatically or the LAN settings can be configured manually.

e. X.509 Certificates
   - Support generation and/or import of multiple CA certificates through use of SHA-256.
   - User can add and delete user's root certificates in addition to the certificates from the /etc/ssl by application.

f. PAP/CHAP
   - Authentication protocols for secure PPP connections

g. SMS Security Features
   - SMS configuration allows users to specify passwords and whitelisted numbers that are required when receiving SMS commands from remote users

4. Secure Access
   a. Password Strength Controls
      i. Must be eight characters in length
      ii. Contains three or more different types of characters such as: uppercase alphabetic, lowercase alphabetic, numeric, and non-alphanumeric (@ # $!)

   b. UI session inactivity timeout
      i. A user's session will be automatically logged out if it remains dormant for an identified number of minutes

   c. Administration controls (Save and Restore Configuration)
      i. Continued support
      ii. Customer can restore the configuration of the device from a file on their PC, save the configuration to a file on their PC, or save user-defined-defaults on the device that can be restored at a later time back to the current configuration

   d. User Accounts
      The system offers three roles or user types: administrator, engineer, and monitor. The system automatically checks for a strong password and tells you how to improve it.
      i. Administrators have full rights and permissions including change settings on the device.
      ii. Engineers have read/write privileges and some access to controls on the device.
      iii. Monitors have read-only access.

e. Firewall Rule settings enforce a set of rules that determine how incoming and outgoing packets are handled. Additional settings can be made to add:
   i. Inbound and outbound forwarding rules
   ii. Input filter rules
   iii. Output filter rules
   iv. Advanced settings are available to allow users to manipulate DNAT, SNAT, and filter rules directly and set prerouting rules and postrouting rules.
   v. Trusted IP is a separate firewall configuration that allows users to create whitelists (which are allowed or trusted IPs) or black lists (which are blocked or unwanted IPs).
      - Trusted IP options are:
        - Name
        - IP Address Range or Subnet
        - Destination Port (default port is ANY)
        - By default the port shall be ANY. The System will allow a range of ports (10000:20000) to be added, the list of ports using comma (443, 82), or list of ranges and ports (10000:20000, 443, 88).
        - Protocol (ANY, TCP/UDP, TCP, UDP)
      - A warning message displayed if a user enables the Trusted IP White List and leaves the IP Range empty:
        "There are no IP addresses in the Trusted IP list. All incoming traffic will be dropped."
      - A warning message displayed if a user enables the Trusted IP Black List and leaves the IP Range empty:
        "*There are no IP addresses in the Trusted IP list. All incoming traffic will be allowed."*
   vi. Static Routes allow the customer to add static network routes that will be created when the device boots. The customer can manually configure a route to an IP address through a next-hop routing device. This is useful for when the device being reached is not reachable through a WAN interface, but can be reached through a device on the LAN.

f. Access Configuration determines how the device can be accessed and configures the security features that decrease susceptibility to malicious activity
   i. HTTP Redirect to HTTPS. A set of rules that automatically redirect HTTP requests to the device's secure HTTPS port.
   ii. HTTPS. A secure Web UI access to modify its configurations and execute actions
   iii. HTTPS Security. Configurable security settings when SSL/TLS Protocol is selected.
   iv. SSH. For advanced troubleshooting and/or custom deployment options.
   v. SSH Security. Configurable security settings when SSL/TLS Protocol is selected.
   vi. Internet Control Message Protocol (ICMP). Configurable method of responding to ICMP (ping) requests received via LAN and/or WAN.
   vii. Standard Network Management Protocol (SNMP). Used to collect information from, and configure network devices on the IP network.
   viii. Modbus Slave. Enables Modbus query server so Modbus-TCP can query status information.

g. Signed Firmware Upgrade
   i. Added support for signed firmware validation when upgrading AEP firmware
   ii. The customer can choose to enable or disable signed firmware upgrade.
   iii. If signed firmware upgrade is enabled, each component of the firmware image is required to be signed and the signature must reside in a file corresponding to the image file.

h. Save and Restore Configuration
   i. Customer allowed to restore the configuration of the device from a file on their PC, save the configuration to a file on their PC, or save user-defined-defaults on the device that can be restored at a later time to revert back to the current configuration.
   ii. The user-defined-defaults can be cleared or set at any time.

5. Secure Connectivity
   a. OpenVPN (Server and Client)
      i. Upgraded to version 2.4.6
      ii. Open VPN is one of the most popular and well-received implementations of VPN technology. It is open source based and uses a customized protocol to achieve secure connectivity using SSL/TLS (Secure Socket Layer) in the process for security. Many VPN providers offer OpenVPN as a preferred protocol for security and reliability reasons.
         - Strong Security With security features such as peer authentication using pre-shared keys, certificates and other usual forms of authentication, strong encryption standards using the OpenSSL Library, and HMAC packet authentication, OpenVPN are ideal for customers who want to keep their networks safe and secure from prying eyes and hackers. Also, OpenVPN runs in the user space without root privileges, making it safe and robust.
         - High Reliability When OpenVPN goes down, the network is brought to a pause to allow for repair or reconfiguration, thereby ensuring that no data loss or corruption or miscommunication happens. This also acts as an additional layer of security.
            - VPN: IPSec, IKEv1,v2
            - Cipher suite:
            - DHGroup 14
            - Configurable Encryption: AES256, DES, 3DES
            - Configurable Hash: SHA-1, 2, MD5, RSA
            - Configurable TLS: 1.0, 1.1, 1.2
            - Encapsulation: ESP
      iii. Three configuration modes:
         - Custom. OpenVPN Tunnel with TLS Authorization Mode (Device only)
         - Server. OpenVPN Tunnel with TLS Authorization Mode (Device and Connected PC)
         - Client. OpenVPN Tunnel with TLS Authorization Mode (Device only)

   b. Generic Routing Encapsulation (GRE) Tunnels
      i. GRE tunnel support added
      ii. Allows the use of a public network to convey data on behalf of two remote private networks. It is also a way to transform data frames to allow them to pass networks with incompatible address spaces or even incompatible protocols.

   c. Network-to-Network VPNs
      i. Site-to-Site VPNs via Internet Protocol Security (IPsec) tunnels added
      ii. IPSec is a secure network protocol suite that authenticates and encrypts the packets of data sent over an internet protocol network and is used in Virtual Private Networks (VPN)
      iii. The Basic IPSec tunnel configuration and authentication now requires digital certificate-based authentication in addition to pre-shared keys (PSK) for enhanced security.

iv. Encryption Methods supported: 3DES, AES-128, AES-192, AES-256, and Advanced, which allows encryption, authentication, and Key Group components to be specified. Advanced encryption also allows configuration of the IKE Lifetime, key line, max retries, and checking period to timeout the runnel if checks don't meet requirements.
v. Default Hash Algorithms: SHA-1, SHA-2, and MD5
vi. Default DH Group Algorithms: DH2 (1024-bit), DH5 (1536-bit), DH14 (2048-bit), DH15 (3072-bit), DH16 (4096-bit), DH17 (6144-bit), DH18 (8192-bit), DH22 (1024-bit), DH23 (2048-bit), and DH24 (2048-bit)
vii. The System will issue a warning if the configured tunnel uses encryption or a hash algorithm that is known to be weak:
- Encryption: 3DES, ANY
- Authentication: MD5, SHA-1, ANY

d. Added support for X.509 Certificates
i. A certificate management capability has been implemented which allows adding user's root (CA) certificates.
ii. Users can manage root certificates that can be used by different applications on the device, including RADIUS, with the new certificate manager feature.
iii. The certificates available in the /etc/ssl can be used by the applications.
iv. The user can add and delete user's root certificates in addition to the certificates from the /etc/ssl by application.
v. All CA certificates that are uploaded, deleted or expired are logged.

e. Ciphersuite
SSL/TSL communication was upgraded to use TLS 1.2 and requires ciphers offering no less than 128 bits equivalent strength - without incorporating outdated and vulnerable technologies such as compression, RC4 or MD5.

