Software Release Notes

mPower® Edge Intelligence Software

Includes mPower 6.0.0

Models Impacted:

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

Overview

mPower™ Edge Intelligence is MultiTech's embedded software offering delivering 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.

Contents

Notes

This document includes the release notes and cumulative changelog for mPower Edge Intelligence software. Detailed information is listed in reverse chronological order, starting with the most recent mPower release:

- Operating system updates
- New hardware supported
- New features
- Enhanced features
- Known behaviors
- Bug fixes
- Feature deprecations

Additional Resources:

- mPower 5.X Software Release Notes:
  https://www.multitech.com/documents/publications/sales-flyers/mPower
- Downloads: http://www.multitech.net/developer/downloads/
- Getting Started: http://www.multitech.net/developer/software/aep/creating-a-custom-application/
- API Reference: http://www.multitech.net/developer/software/mtr-api-reference/
- Support: Visit https://support.multitech.com/ to create a support case
- DeviceHQ, Cloud-based IoT Device Management, Login: https://www.devicehq.com/sign_in

mPower 6.0.0 Changelog and Overview

May 2022

Updates in mPower 6.0.0, from mPower 5.3.X

OS Changes	New Hardware	New Features	Feature Enhancement	Known Behaviors	Bug Fixes	Deprecations	Schedule	Models Impacted	Upgrade Process

Operating System Updates (mPower 6.0.0)

Updated Yocto Version • Yocto version updated to Dunfell (version 3.1). • Previous versions of mPower used Yocto Thud (version 2.6)	GP-1322 MTX-4162
Updated Linux Kernel • Linux kernel updated to version 5.4.81 • Previous versions of mPower used Linux kernel v4.9.240	-
Updated Python • Python updated to version 3.8.11 • Previous versions of mPower used Python 2.7	GP-1224 MTX-4164

New Features (mPower 6.0.0)

IP Masquerading The IP Masquerading feature allows users to enable or disable IP Masquerading for WAN interfaces of the device • Main points ○ IP Masquerading feature can be used with WAN interfaces only ○ IP Masquerading is enabled by default. When IP Masquerading feature is enabled, the device performs IP address translation of client network traffic to the corresponding WAN interface ○ When IP Masquerading feature is disabled, the device passes client network requests unchanged to the corresponding WAN interface ○ API Changes ○ api/ni/nis: “wanMasquerade” option is added for each network interface	MTX-4104
Downgrade Protection • mPower 6.0.0 includes a means of identifying MTCDT (MTCDT-0.2) and MTCDTIP (MTCDTIP-0.1) devices with substitute components and limits the version of mPower that customers can use ○ Devices with substitute components can only be used with mPower 5.3.7 and later ○ Future mPower versions will not allow MTCDT-0.2 and MTCDTIP-0.1 devices with substitute components to downgrade to versions of mPower prior to mPower 5.3.7 • Error Messages: If a user attempts to downgrade a device with substitute components to an incompatible firmware version, an error message will be displayed: ○ Downgrade using API Command: "Firmware check failed. Invalid firmware version for [MTCDT-0.2] hardware." "Firmware check failed. Invalid firmware version for [MTCDTIP-0.1] hardware." ○ Downgrade using DeviceHQ: "Software check failed. Invalid firmware version for [MTCDT-0.2] hardware." ○ "Software check failed. Invalid firmware version for [MTCDTIP-0.1] hardware." • MTCAP, MTCAP2, and MTCDTIP2 devices do not include downgrade protection	GP-1431 MTX-4299 GP-1385

New Features (mPower 6.0.0)

<table>
<tr><td>Remote Syslog Feature Enhancement: TCP and SSL/TLS support
• New settings are implemented for the Remote Syslog feature:
○ TCP Protocol support
○ SSL/TLS Protocol support
○ Configurable Port
• The Hostname read-only field is added to the Remote Syslog pane. The hostname value is a part of log entries that are transferred to the remote Syslog Server. The hostname value can be configured in the Hostname Configuration pane on the Status | Global DNS page
• API Changes
○ api/syslog
○ api/help/syslog
○ api/secureprotocols/rsyslogd</td><td>GP-869
MTX-4178
GP-1365
MTX-4205</td></tr>
<tr><td>Support 802.1X authentication on the Ethernet interface(s)
• 802.1X Authentication feature is available for Ethernet network interface (Eth0, Eth1, Eth2) if it is not in the Bridge (BR0). For other network interfaces, including Bridge (BR0) this feature is not available and is hidden on Web UI
• The 802.1X Authentication settings depend on the Authentication Method. By default, the Authentication Method is NONE
• The system supports the following authentication methods:
○ EAP-PWD
○ EAP-TLS
○ EAP-TTLS
○ EAP-PEAP
The following settings are available and depend on the Authentication Method:
<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>Authentication method</td><td>Type of the authentication</td></tr>
<tr><td>Username</td><td>Identity (user name) to authenticate the user in the inner (phase 2) authentication</td></tr>
<tr><td>Password (not used in EAP-TLS)</td><td>The secret string to be used for EAP-PWD authentication</td></tr>
<tr><td>Anonymous ID</td><td>Anonymous identity to authenticate the user in the outer (phase 1) authentication</td></tr>
<tr><td>CA Certificate (not used in EAP-PWD)</td><td>X.509 Certification Authority certificate</td></tr>
<tr><td>Domain Match (not used in EAP-PWD, optional)</td><td>Domain substring for server certificate validation</td></tr>
<tr><td>Subject Match (EAP-TLS only, optional)</td><td>Subject substring for server certificate validation</td></tr>
<tr><td>Client Certificate (EAP-TLS only)</td><td>X.509 client certificate</td></tr>
<tr><td>Private Key (EAP-TLS only)</td><td>Private key of the client</td></tr>
<tr><td>Private Key Password (EAP-TLS only)</td><td>Password to decrypt the private key</td></tr>
<tr><td>Authentication Method (EAP-TTLS and EAP-PEAP only)</td><td>Type of the inner (phase 2) authentication</td></tr>
<tr><td>PEAP Version (EAP-PEAP only)</td><td>Version of the PEAP protocol</td></tr>
</table>
</td><td>GP-355
GP-1328
MTX-3053
MTX-4119
MTX-4170</td></tr>
</table>

New Features (mPower 6.0.0)

Ping Feature Settings: New Options • Number of Requests: The number of ping requests. The default is 4. The maximum is 120 • Packet Size (Bytes): Specifies the number of data bytes to be sent ○ Packets include an additional 28 bytes of data (8 bytes ICMP header and 20 bytes IP header) ○ The default packet size is 56 bytes (which equates to into 84 bytes of data due to ICMP header and IP header) • When packet size of 0 bytes is requested, the actual packet size is 28 bytes due to ICMP header and IP header • Do Not Fragment: Enable to prevent fragmentation. Without fragmentation, the ping fails if the ping packet exceeds MTU size for the network path. By default, the option is disabled	GP-1279 MTX-4036 MTX-4131
Continuous Ping • The Continuous Ping feature allows users to start a continuous ping to an IP address or URL through a specific interface • Continuous Ping is available on the Debug Options page • To start a continuous ping, users specify **IP Address** or **URL**, **Network Interface**, **Packet Size,** and enable or disable the **Do Not Fragment** option ○ Continuous Ping starts when the user clicks the **Start Continuous Ping** button 1. The system starts pinging 2. The button label changes to **Stop Continuous Ping** 3. The message "Ping is in progress…" is displayed next to the button ○ Continuous Ping stops when the user clicks the **Stop Continuous Ping** button 1. The system stops pinging 2. The button label changes to **Start Continuous Ping** 3. The ping results are shown next to the **Start Continuous Ping** button • API Changes ○ api/stats/continuousPing - Continuous Ping status is stored in the "**isRunning**" field	GP-1229 MTX-4033 MTX-4131
ICMP Keep Alive feature • Overview: Sometimes when working with private networks, the size of the ping request is regulated. It needs to be configurable to satisfy private network requirements • In mPower 6.0.0, new setting "Packet Size (Bytes)" is added next to the ICMP Count in the ICMP/TCP Check pane ○ The Packet Size setting specifies the number of data bytes to be sent ○ Packets include an additional 28 bytes of data (8 bytes ICMP header and 20 bytes IP header) ○ The default packet size is 56 bytes (which equates to into 84 bytes of data due to ICMP header and IP header) ○ When packet size of 0 bytes is requested, the actual packet size is 28 bytes due to ICMP header and IP header	GP-79 MTX-4167