6. Remote Authentication Dial-In User Service (RADIUS) Support
a. Continued support for RADIUS

b. RADIUS protocol supports authentication, user session accounting, and authorization of users to the device. This authentication, accounting, and authorization is independent of the local users created on the device.

c. The user can enable Authentication, Accounting, or both options.

7. Notifications
The device has the option of sending time-stamped notifications to individuals or groups of individuals based on events, system statistics, or self-diagnostic monitoring.
a. Customers can configure the notifications they receive for different events and status information
b. Notifications can be sent/received in up to three ways: Email, SMS, and SNMP trap
c. SMS behavior can also be set to
i. Resend failed SMS
ii. Send SMS to keep
iii. Received SMS to keep

d. SNMP traps
   i. SNMP are unique when compared to other message types, since they are the only method that can be directly initiated by a SNMP agent
   ii. Other types of messages are either initiated by the SNMP manager or sent as a result of the manager's request.
   iii. This ability makes SNMP traps indispensable in most networks. It is the most convenient way for an SNMP agent to notify the manager that something is wrong, that an event has occurred, or that a malicious activity is suspected.
   iv. Device can support five SNMP configurations and enable up to three SNMP configurations at one time
   v. Device can support five SNMP trap destinations and enable up to three SNMP trap destinations at one time

e. Customers must configure an SMTP server for Email notifications

f. Recipient groups can be created for Email and SMS message distribution

g. Sent messages and message status can be managed in three ways:
   i. Mail Log: A list of recent Email delivery attempts and the Email log details
   ii. Mail Queue: Emails that are waiting to be sent from the router or gateway
   iii. Notifications Sent: A listing of the notifications sent, over what method (Email, SMS, or SNMP) and to what individual or Recipient Group

Event	**Description**	**Notification Mechanism**
High Data Usage	High Data Usage against Data Plan	Email, SMS, SNMP
Low Signal Strength	Low Cellular Signal Strength	Email, SMS, SNMP
Device Reboots	Notify of Device Reboot	Email, SMS, SNMP
Ethernet Interface Failure	The Ethernet interface has lost connectivity	Email, SMS, SNMP
Wi-Fi Interface Failure	The Wi-Fi interface has lost connectivity	Email, SMS, SNMP
Cellular Interface Failure	The Cellular interface has lost connectivity to the Internet	Email, SMS, SNMP
Ethernet Data Traffic	Traffic stats for Ethernet Interface(s)	Email, SMS
Wi-Fi Data Traffic	Traffic stats for Wi-Fi Interface(s)	Email, SMS
Cellular Data Traffic	Traffic stats for Cellular Interface	Email, SMS
WAN Interface Failover	Failover to alternative WAN has happened	Email, SMS, SNMP
Ping Failure	Ping has failed over the configured interface	Email, SMS, SNMP
Security Violation	Detects security rule violations (*)	Email, SMS, SNMP
Flash Memory Violation	Flash memory checksum check to protect the integrity of the device firmware (*)	Email, SMS, SNMP
Resource Overuse	Detects memory leaks or errors (*)	Email, SMS, SNMP

(*) Self-diagnostic monitoring is intended to improve performance, detect corruption, or help prevent malicious activity. After an event is detected, the system disables the cellular radio module, sends an alarm or notification, logs the event, and sends a record of it to the SNMP server.

8. Debugging
   The device has a number of utilities to help customers troubleshoot and solve technical issues.
   a. Cellular AT Commands. Communicate directly with the device's cellular radio (if available) using AT commands
      i. Additional information on the MultiConnect Conduit AEP API, including API information that has changed or is remaining the same, can be found at: http://www.multitech.net/developer/software/aep/conduit-aep-api/

   b. Automatic Reboot Timer. Specify the amount of time that passes before the device automatically reboots itself. Customers can schedule a reboot at the same time every day or at the end of a configured time interval.

   c. Setting up Telnet. When Telnet Radio Access is enabled, devices with an integrated cellular radio can be communicated with directly, without using any router functions.

   d. Remote Syslog Server. A Remote Syslog server can be configured where the device will stream syslog logging data. Logging levels are configurable (minimum, error, warning, info, debug, maximum).

   e. Statistics Settings. Cellular and Ethernet statistics can be saved periodically.
      i. Status and Logs are available for the System, Ethernet, Wi-Fi WAN, Wi-Fi Access Point, Cellular, Bluetooth, IPSec, OpenVPN and LoRa statistics
      ii. Logs can be downloaded for analysis and troubleshooting

   f. Ping Options. Device can ping an IP address or URL to ensure that it is operational. Ping failure can be communicated as an email, SMS, or SNMP and configured in the Notifications settings.

   g. Reset Options. Customer can reset the cellular modem, Wi-Fi module or Bluetooth module.

   h. SNMP Support. Simple Network Management Protocol (SNMP) can be used to collect information from and configure network devices on an IP network.

   i. Dynamic Domain Naming System (DDNS). This feature allows your device to use a DDNS service to associate a hosted server's domain name with a dynamically changing internet address.

   j. Domain Name Server (DNS). The device can manage traffic for the local area network (LAN) and behave as a local DNS forwarder. Three configuration options are available:
      i. DNS forwarding server is enabled. Global DNS is not configured
      ii. Primary/Secondary DNS servers are customer configurable. DNS forwarding is disabled
      iii. Primary/Secondary DNS servers are added. DNS forwarding is enabled
      NOTE: If DNS forwarding is not enabled, the device will not forward any DNS requests from the LAN devices. DNS for local services and applications on the device is based on whatever the current WAN and how DNS settings were obtained for that interface.

k. Dynamic Host Configuration Protocol (DHCP). The device can be configured to function as a DHCP server and supply network configuration information, such as IP address, subnet mask, and broadcast address, to devices on the network

l. SMS Configuration. SMS commands can be used to send a number of commands to the device and aid in troubleshooting. It is also possible to send and receive SMS messages from the device in order to test the SMS functionality.

m. Usage Policy. The device has a usage policy for the system. A default usage policy is provided, or the customer can customize the policy to meet their needs.