New Features (mPower 6.0.0)

Firewall Status Page • The **Status** page is added under the **Firewall** main menu • Firewall status page contains Filter tables in the **Filter Rules** pane, NAT tables in the **NAT Rules** pane, and iptables-save command output in the **IP Tables Dump** • The **Download** button allows users to download an archive file that contains the same information that is displayed on Web UI; there are three files in the archive: ○ **iptables-filter.log** ○ **iptables-nat.log** ○ **iptables-save.log** • API Changes. The following API endpoints are added: ○ https://192.168.2.1/api/firewall/downloadStatus ○ https://192.168.2.1/api/firewall/status	MTX-4106
IPSec Tunnels - the "Allow All Traffic" option (firewall rule that drops or allows all traffic through the tunnel) • The "Allow All Traffic" checkbox is added to the IPsec tunnel configuration. The option is disabled by default when adding a new tunnel • When the checkbox is disabled, all traffic through the tunnel is dropped and the user has to add firewall rules manually to allow the traffic. Enabling the checkbox allows all traffic through the tunnel without creating explicit rules to allow traffic by subnet and/or connection attributes • When performing a firmware upgrade from a previous firmware version that does not have this setting, all existing tunnels will have the "Allow All Traffic" checkbox enabled and corresponding firewall rules will be set in the system, so nothing will change in tunnel behavior after upgrade • When adding a new tunnel, if the "Allow All Traffic" checkbox is not checked, then ALL traffic through the tunnel will be dropped. The user will have to add a corresponding firewall rules on the Firewall Settings page • API Changes ○ The "allowAllTraffic" is added to the api/ipsecTunnels collection	GP-1361 MTX-4200
IPSec Tunnels - Multiple Remote Networks Support • The system allows to specify multiple local networks and remote networks when configuring an IPSec tunnel • API changes ○ "remoteSubnets" array replaced the "remoteNetworkIp" and "remoteNetworkMask" in the /api/ipsecTunnels collection	GP-1337 MTX-4180

New Features (mPower 6.0.0)

Making cellular radios data-only on AT&T network • Overview: Since all new mPower devices are certified as data-only devices, mPower shall disable voice support for new voice-capable radios in an AT&T-Compatible configuration • The change affects the following list of AT&T-compatible voice-capable cellular radios: ○ -L4N1 radios with the "AT&T-compatible" firmware image ○ -L4G1 radios with AT&T SIM cards installed ○ -LNA7 radios with AT&T SIM cards installed • If the system detects that the modem is -L4N1, -L4G1, or -LNA7 and the carrier is AT&T, it checks for the voice-related configuration in the modem. If the voice support is enabled and SMS-only mode is disabled, the system executes AT commands to disable voice support and enable SMS-only mode • UI changes ○ If the voice support is disabled, the Wake Up On Call feature does not support the Wake Up settings "On Caller-ID" and "On Ring." ○ The system displays a message if one of these settings is enabled when user saves changes in the Wake Up On Call configuration **On Ring and On Caller ID options cannot be enabled in the Wake Up On Call configuration as voice calls are not supported by your carrier** • The radio-query has a new option (--voice-support) that allows the user to get the current voice support settings set in the cellular radio ○ radio-query --voice-support shows the information in the following format: { *"smsOnly" : "Indicates that registration flag is enabled or not : BOOL"* *"voiceEnabled" : "Indicates that voice support is enabled or not : BOOL"* *}* • The **radio-cmd** has a new option (**--disable-voice-support)** that disables support of voice calls. It accepts no additional parameters and returns "0" on success and "1" on failure. ○ Usage: *root@mtcdt:/var/config/home/admin# radio-cmd –disable-voice-support* *Success* • There is no command to enable voice support. To enable voice support, the user shall use the appropriate AT commands	GP-1364 MTX-4206 GP-1390 MTX-4251
Serial Port Configuration • Models Impacted: MTCDT with MTAC-MFSER-DTE or MTAC-MFSER-DCE Gateway Accessory Card • Device is configurable to one of the following protocols: RS-232, RS-485 (half-duplex), or RS485 (full duplex) • If RS-485 is selected, the checkbox **RS-485 Termination** is shown. RS-485 termination should be enabled if this is the first or the last device in the chain	GP-1178 MTX-3995 MTX-4337

Feature Enhancement (mPower 6.0.0)

Updated Modbus slave feature • In order to add support of new cellular radios, the Modbus Slave feature is updated in mPower 6.0.0 to use the generic implementation for all band-related queries • For Modbus query information: http://www.multitech.net/developer/software/mtr-software/mtr-modbus-information/	GP-862 MTX-4190
Serial-IP: Modbus Gateway and Serial-IP settings improvements • The Mode dropdown is added to the General Configuration pane. It allows users to enable one of the following features: ○ Disabled (default). Serial-IP and Modbus RTU/TCP Gateway are disabled ○ Serial-IP ○ Modbus RTU/TCP Gateway ○ Serial-IP and Modbus RTU/TCP Gateway cannot work simultaneously • The system allows customers to configure the Serial Port. Serial Port can be used by other features such as GPS • To use Modbus Gateway, check Protocol under IP Pipe and select SSL/TLS ○ Modbus RTU slave is connected to the Serial Port and a remote Modbus TCP Master ○ Modbus Gateway application works as a translator between Modbus RTU (slave) and Modbus-TCP (master) devices ○ Without Modbus Gateway enabled, the Serial-IP feature simply passes raw data between the serial DB9 interface and the socket representing the TCP connection in the system to a configured remote device ○ When the Modbus Gateway is enabled, its application runs in the system. The application works as a translator converting between the Modbus-TCP and Modbus RTU protocols. The Modbus Gateway passes data between an RTU connected to the serial port and a Modbus TCP remote client/server	GP-1432 MTX-4301
Ping Feature – Update the Network Interfaces List • The list of the network interfaces available in the Network Interface dropdown list is updated • The list of available network interfaces depends on the hardware configuration • The following network interfaces are available: ○ ANY ○ BRIDGE (BR0) ○ CELLULAR ○ WI-FI WAN ○ WI-FI AP ○ ETHERNET (ETH0) ○ ETHERNET (ETH1) ○ ETHERNET (ETH2)	GP-1320 MTX-4150
PPP-IP Pass-through / Serial Modem Mode - Hide Ping features from the Debug Options Page • PPP-IP Pass-through Mode: ○ It is not possible to ping directly from the device ○ The Ping and Continuous Ping features are not available in the Debug Options Page • Serial Modem Mode: ○ Continuous Ping feature is not available ○ Ping feature is available. Network Interface options include: ANY, BRIDGE (BR0) and ETHERNET (ETH0)	MTX-4093

Feature Enhancement (mPower 6.0.0)

Service Statistics Enhancement The status for new services are added to the Service Statistics Page. Services and their possible statuses are listed below: SNMP Server ○ SNMP Server is disabled ○ SNMP Server is running ○ SNMP Server is stopped Security Violation ○ Security violation is disabled ○ Security violation has not been detected ○ Security violation has been detected (shown if the /var/log/tomoyo/reject_003.log log is NOT empty) Reverse SSH ○ Reverse SSH service is disabled ○ Reverse SSH service is running ○ Reverse SSH service is stopped MQTT Broker ○ MQTT Broker service is disabled ○ MQTT Broker service is running ○ MQTT Broker service is stopped Remote Management ○ Displaying statuses from the Remote Management page. Continuous Ping ○ Continuous ping is running ○ Continuous ping is disabled	GP-1295 MTX-4142
Cellular Radio Firmware Upgrade Changes • Menu name changed to "Cell Radio FW Upgrade" • Page name changed to “Cellular Radio Firmware Upgrade” • “Cell Radio Firmware Upgrade” shall be in the setup menu, below time configuration (PPP-IP pass-through mode and serial modem mode)	GP-1451 MTX-4343
Rogers Wireless – Web Interface Update • In earlier versions of mPower software, the Web Interface (Cellular, Radio Status) displays the following when a Rogers SIM was inserted in the MTR device **Home Network: Rogers AT&T Wireless** • In mPower MTR 5.3.5A, the Web Interface (Cellular, Radio Status) has been updated to display the following with a Rogers SIM is inserted in the MTR device **Home Network: Rogers Wireless**	GP-1388 MTR only?
Web UI Improvement • Material design icons added throughout the web UI • Material design icons are a set of universal icons used to promote simplicity • Additional Information: https://materialdesignicons.com/	GP-1362 MTX-4201
Web UI Improvement (Wizard and Support Page) • Updated product images added to the First-Time Setup Wizard and Support Page	GP-1371 MTX-4217