The default Usage Policy text is:
This system is for the use of authorized users only. Individuals using this system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

9. Serial Port Protocols
The serial terminal connected to the device RS-232 connection can be configured using TCP, UDP, or SSL/TLS server protocol:
   a. Device can be configured to act as a client

   b. Device can be configured to act as a server

   c. Device can be configured to use Modbus protocol to communicate with serial devices
      i. The Modbus Query Server provides the device with the capability to return a set of values over Modbus TCP to a client connecting from the Ethernet LAN. The values to be reported include the device model type, PPP WAN IP address, and various cellular related parameters such as signal strength, MCC, MNC and cellular band. The combination of MCC and MNC codes are parameters that could be used to uniquely identify a mobile network operator (carrier).
      ii. Details on Modbus queries using a Modbus application can be found at: http://www.multitech.net/developer/software/mtr-software/mtr-modbus-information/

10. Remote Management
   a. Signed Firmware Authentication / Integrity Check
   The device supports a private, secure, digital signature technique to enable transferring the device firmware safely. The technique defeats attempts to load invalid firmware files or files that have been subjected to damage or tampering. MultiTech signs and distributes the firmware through a secure, standard firmware distribution process, and verifies the firmware signature before it installs the firmware files to ensure integrity.

   IMPORTANT
   The Signed Firmware validation feature is enabled by default, and can be disabled if required. The System will always verify the signature of the firmware before the firmware upgrade starts if Signed Firmware validation is enabled.

The firmware upgrade **WILL FAIL** and display an error message if a user tries to upgrade with unsigned firmware. The firmware upgrade **WILL NOT FAIL** if a user upgrades with unsigned firmware (releases 4.0 and older) and if Signed Firmware validation is disabled.

b. Simple Network Management Protocol (SNMP) Support

The device offers Simple Network Management Protocol (SNMP) which is used for collecting information from, and configuring network devices on an IP network.

i. SNMPv1/v2c, and SNMPv3 support

ii. Configure SNMPv1/v2c Server Configuration using:
- Allowed IP addresses
- Configuration Name
- Configuration String

iii. Configure SNMPv3 Server Configuration using:
- Authentication Protocol: MD5 or SHA1
  - Security Name (user name)
  - Authentication Password (authenticates incoming SNMPv3 requests)
- Encryption Protocol: DES or AES-128
  - Encryption Password

iv. Multiple SNMP trap servers and SNMP server configurations configured through an enhanced web user interface

v. Extended SNMP Read Parameters
- The SNMP read parameters have been extended with additional configuration settings.
- The following parameters were added to reflect the updated SNMP capabilities:

Router System	SMS	Firewall
DNS, DDNS	SMTP, SNTP	Static Routes
DHCP	SNTP	Tunnels
Syslog	Diagnostics	RADIUS

c. Remote Management

i. Continued support for DeviceHQ

ii. The device is able to connect to DeviceHQ, a remote device management platform that provides device status and information in a clear graphical format. Manage, monitor, group, configure and upgrade devices remotely.

iii. DeviceHQ reduces the cost and complexity of IoT deployments by:
- Simplifying the deployment of gateways with zero-touch provisioning
- Reducing truck rolls when devices are managed by a single web-based application
- Updating firmware and custom applications remotely

iv. Additional information: https://www.multitech.com/brands/devicehq

v. DeviceHQ log-in: https://www.devicehq.com/sign_in

d. Customizable Web User Interface
   i. Added support for customizable web UI
   ii. Customer limited ability to customize the device to their company's name, look-and-feel, and supporting information

11. Bug Fixes

These are the bug fixes that have been implemented since the MTCDT AEP 1.7.4 and MTCAP AEP 1.7.3 releases:

Bug Fixes (AEP 5.x)	**Firmware Version**	
	MTCDT AEP 5.x	**MTCAP AEP 5.x**
	Conduit Conduit IP67	Access Point
In MTCAP AEP 1.7.3, it was identified that when the Ethernet cable was unplugged and plugged back in, the IP address would revert to the factory default setting (192.168.2.1) instead of the customer-defined IP address. This issue was corrected in maintenance release MTCAP AEP 1.7.4		X

Upgrading AEP Firmware:

Instructions on upgrading AEP firmware can be found on the MultiTech Developer Website: http://www.multitech.net/developer/software/aep/upgrading-the-aep-firmware/

1. Download the latest firmware file from the Downloads page.

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

2. Log into the AEP Web interface.
3. In the left navigation pane, click **Administration > Firmware Upgrade**.
4. Click Browse and select the **conduit_AEP-X_upgrade.bin** 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.
7. If you want to save any Node-RED applications, you have two options:
   - If you have a DeviceHQ account, upload Node-Red apps to DeviceHQ. (Recommended)
   - If you do not have a DeviceHQ account, save Node-RED apps you want to keep. Node-RED flows are stored on the Conduit at **/var/config/app/current/flows.json**. You can export flows to the clipboard from the Node-RED menu or use a tool like WinSCP or SCP in Cygwin to copy **flows.json** to your PC.

Customers can also send an email to support@multitech.com if they have questions or require additional information.

VII. mLinux 5.x Overview

The mLinux 5.x firmware release represents a major release for MultiTech. It not only consolidates the firmware used by several other MultiTech hardware devices into one firmware version, it also delivers several new features to the Conduit AEP firmware and enhances several of the features already available, including:

- Software Support
  - Updated Linux version (Linux 4.9)
    - Access to over 500 resolved Common Vulnerabilities and Exposures (CVE)
  - Updated LoRa capabilities
  - Updated software protocols
- Hardware Support
  - Added support for new cellular radios
  - Updated radio API references
  - Added support for new LoRa channel plans
- Bug Fixes
  - Bugs that were identified in previous firmware versions have been corrected
- Notable Feature Behaviors
  - Features considered, but not implemented

Model Name	Current mLinux Firmware Version	NEW mLinux Firmware Version
Conduit IoT Programmable Gateway **Conduit IP67 Base Station**	mLinux 4.1.9	mLinux 5.x
Conduit IP67 Geolocation Base Station	mLinux 4.1.7	mLinux 5.x
Conduit AP Access Point	mLinux 4.1.7	mLinux 5.x

Minimum System Requirements (mLinux 5.x):

To install mLinux 5.x, the Conduit gateway must have the proper firmware version:

- mLinux 3.3.9 or higher

Feature Enhancements (mLinux 5.x):

An overview of the feature enhancements for firmware version mLinux 5.x is listed below

1. Software Support
   i. Operating System
      - Continued support for Yocto v2.2
      - Linux kernel support upgraded from v3.12.70 to v4.9
        - Common Vulnerabilities and Exposures (CVE) resolved: 529 identified Linux vulnerabilities have been resolved, including some "higher profile" CVE:

CVE Addressed	Nickname/Kernel Area
CVE-2016-5195	Dirty Cow
CVE-2017-18017	netfilter:xt_TCPMSS
CVE-2016-10229	udp.c
CVE-2014-2523	netfilter/nf_conntrack_proto_dccp.c
CVE-2016-7117	net/socket.c
CVE-2015-8787	net/netfilter/nf_nat_redirect.c

        - For a list of all resolved CVE, visit Resolved CVE
        - For more information on CVE vulnerabilities, visit https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

      - Kernel Commonality: Kernel configuration for MTR, MTCDT AEP, and MTCAP AEP firmware is now the same, which simplifies software support
      - Kernel Preemption: Feature makes hardware more responsive to interrupts
      - Package upgrade support for Java, Ruby, Python, C/C++, and Javascript
      - MTS-IO Driver:
        - Continued support for existing MTS-IO driver features
        - Added support for new feature that allows driver to read the EEPROM by loading the driver. Reboot is not required after writing the EEPROM for the first time.
      - MTAC Driver:
        - Continued support for MTAC driver
        - Added support for new feature to read the EEPROM(s) of MTAC cards when the driver is loaded. Reboot is not required after writing the EEPROM for the first time.
      - BLE GATT Server Support: Added support for BLE GATT server

   ii. Software protocol updates from mLinux 4.1.9 to mLinux 5.x

Protocol	Description	Overview of changes
bluez5	Linux Bluetooth protocol stack	pand sub-package was missing the dependencies python-subprocess and python-argparse
hostap-daemon	Network interface enabler	hostapd stability update to 2.7
Linux Kernel	Open-source operating system	Updated to Linux 4.9 for better support and security, including gattserver for BLE

Protocol	Description	Overview of changes
libmts-io	Multi-threads socket library	Support for ME910C1, LE4E1 and L4N1 cellular modems
libudev1	Access to device information	Quactel modem support
mtd-utils	Memory Technology Devices	Support for Linux 4.9
mts-io, mtac	Device Driver	Reads eeprom and device tree on load of driver
rs9113-autostart	Bluetooth startup	New package to start rs9113 at boot for mLinux
rs9113 related packages at version 1.6.1	Bluetooth startup	New Redpine rs9113 driver updates to support Linux 4.9

iii. LoRa Features Supported

LoRa Features	Hardware Version	
	Conduit Conduit IP67	Access Point
Continued support for LoRa Network Server v 2.2.18	X	X
Continued support for LoRa Packet Forwarder v4.0.1	X	X
Continued support for two MTAC-LORA-H cards	X	

- Continued support for LoRaWAN 1.0.1 and LoRaWAN 1.0.2
- Updated support for LoRaWAN 1.0.3rA, including
  - Changes to AU915 Channel Plan (dwelltime settings, CFList with Join Accept)
  - Changes to US915 Channel Plan (CFList with Join Accept)
- Continued support for LoRaWAN Class A end-devices
  Class A end-devices are ideal for minimal power applications where the majority of data is transmitted to the network server with only occasional downlinks. Each uplink transmission is followed by two short downlink receive windows in which only one packet can be received. The second receive window is only opened when a packet is not received within the first window. Downlink communications from the server must wait for the next received uplink.
- Updated support for LoRaWAN Class B end-devices (beacons)
  Class B end-devices operate according to Class A and additionally open extra receive windows at scheduled times
  - Send beacon from gateway at 128s intervals if GPS is available
  - Scheduled downlink will be queued for next available ping slot. Ping slots are adjustable by the end-device to be one per interval up to one second
  - Beacon frequency and power can be configured as well as the info descriptor of the transmitted beacon
- Updated support for LoRaWAN Class C end-devices (multicast)
  Class C end-devices have an always-open receive window except when transmitting.
  - Now schedule downlinks for all connected gateways

2. Hardware Support

i. Cellular Radio Support

Cellular WAN Support	Wireless Carrier	Firmware Version	
		MTCDT AEP 5.x	MTCAP AEP 5.x
		Conduit Conduit IP67	Access Point
Radio support **added** for the following cellular technologies			
4G-LTE Category 4 Europe (-L4E1 models)	European Carriers	X	X
4G-LTE Category 4 North America (-L4N1 models)	AT&T Verizon	X	X
Radio support **continued** for the following cellular technologies:			
3G-HSPA+ Global (-H5 models)	AT&T Global	X	
4G-LTE Category 1 North America (-LAT3 models)	AT&T	X	
4G-LTE Category 1 North America (-LVW3 models)	Verizon	X	
4G-LTE Category 1 North America (-LSP3 models)	Sprint		X
4G-LTE Category 1 Australia (-LAP3 models)	Telstra	X	
4G-LTE Category 1 Japan (-LDC3 models)	NTT Docomo	X	
4G-LTE Category 1 Japan (-LSB3 models)	Softbank	X	
4G-LTE Category 3 Europe (-LEU1 models)	European Carriers	X	X
4G-LTE Category 1 North America (-LNA3 models)	AT&T Verizon		X
4G-LTE Category 3 North America (-LAT1 models)	AT&T	X	
4G-LTE Category 3 North America (-LVW2 models)	Verizon	X	

ii. Cellular Radio API References

- Devices with cellular radio support use a RESTful JSON API for managing configurations, polling statistics, and issuing commands.
- Additional information on the MultiConnect Conduit AEP API, including API information that has changed or is remaining the same, can be found at: http://www.multitech.net/developer/software/aep/conduit-aep-api/

iii. Cellular Radio Configuration

Devices with a cellular radio continue to have several configuration options available, including connection timeout and retry, dial-on-demand, dial number settings, authentication, keep alive, wake-up on call, and radio status.

iv. Wireless Support (Conduit and Conduit IP67 only)

Devices with a Wi-Fi/BT radio continue to have several configuration options available.

i. The device can be configured as a Wi-Fi access point (up to eight clients) or Wi-Fi as WAN station and connect to local Wi-Fi networks

ii. Bluetooth data can be sent over the Internet to a target server or client and the device can scan for available Bluetooth devices and save Bluetooth devices for connection as a later time.

iii. Bluetooth Low Energy (BLE) power settings can be configured and the device can scan for local BLE devices.

v. LoRa Channel Plan Support

Continued support for the following LoRa channel plans:

LoRa Channel Plan Support	**Hardware Version**	
	Conduit Conduit IP67	Access Point
AS923 (Asia Pacific) with Listen Before Talk	X	X
AS923 (Japan)	X	X
AU915 (Australia)	X	X
EU868 (Europe)	X	X
IN865 (India)	X	X
KR920 (Korea)	X	X
RU864 (864 – 870 MHz) (Russia)	X	X
US915 (North America)	X	X

vi. GNSS/GPS Support (Conduit and Conduit IP67 only)

Some devices are supplied with a GNSS/GPS receiver and antenna for location and timestamping information. Continued support for these features.

vii. MultiConnect mCard Accessory Card Support (Conduit and Conduit IP67 only)

The MultiConnect mCard Accessory Cards are for use in the Conduit IoT Programmable Gateway.