Feature Enhancement (mPower 6.0.0)

Support static IP on Wi-Fi as WAN • Ability to disable DHCP Client and enable **Static** mode is implemented for WLAN0 (Wi-Fi as WAN) network interface • In mPower 6.0.0 the WLAN0 network interface can be configured in the following modes: ○ DHCP Client (default) ○ DHCP Client – Addresses Only ○ Static	GP-76 MTX-4186 SP-5084144
Firewall Settings Improvement • Firewall settings, "Normal" now includes the following. This is also the default view. This view was formerly "Advanced" ○ Prerouting Rules ○ Input Filter Rules ○ Forward Filter Rules ○ Output Filter Rules • Firewall settings, "Normal" now includes the following. This view was formerly "Legacy" ○ Port Forwarding ○ Input Filter Rules ○ Output Filter Rules	GP-1426 MTX-4286
IPsec, GRE, OpenVPN Tunnels - Enabled checkbox is moved to the tunnel configuration page • This is an improvement that does not affect the GRE, IPSec and OpenVPN functionality and API • The "Check" icon in the Enabled column on the GRE, IPSec or OpenVPN Tunnel Configuration page does not allow the user to enable or disable a tunnel • To enable or disable a tunnel, click the **Enabled** checkbox while adding or editing tunnel	GP-1392 MTX-4255
SNMP Configuration Page - Network Address and Mask validation, IP address conversion to the Network address • In the previous mPower releases, the system displayed an error if the entered IP Address and Mask do not match while adding an IP network to the Allowed IP Addresses list on the SNMP Configuration page • In mPower 6.0.0 the system automatically converts the IP address based on the Mask value, and adds a corresponding valid Network Address to the list:	GP-1468 MTX-4387
Network IP and Mask validation (GRE and IPSec Configuration) • The system (Web UI) checks the entered IP Address and Mask and automatically converts the IP address value to a valid Network Address while adding or editing GRE or IPsec Tunnels • The API validation of the entered Network Address and Mask is implemented and the system does not allow to save the settings if the Network Address and Mask do not match • For example, user enters **Remote Network Route** as **192.168.2.2** and the **Remote Network Mask** as **24** while editing a GRE Tunnel. The Network Address in this case is 192.168.2.0, and the system will automatically change it and add a valid Network address, so the remote network route will be a valid value of **192.168.2.0/24** • The same conversion is performed for Local Networks and Remote Networks when adding or editing an IPSec tunnel	GP-1453 GP-1287 MTX-4353 MTX-4118

Feature Enhancement (mPower 6.0.0)

Add a status message when a partial configuration in the Web UI is applied via DHQ • In the previous releases, the system does not show a message when a partial configuration upgrade is performed • In mPower 6.0.0, when a device checks into DeviceHQ and performs a partial configuration upgrade, the system displays a status message on Web UI: "Partial configuration has been applied. The system is going down for reboot now. (DATE/TIME)"	GP-418 MTX-4140 IN003879
UXPF utility upgrade • Utilities used to upgrade Telit radio firmware (v.1.7.2-0) • Models Impacted: MTCAP-L4E1, MTCAP-LNA3, MTCDT-L4E1, MTCDT-LAT3, MTCDT-L4N1, MTCDTIP- L4E1, MTCDTIP-L4N1 http://www.multitech.net/developer/software/mlinux/using-mlinux/using-uxfp-to-upgrade-telit-firmware/	GP-1079 MTX-4037
Web Server X.509 Certificate - Default details are updated • The CN value in the default Web Server X.509 certificate is changed from **ocg.example.com** to **mtx.example.com**	GP-1247 MTX-4058
Reset to User Defined Defaults shall restore custom applications • If a custom application is installed while a user sets the current configuration as user-defined defaults, the system shall try to restore it when performing reset to User Defined defaults • Main use case ○ Install a custom application, configure the device, save the changes and set the current configuration as user-defined defaults ○ Change the configuration (make any changes you need), save and apply the changes ○ Click "Reset to User Defined Defaults" • **Result** ○ Device reboots ○ overlayfs is reset ○ The system installs the custom application from /var/persistent ○ Device reboots again as soon as the custom app is installed NOTE: Actual behavior depends on the custom application ○ When device boots, the custom application is installed	GP-1326 MTX-4154
Update MODBUS slave feature • In order to add support of new cellular radios, the Modbus Slave feature is updated in mPower 6.0 to use the generic implementation for all band-related queries	GP-862 MTX-4190
Add a status message when a partial configuration in the Web UI is applied via DHQ • In the previous releases, the system does not show a message when a partial configuration upgrade is performed • In mPower 6.0.0, when a device checks into DeviceHQ and performs a partial configuration upgrade, the system displays a status message on Web UI: "Partial configuration has been applied. The system is going down for reboot now. (DATE/TIME)"	GP-418 MTX-4140 IN003879

Feature Enhancement (mPower 6.0.0)

LoRa UI/API Changes: • Added Duty-cycle info to Gateways page if ISRAEL plan is selected or duty-cycle is enabled • Added Default Device Profile for local join server on Key Management page • API Default packet forwarder GW SOURCE for EUI to hardware ○ The web page would not load an EUI unless the Basic Settings were shown • Add delete all end-device and session records button • Add option to append csv/json device records to the current list on key management page • Add button to delete all items from downlink queue for all devices • API options to get a single device or session record use DevEUI ○ /api/lora/devices/00-11-22-33-44-55-66-77 ○ /api/lora/sessions/00-11-22-33-44-55-66-77 • Added option for settingmulticastGroupID for operations • Add option for max FUOTA packet size ○ Field in Network Settings > Datarate settings ○ Field in Operations > Show Settings section	
LoRa Firmware Update Over The Air (FUOTA) Changes: • LoRa FUOTA Version 1.0.17 • Added option for maximum packet size to control fragmentation • Added option for setting multicast group ID	
LoRa Network Server Changes: • LoRa Network Server Version 2.5.37 • Add setting for max FOTA packet size (maxRx2PacketSize) • Add command to delete all queued downlinks • Add command to get single device or session by EUI • Add command to delete all devices and sessions • Add command to add list of devices or sessions • Publish lora/<APP-EUI>/<DEV-EUI>/moved topic when device is deleted by command, UI or LENS ○ Message contains list of GW-EUI • Database backup to tar.gz ○ Backup to RAM and move into /var/config directory ○ Reduce database in /var/config/ to one-fifth ▪ 2MB database takes 400K with redundant backup files • Activate Tx Param controller for LW102 AU915 and AS923 devices on Join • LENS: published moved MQTT messages when check in update moves devices • 2.5.37 Added fields to the “up” mqtt messages ○ name – device name ○ product_id – device product ID ○ serial_number – device serial number ○ hardware_version – device hardware versionm ○ firmware_version – device firmware version	

Feature Enhancement (mPower 6.0.0)