- Added support for two MTAC-LORA-H-XXX mCards (of the same channel plan) to be installed and configured as packet forwarder with use with:
  - Built-in LoRa Network Server
    or
  - 3rd party LoRa Network Server
- Continued support for the following MultiConnect mCards:

MultiConnect mCard Accessory Card Support	**Hardware Version**	
	Conduit **Conduit IP67**	**Access Point**
MTAC-LORA-H-868	X	
MTAC-LORA-H-915	X	
MTAC-LORA-H-923-JP	X	
MTAC-GPIO	X	
MTAC-XDOT	X	
MTAC-PULSE (proprietary)	X	

viii. List of package changes from earlier mLinux versions: http://www.multitech.net/mlinux/feeds/

ix. Bug Fixes

The following Linux patches were found necessary for the new Linux 4.9 release:

- Ten second watchdog timeout
- Number of accessory ports supported in the kernel
- ECC error correction timeout lengthened
- ACM driver modified to ignore the EXAR part
- LED Netdev trigger patch for MTCDT AEP and MTCAP AEP software to detect network traffic.
- Qmi-wwan patch for Sprint LSP3 firmware updates
- Removal of Atmel Version from the Linux kernel to simplify the kernel version.

x. Notable Feature Behaviors

Features considered, but not implemented

- Yocto 2.6 will not be supported. Continued support for Yocto 2.2, Morty.

Upgrading mLinux Firmware (mLinux 5.x):

There are three means of upgrading the existing mLinux firmware

1. Upgrading mLinux using an image install
2. Updating packages during a reboot
3. Creating an update package that uses opkg

1. Upgrading mLinux using an image install

The command **/usr/sbin/mlinux-firmware-upgrade** may be used to upgrade the firmware. The upgrade file should be placed in **/var/volatile** or one of its subdirectories. The command must be run as the root user.

There are two types of upgrade files. One type is created by the build named ***upgrade*.bin** and found in the deploy image directory of the build see: http://www.multitech.net/developer/software/mlinux/mlinux-building-images/building-a-custom-linux-image/

Example image upgrade files:
build/tmp/deploy/images/mtcdt/mlinux-factory-image-mtcdt-upgrade.bin
build/tmp/deploy/images/mtcap/mlinux-mtcap-image-mtcap-upgrade-withboot.bin

Files with **withboot** in the name include the bootstrap and U-Boot partitions. Unless you are upgrading from mLinux 3 to mLinux 4, it is usually not necessary to update bootstrap or U-Boot

2. **Updating packages during a reboot**
   The second type of upgrade file does not do a complete firmware update. It updates packages using the **opkg** command. A package update only affects packages that are changed. Unlike an image update, most files are maintained.

   The purpose of updating packages during a reboot is to provide greater resources (memory and temporary file space) for the upgrade. Very small upgrades to commands can be applied without rebooting using the **opkg** command and the feeds. See: http://www.multitech.net/mlinux/feeds

   If you have initscripts 2.0-r155.43 (mLinux 4.0.0 or greater), it is possible to upgrade packages using **mlinux-firmware-upgrade**.

   These files are found at http://www.multitech.net/mlinux/upgrades when available. Choose your device (mtcdt or mtcap). The version pertains to the specific firmware update or where a fix applies.

   Since these are not image updates, they may take longer to apply. They leave the configuration alone, except for the packages being updated. NOTE: Make sure that newly installed packages are correctly configured.

3. **Creating an update package that uses opkg**
   This method uses opkg and local files.

   See an update package example: http://multitech.net/mlinux/upgrades/example/

   Carefully review the initial list of packages and verify that they match the final list. Packages may be split or merged. In these cases a package may need to be removed or added, not just updated. Packages may require other packages. So dependencies also need to be in the update package tree. An easy way to determine what packages are required is to use the mLinux feeds, http://www.multitech.net/mlinux/feeds/ with **opkg**. The file **/etc/opkg/mlinux-feed.conf** may need to be configured for the desired level of mLinux in the update.

   The update package is a tar file containing **IPK files** and a **shell script** to initiate the update.

Customers can also send an email to support@multitech.com if they have questions or require additional information.

VIII. Ordering Part Numbers Impacted (Page 1 of 3)

The following products and ordering part numbers are impacted by these updates:

Model Name	MTCDT AEP 5.x Ordering Part Numbers	mLinux 5.x Ordering Part Numbers
MultiConnect® Conduit® IoT Programmable Gateways	MTCDT-246A-US-EU-GB MTCDT-247A-US-EU-GB MTCDT-H5-246A-US-EU-GB MTCDT-H5-247A-US-EU-GB MTCDT-L4E1-246A-EU-GB MTCDT-L4E1-247A-EU-GB MTCDT-LAP3-246A-AU MTCDT-LAT1-246A-US MTCDT-LAT1-247A MTCDT-LAT1-247A-US MTCDT-LDC3-246A-JP MTCDT-LDC3-247A-JP MTCDT-LEU1-246A-AU * MTCDT-LEU1-246A-EU-GB * MTCDT-LEU1-247A-AU * MTCDT-LEU1-247A-EU-GB * MTCDT-LSB3-246A-JP MTCDT-LSP3-246A-US MTCDT-LVW2-246A-US MTCDT-LVW2-247A MTCDT-LVW2-247A-US	MTCDT-246L-US-EU-GB MTCDT-247L-US-EU-GB MTCDT-H5-246L-US-EU-GB MTCDT-H5-247L-US-EU-GB MTCDT-L4E1-246L-EU-GB MTCDT-L4E1-247L-EU-GB MTCDT-LAT1-246L-US MTCDT-LAT1-247L-US MTCDT-LDC3-246L-JP MTCDT-LDC3-247L-JP MTCDT-LEU1-246L-AU * MTCDT-LEU1-246L-EU-GB * MTCDT-LEU1-247L-AU * MTCDT-LEU1-247L-EU-GB * MTCDT-LSB3-246L-JP MTCDT-LVW2-246L-US MTCDT-LVW2-247L-US
MultiConnect® Conduit® IoT Programmable Gateways with LoRa Accessory Cards	MTCDT-246A-868-EU-GB MTCDT-247A-868-EU-GB MTCDT-247A-915-US-EU-GB MTCDT-H5-246A-868-EU-GB MTCDT-H5-247A-868-EU-GB MTCDT-H5-247A-915-US MTCDT-L4E1-246A-868-EU-GB MTCDT-L4E1-246A-915-EU-GB-AU MTCDT-L4E1-247A-868-EU-GB MTCDT-L4E1-247A-915-EU-GB-AU MTCDT-LAP3-246A-915-AU MTCDT-LAP3-247A-915-AU MTCDT-LAT1-246A-915-US MTCDT-LAT1-247A-915-US MTCDT-LDC3-246A-923-JP MTCDT-LEU1-246A-868-EU-GB * MTCDT-LEU1-246A-915-EU-GB-AU * MTCDT-LEU1-247A-868-EU-GB * MTCDT-LEU1-247A-915-EU-GB-AU * MTCDT-LSB3-246A-923-JP MTCDT-LVW2-246A-915-US MTCDT-LVW2-247A-915-US	MTCDT-246L-868-EU-GB MTCDT-246L-923-JP MTCDT-247L-868-EU-GB MTCDT-H5-247L-868-EU-GB MTCDT-LAP3-246L-915-AU MTCDT-LAT1-246L-915-US MTCDT-LDC3-246L-923-JP MTCDT-LEU1-246L-868-EU-GB * MTCDT-LEU1-247L-868-EU-GB * MTCDT-LSB3-246L-923-JP MTCDT-LVW2-246L-915-US