LoRa Default App Changes • MQTT QoS and Persist settings • MQTT Resubscribe on connect • Add ClientID configuration option • Add subscriptions for downlinks from remote broker ○ lorawan/gweui/deveui/down ○ lorawan/gwuuid/deveui/down • Add subscription for moved devices to publish to remote broker ○ lorawan/appeui/deveui/moved	
LoRa Packet Forwarder Changes: • Packet Forwarder Version 4.0.17 • LoRa Gateway Version 5.0.11 • Add hardware reset on start-up and restart • Support added for two MTAC-LORA-H-868 or two MTAC-LORA-H-915 LoRa gateway accessory cards •	
LoRa: Semtech LoRa Basics™ Station Changes: • Updated to version 2.0.6-5 • AU915 Channel Plan – Default transmit power changed to 30 dBm • 16 Channel support added – Ability to manage MTCDT and MTCDTIP devices with two MTAC gateway accessory cards as one 16-channel device on The Things Network	GP-1459 GP-1270 TS-5107644

Known Behaviors (mPower 6.0.0)

The following devices and device configurations can be downgraded from mPower 6.0.0 to mPower 5.3.7 or mPower 5.3.8 • When the downgrade process is complete, a factory default is recommended • MTCDT with gateway accessory card: MTAC-LORA-H-868 or MTAC-LORA-H-915 • MTCDTIP with gateway accessory card: MTAC-LORA-H-868 or MTAC-LORA-H-915 • MTCAP, MTCAP2 • MTCDTIP2	-

Bug Fix (mPower 6.0.0)

Custom OpenVPN config breaks iptables • Customer unsuccessfully tried to setup a VPN connection using custom OVPN config file. • Upon investigation the root cause was found in this string: *remote 20.191.55.208 1194 udp* • If we split the string to these two, VPN connection works properly: *proto udp* *remote 20.191.55.208 1194* • Corresponding changes are implemented and such custom configuration can be applied and the tunnel connection will be established successfully.	GP-1421 MTX-3873 SP-5105937

Bug Fix (mPower 6.0.0)

Save & Apply restart redirects to LAN when connected through WAN • When connected through the WAN, the Web UI redirects to a LAN IP (Ethernet eth0) when executing a Save & Apply that requires a reboot • In mPower 6.0.0, if the current device IP is external (public) IP address or this is a domain name, redirection will be performed to the same address. Otherwise, the system will redirect to LAN IP address	GP-1006 IN-4375 MTX-4040
Device UI inaccessible after firmware upgrade if User Authentication enabled • If User Authentication feature was enabled prior to the firmware upgrade, UI will be inaccessible with SSL error when the upgrade is finished. To restore access to the device user should either reboot the device or restart lighttpd service. This may lead to the issues with upgrade in the field if there is no physical access to the device and no ssh access or SMS commands are enabled • This issue exists in the previous released firmware (mPower 5.2.1 and mPower 5.3.0) • In mPower 6.0.0, the issue is resolved and user can access the device after performing upgrade if the User Authentication is enabled	GP-1301 MTX-4143
SMS - quotation mark character (Double universal) " is displayed with the backslash \ character in the received SMS message (like an escaped character) • An extra slash character is added before the quotation mark " in the sent and received messages • In mPower 6.0.0, the issue is resolved and an extra slash is no longer added to the Sent and Received SMS messages	MTX-4359
PPP-IP Passthrough Mode – multiple farpd instances are running if connection re-establishes • In some cases there are multiple farpd instances running at the same time. The issue occurs when the PPP-IP Passthrough mode cellular connection is interrupted. When the cellular connection reestablishes, the system runs a new farpd instance, but does not end the previous one. This issue does not affect the functionality • In mPower 6.0.0, when cellular connection re-establishes and new settings are obtained, the farpd service restarts and there is only one farpd service in the services list	MTX-4350
libmts-io: • MCC and MNC values are retrieved incorrectly from table • In mPower 6.0.0, MCC and MNC values are retrieved correctly for further carrier detection	GP-114 MTX-4168

Deprecations (mPower 6.0.0)

DeviceHQ/Node-RED Custom Application • mPower 6.0.0 does not include support for the DeviceHQ/Node-RED Custom Application • Native support for Node-RED was deprecated in mPower 5.3.3 • For details on other methods to create custom applications, see creating a custom application	-
Python 2 support • Python 2 is not present in mPower. Only Python 3.8.11 is supported	GP-1224 MTX-4164
RF Survey • The RF Survey is not available for LTE devices and is removed from mPower 6.0.0 • **Page 404** is displayed when trying to access the page using the direct link: /rf_survey	GP-1444 MTX-4321

Schedule (mPower 6.0.0)

- Downloadable Versions
  - mPower 6.0.0 Availability: May 2022
  - Visit http://www.multitech.net/developer/downloads/
- Manufacturing Updates:
  - Devices that ship from MultiTech starting in July 2022 will include mPower 6.0.0
  - See part numbers impacted for details
- DeviceHQ: May 2022
- Differential Images:
  - Differential mPower updates are not available for mPower 6.0.0

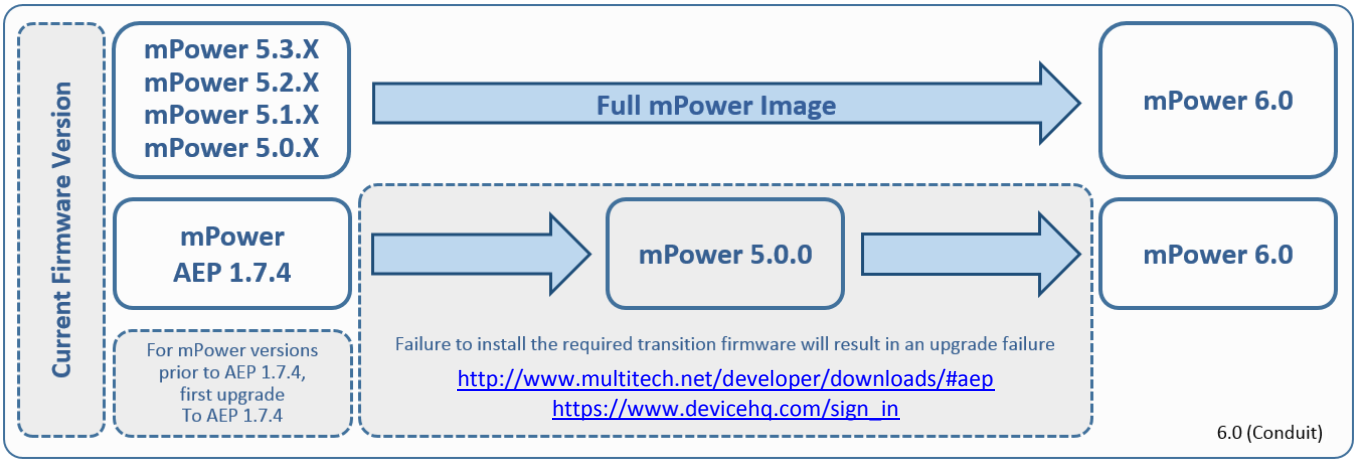
Models Impacted (mPower 6.0.0)

- MultiTech Conduit® Gateway
  - MTCDT-240A, MTCDT-246A, MTCDT-247A
  - MTCDT-L4E1, MTCDT-L4N1, MTCDT-LAT3, MTCDT-LAP3, MTCDT-LDC3, MTCDT-LSB3
- MultiTech Conduit® IP67 200 Series Base Station
  - MTCDTIP2-EN
  - MTCDTIP2-L4E1, MTCDTIP2-LNA3
- MultiTech Conduit® IP67 Base Station
  - MTCDTIP-266A, MTCDTIP-267A
  - MTCDTIP-L4E1, MTCDTIP-L4N1, MTCDTIP-LAP3, MTCDTIP-LDC3, MTCDTIP-LSB3
- MultiTech Conduit® AP Access Point
  - MTCAP-868, MTCAP2-868, MTCAP-915, MTCAP2-915
  - MTCAP-L4E1, MTCAP2-L4E1, MTCAP-LNA3, MTCAP2-LNA3

Upgrade Process (mPower 6.0.0)

To install mPower 6.0.0, 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.

NOTE: Differential mPower images are not available for mPower 6.0.0.



Revision History

Version	Author	Date	Change Description
-002	DT	05/19/2022	GPSD update removed from mPower 6.0.0
-001	DT	05/03/2022	Initial Version