* Products must be individually updated by the customer using information on www.multitech.net/developer/downloads or using DeviceHQ https://www.devicehq.com/sign_in

VIII. Ordering Part Numbers Impacted (Page 2 of 3)

The following products and ordering part numbers are impacted by these updates:

Model Name	MTCDT AEP 5.x Ordering Part Numbers	mLinux 5.x Ordering Part Numbers
MultiConnect® Conduit® IP67 Base Stations	MTCDTIP-266A-868 MTCDTIP-266A-868/2 MTCDTIP-266A-915 MTCDTIP-266A-915/2 MTCDTIP-266A-923-JP MTCDTIP-267A-868 MTCDTIP-267A-868/2 MTCDTIP-267A-915 MTCDTIP-267A-915/2 MTCDTIP-L4E1-266A-868 MTCDTIP-L4E1-266A-915 MTCDTIP-L4E1-267A-868 MTCDTIP-LAP3-266A-915 MTCDTIP-LAP3-266A-915/2 MTCDTIP-LAP3-267A-915 MTCDTIP-LAT1-266A-915 MTCDTIP-LAT1-266A-915/2 MTCDTIP-LAT1-267A-915 MTCDTIP-LAT1-267A-915/2 MTCDTIP-LDC3-266A-923-JP MTCDTIP-LEU1-266A-868 * MTCDTIP-LEU1-266A-868/2 * MTCDTIP-LEU1-266A-868-FRU * MTCDTIP-LEU1-266A-915 * MTCDTIP-LEU1-266A-915/2 * MTCDTIP-LEU1-267A-868 * MTCDTIP-LEU1-267A-868/2 * MTCDTIP-LEU1-267A-915/2 * MTCDTIP-LSB3-266A-923-JP MTCDTIP-LVW2-266A-915 MTCDTIP-LVW2-266A-915/2 MTCDTIP-LVW2-267A-915 MTCDTIP-LVW2-267A-915/2	MTCDTIP-266L-868 MTCDTIP-266L-868/2 MTCDTIP-266L-868/915 MTCDTIP-266L-915 MTCDTIP-266L-915/2 MTCDTIP-266L-923-JP MTCDTIP-267L-868 MTCDTIP-267L-868/2 MTCDTIP-267L-915 MTCDTIP-267L-915/2 MTCDTIP-LAT1-266L-915 MTCDTIP-LAT1-266L-915/2 MTCDTIP-LAT1-267L-915 MTCDTIP-LAT1-267L-915/2 MTCDTIP-LDC3-266L-923-JP MTCDTIP-LEU1-266L-868 * MTCDTIP-LEU1-266L-868/2 * MTCDTIP-LEU1-266L-868/915 * MTCDTIP-LEU1-266L-915 * MTCDTIP-LEU1-267L-868 * MTCDTIP-LEU1-267L-868/2 * MTCDTIP-LSB3-266L-923-JP MTCDTIP-LVW2-266L-915 MTCDTIP-LVW2-266L-915/2 MTCDTIP-LVW2-267L-915 MTCDTIP-LVW2-267L-915/2

* Products must be individually updated by the customer using information on www.multitech.net/developer/downloads or using DeviceHQ https://www.devicehq.com/sign_in

VIII. Ordering Part Numbers Impacted (Page 3 of 3)

The following products and ordering part numbers are impacted by these updates:

Model Name	MTCDT AEP 5.x Ordering Part Numbers	mLinux 5.x Ordering Part Numbers
MultiConnect® Conduit® IP67 Geolocation Base Station	MTCDTIP-LAT1-270A-915 MTCDTIP-LAT1-275A-915 MTCDTIP-LEU1-270A-868 * MTCDTIP-LEU1-275A-868 * MTCDTIP-LVW2-270A-915 MTCDTIP-LVW2-275A-915	MTCDTIP-L4E1-270L-868 MTCDTIP-L4E1-275L-868 MTCDTIP-LAT1-270L-915 MTCDTIP-LAT1-275L-915 MTCDTIP-LAT3-275L-915 MTCDTIP-LDC3-270L-923-JP MTCDTIP-LDC3-275L-923-JP MTCDTIP-LEU1-270L-868 * MTCDTIP-LEU1-275L-868 * MTCDTIP-LVW2-270L-915 MTCDTIP-LVW2-275L-915
MultiConnect® Conduit® AP (Access Point)	MTCAP-868-001A MTCAP-915-001A MTCAP-915-041A MTCAP-L4E1-868-001A MTCAP-LEU1-868-001A * MTCAP-LNA3-915-001A MTCAP-LNA3-915-041A MTCAP-LSP3-915-001A MTCAP-LSP3-915-041A	MTCAP-868-001L MTCAP-915-001L MTCAP-L4E1-868-001L MTCAP-LEU1-868-001L * MTCAP-LNA3-915-001L MTCAP-LSP3-915-001L

* Products must be individually updated by the customer using information on www.multitech.net/developer/downloads or using DeviceHQ https://www.devicehq.com/sign_in

IX. Resolved Common Vulnerabilities and Exposures (CVE) Resolved (page 1 of 3)

The operating system of the device has been upgraded from Linux kernel v3.12.70 to Linux kernel v4.9, which has resolved the following identified CVE:

CVE-2013-4312	CVE-2014-9892	CVE-2016-1575	CVE-2016-9685	CVE-2017-18218
CVE-2013-7421	CVE-2014-9900	CVE-2016-1576	CVE-2016-9754	CVE-2017-18221
CVE-2013-7445	CVE-2014-9904	CVE-2016-1583	CVE-2016-9755	CVE-2017-18222
CVE-2013-7446	CVE-2014-9914	CVE-2016-2053	CVE-2016-9756	CVE-2017-18224
CVE-2014-0038	CVE-2014-9922	CVE-2016-2069	CVE-2016-9777	CVE-2017-18232
CVE-2014-0049	CVE-2014-9940	CVE-2016-2070	CVE-2016-9793	CVE-2017-18241
CVE-2014-0069	CVE-2015-0239	CVE-2016-2085	CVE-2016-9794	CVE-2017-18249
CVE-2014-0077	CVE-2015-0274	CVE-2016-2117	CVE-2016-9806	CVE-2017-18255
CVE-2014-0131	CVE-2015-0275	CVE-2016-2184	CVE-2016-9919	CVE-2017-18257
CVE-2014-0155	CVE-2015-1328	CVE-2016-2185	CVE-2017-0523	CVE-2017-18261
CVE-2014-0181	CVE-2015-1333	CVE-2016-2186	CVE-2017-1000111	CVE-2017-18270
CVE-2014-0196	CVE-2015-1339	CVE-2016-2187	CVE-2017-1000112	CVE-2017-2583
CVE-2014-0206	CVE-2015-1420	CVE-2016-2188	CVE-2017-1000251	CVE-2017-2584
CVE-2014-1737	CVE-2015-1421	CVE-2016-2383	CVE-2017-1000252	CVE-2017-2596
CVE-2014-1738	CVE-2015-1465	CVE-2016-2384	CVE-2017-1000363	CVE-2017-2636
CVE-2014-1739	CVE-2015-1573	CVE-2016-2543	CVE-2017-1000364	CVE-2017-2647
CVE-2014-1874	CVE-2015-1593	CVE-2016-2544	CVE-2017-1000365	CVE-2017-2671
CVE-2014-2038	CVE-2015-1805	CVE-2016-2545	CVE-2017-1000370	CVE-2017-5549
CVE-2014-2039	CVE-2015-2041	CVE-2016-2546	CVE-2017-1000380	CVE-2017-5550
CVE-2014-2309	CVE-2015-2042	CVE-2016-2547	CVE-2017-1000405	CVE-2017-5551
CVE-2014-2523	CVE-2015-2150	CVE-2016-2548	CVE-2017-10661	CVE-2017-5576
CVE-2014-2568	CVE-2015-2666	CVE-2016-2549	CVE-2017-10662	CVE-2017-5577
CVE-2014-2672	CVE-2015-2672	CVE-2016-2550	CVE-2017-10663	CVE-2017-5669
CVE-2014-2673	CVE-2015-2830	CVE-2016-2782	CVE-2017-10810	CVE-2017-5967
CVE-2014-2678	CVE-2015-2922	CVE-2016-2847	CVE-2017-10911	CVE-2017-5970
CVE-2014-2706	CVE-2015-2925	CVE-2016-3070	CVE-2017-11176	CVE-2017-5986
CVE-2014-2851	CVE-2015-3212	CVE-2016-3134	CVE-2017-11472	CVE-2017-6001
CVE-2014-3122	CVE-2015-3288	CVE-2016-3135	CVE-2017-11473	CVE-2017-6074
CVE-2014-3144	CVE-2015-3290	CVE-2016-3136	CVE-2017-11600	CVE-2017-6214
CVE-2014-3145	CVE-2015-3291	CVE-2016-3137	CVE-2017-12146	CVE-2017-6345
CVE-2014-3153	CVE-2015-3331	CVE-2016-3138	CVE-2017-12153	CVE-2017-6346
CVE-2014-3181	CVE-2015-3332	CVE-2016-3139	CVE-2017-12154	CVE-2017-6347
CVE-2014-3182	CVE-2015-3339	CVE-2016-3140	CVE-2017-12168	CVE-2017-6348
CVE-2014-3183	CVE-2015-3636	CVE-2016-3156	CVE-2017-12188	CVE-2017-6353
CVE-2014-3184	CVE-2015-4001	CVE-2016-3672	CVE-2017-12190	CVE-2017-6874
CVE-2014-3185	CVE-2015-4002	CVE-2016-3689	CVE-2017-12192	CVE-2017-6951
CVE-2014-3534	CVE-2015-4003	CVE-2016-3713	CVE-2017-12193	CVE-2017-7187
CVE-2014-3601	CVE-2015-4004	CVE-2016-3841	CVE-2017-13693	CVE-2017-7261

IX. Resolved Common Vulnerabilities and Exposures (CVE) Resolved (page 2 of 3)

The operating system of the device has been upgraded from Linux kernel v3.12.70 to Linux kernel v4.9, which has resolved the following identified CVE:

CVE-2014-3631	CVE-2015-4170	CVE-2016-4470	CVE-2017-13715	CVE-2017-7308
CVE-2014-3646	CVE-2015-4176	CVE-2016-4482	CVE-2017-14051	CVE-2017-7346
CVE-2014-3647	CVE-2015-4177	CVE-2016-4485	CVE-2017-14106	CVE-2017-7374
CVE-2014-3673	CVE-2015-4178	CVE-2016-4486	CVE-2017-14140	CVE-2017-7472
CVE-2014-3687	CVE-2015-4692	CVE-2016-4557	CVE-2017-14156	CVE-2017-7477
CVE-2014-3688	CVE-2015-4700	CVE-2016-4558	CVE-2017-14340	CVE-2017-7487
CVE-2014-3690	CVE-2015-5156	CVE-2016-4565	CVE-2017-14489	CVE-2017-7495
CVE-2014-3917	CVE-2015-5157	CVE-2016-4568	CVE-2017-14497	CVE-2017-7533
CVE-2014-3940	CVE-2015-5257	CVE-2016-4569	CVE-2017-14954	CVE-2017-7541
CVE-2014-4014	CVE-2015-5283	CVE-2016-4578	CVE-2017-14991	CVE-2017-7542
CVE-2014-4027	CVE-2015-5307	CVE-2016-4580	CVE-2017-15102	CVE-2017-7616
CVE-2014-4157	CVE-2015-5327	CVE-2016-4581	CVE-2017-15115	CVE-2017-7618
CVE-2014-4171	CVE-2015-5364	CVE-2016-4794	CVE-2017-15116	CVE-2017-7645
CVE-2014-4322	CVE-2015-5366	CVE-2016-4805	CVE-2017-15127	CVE-2017-7889
CVE-2014-4508	CVE-2015-5697	CVE-2016-4913	CVE-2017-15128	CVE-2017-7895
CVE-2014-4608	CVE-2015-6252	CVE-2016-4951	CVE-2017-15129	CVE-2017-8797
CVE-2014-4611	CVE-2015-6526	CVE-2016-4997	CVE-2017-15265	CVE-2017-8824
CVE-2014-4652	CVE-2015-6937	CVE-2016-4998	CVE-2017-15274	CVE-2017-8831
CVE-2014-4653	CVE-2015-7513	CVE-2016-5195	CVE-2017-15299	CVE-2017-8890
CVE-2014-4654	CVE-2015-7515	CVE-2016-5243	CVE-2017-15306	CVE-2017-8924
CVE-2014-4655	CVE-2015-7550	CVE-2016-5244	CVE-2017-15537	CVE-2017-8925
CVE-2014-4656	CVE-2015-7566	CVE-2016-5400	CVE-2017-15649	CVE-2017-9059
CVE-2014-4667	CVE-2015-7613	CVE-2016-5412	CVE-2017-15868	CVE-2017-9074
CVE-2014-4699	CVE-2015-7799	CVE-2016-5696	CVE-2017-15951	CVE-2017-9075
CVE-2014-5045	CVE-2015-7872	CVE-2016-5728	CVE-2017-16525	CVE-2017-9076
CVE-2014-5077	CVE-2015-7884	CVE-2016-5828	CVE-2017-16526	CVE-2017-9077
CVE-2014-5206	CVE-2015-7885	CVE-2016-5829	CVE-2017-16527	CVE-2017-9150
CVE-2014-5207	CVE-2015-7990	CVE-2016-6130	CVE-2017-16528	CVE-2017-9211
CVE-2014-5471	CVE-2015-8104	CVE-2016-6136	CVE-2017-16529	CVE-2017-9242
CVE-2014-5472	CVE-2015-8215	CVE-2016-6156	CVE-2017-16530	CVE-2017-9605
CVE-2014-6410	CVE-2015-8374	CVE-2016-6187	CVE-2017-16531	CVE-2017-9984
CVE-2014-6416	CVE-2015-8539	CVE-2016-6197	CVE-2017-16532	CVE-2017-9985
CVE-2014-6417	CVE-2015-8543	CVE-2016-6198	CVE-2017-16533	CVE-2017-9986
CVE-2014-6418	CVE-2015-8569	CVE-2016-6213	CVE-2017-16534	CVE-2018-10021
CVE-2014-7145	CVE-2015-8575	CVE-2016-6327	CVE-2017-16535	CVE-2018-10074
CVE-2014-7283	CVE-2015-8660	CVE-2016-6480	CVE-2017-16536	CVE-2018-10087
CVE-2014-7822	CVE-2015-8709	CVE-2016-6516	CVE-2017-16537	CVE-2018-10124
CVE-2014-7825	CVE-2015-8746	CVE-2016-6786	CVE-2017-16538	CVE-2018-10322

IX. Resolved Common Vulnerabilities and Exposures (CVE) Resolved (page 3 of 3)

The operating system of the device has been upgraded from Linux kernel v3.12.70 to Linux kernel v4.9, which has resolved the following identified CVE:

CVE-2014-3610	CVE-2015-4036	CVE-2016-3955	CVE-2017-13694	CVE-2017-7277
CVE-2014-3611	CVE-2015-4167	CVE-2016-4440	CVE-2017-13695	CVE-2017-7294
CVE-2014-7826	CVE-2015-8767	CVE-2016-6787	CVE-2017-16643	CVE-2018-10323
CVE-2014-7841	CVE-2015-8785	CVE-2016-6828	CVE-2017-16644	CVE-2018-1065
CVE-2014-7842	CVE-2015-8787	CVE-2016-7039	CVE-2017-16645	CVE-2018-1066
CVE-2014-7843	CVE-2015-8812	CVE-2016-7042	CVE-2017-16646	CVE-2018-10675
CVE-2014-7970	CVE-2015-8816	CVE-2016-7097	CVE-2017-16647	CVE-2018-1091
CVE-2014-7975	CVE-2015-8844	CVE-2016-7117	CVE-2017-16648	CVE-2018-1092
CVE-2014-8086	CVE-2015-8845	CVE-2016-7425	CVE-2017-16649	CVE-2018-1093
CVE-2014-8133	CVE-2015-8944	CVE-2016-7910	CVE-2017-16650	CVE-2018-1094
CVE-2014-8134	CVE-2015-8950	CVE-2016-7911	CVE-2017-16939	CVE-2018-10940
CVE-2014-8160	CVE-2015-8952	CVE-2016-7912	CVE-2017-16994	CVE-2018-1095
CVE-2014-8369	CVE-2015-8953	CVE-2016-7913	CVE-2017-16995	CVE-2018-1108
CVE-2014-8480	CVE-2015-8955	CVE-2016-7914	CVE-2017-17052	CVE-2018-11232
CVE-2014-8481	CVE-2015-8956	CVE-2016-7915	CVE-2017-17053	CVE-2018-1130
CVE-2014-8559	CVE-2015-8961	CVE-2016-7916	CVE-2017-17448	CVE-2018-11506
CVE-2014-8709	CVE-2015-8962	CVE-2016-7917	CVE-2017-17449	CVE-2018-11508
CVE-2014-8884	CVE-2015-8963	CVE-2016-8630	CVE-2017-17450	CVE-2018-5332
CVE-2014-8989	CVE-2015-8964	CVE-2016-8632	CVE-2017-17558	CVE-2018-5333
CVE-2014-9090	CVE-2015-8966	CVE-2016-8633	CVE-2017-17712	CVE-2018-5344
CVE-2014-9322	CVE-2015-8967	CVE-2016-8636	CVE-2017-17741	CVE-2018-5703
CVE-2014-9419	CVE-2015-8970	CVE-2016-8645	CVE-2017-17805	CVE-2018-5750
CVE-2014-9420	CVE-2015-9004	CVE-2016-8646	CVE-2017-17806	CVE-2018-6412
CVE-2014-9428	CVE-2016-0723	CVE-2016-8650	CVE-2017-17807	CVE-2018-6927
CVE-2014-9529	CVE-2016-0728	CVE-2016-8655	CVE-2017-17862	CVE-2018-7273
CVE-2014-9584	CVE-2016-0758	CVE-2016-8658	CVE-2017-17864	CVE-2018-7480
CVE-2014-9585	CVE-2016-0821	CVE-2016-8660	CVE-2017-17975	CVE-2018-7492
CVE-2014-9644	CVE-2016-0823	CVE-2016-8666	CVE-2017-18075	CVE-2018-7740
CVE-2014-9683	CVE-2016-10044	CVE-2016-9083	CVE-2017-18079	CVE-2018-7755
CVE-2014-9710	CVE-2016-10088	CVE-2016-9084	CVE-2017-18174	CVE-2018-7757
CVE-2014-9715	CVE-2016-10147	CVE-2016-9120	CVE-2017-18193	CVE-2018-7995
CVE-2014-9717	CVE-2016-10150	CVE-2016-9178	CVE-2017-18200	CVE-2018-8043
CVE-2014-9728	CVE-2016-10200	CVE-2016-9191	CVE-2017-18202	CVE-2018-8087
CVE-2014-9729	CVE-2016-10208	CVE-2016-9313	CVE-2017-18203	CVE-2018-8781
CVE-2014-9730	CVE-2016-10229	CVE-2016-9555	CVE-2017-18204	CVE-2018-8822
CVE-2014-9731	CVE-2016-10318	CVE-2016-9576	CVE-2017-18208	
CVE-2014-9803	CVE-2016-1237	CVE-2016-9588	CVE-2017-18216	

X. MultiConnect® Conduit® IoT Gateways

MultiConnect® 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 MultiConnect Conduit series comes in three variants designed to address specific IoT gateway use cases:

- **MultiConnect Conduit:** Indoor industrial gateway, ideal for environments that require metal casing for protection against particles and debris and require an industrial temperature range.

- **MultiConnect Conduit IP67 Base Station:** Outdoor IP67-rated gateway ideal suited for performing in harsh environments such as rain, snow, extreme heat, and high winds.

- **MultiConnect 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.

XI. Additional Information

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

World Headquarters – U.S.A.
+1 (763) 785-3500 | sales@multitech.com

EMEA Headquarters – UK
+(44) 118 959 7774 | sales@multitech.co.uk

For additional information on MultiTech mPower™ Edge Intelligence Software, please visit:

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